

1

NENA i3 Standard for Next Generation 9-1-1

4 **Abstract:** This Standard provides the detailed functional and interface specifications for a
5 post-transition IP (Internet Protocol)-based multimedia telecommunications system,
6 including the Core Services and legacy gateways necessary to support delivery of
7 emergency calls via an IP-based Emergency Services IP network.

8
9
10 **This DRAFT document is not intended for distribution beyond the groups**
11 **developing or reviewing the document. The document is also not intended to be**
12 **used or referenced for development or procurement purposes until final**
13 **publication. All draft material is subject to change, and it is possible that the**
14 **document itself may never be approved for publication.**



17
18 NENA i3 Standard for Next Generation 9-1-1

19
20 ANS CANDIDATE NENA-STA-010.3-202Y

21 DSC Approval: MM/DD/YYYY

22 PRC Approval: MM/DD/YYYY

23 NENA Executive Board Approval: MM/DD/YYYY

24 Next Scheduled Review Date: Continuous review.

26 Prepared by:
27 National Emergency Number Association (NENA) 911 Core Services Committee, i3 Architecture
28 Working Group

30 Published by NENA
31 Printed in USA



32 **1 Executive Overview**

33 "i3" refers to the NG9-1-1 system architecture defined by NENA, which standardizes the
34 structure and design of Functional Elements making up the set of software services,
35 databases, network elements and interfaces needed to process multi-media emergency
36 calls and data for NG9-1-1.

37 This specification builds upon prior NENA publications including i3 requirements [2] and
38 architecture [70] documents. Familiarity with the concepts, terminology, and functional
39 elements described in these documents is a prerequisite. While the requirements and
40 architecture documents describe high-level concepts, the present document describes the
41 detailed functional elements and interfaces to those functional elements. If there are
42 discrepancies between the requirements or architecture documents and this document, this
43 document takes precedence. This document provides a baseline to other NG9-1-1 related
44 specifications.

45 The i3 solution supports end-to-end IP connectivity; gateways are used to accommodate
46 legacy wireline and wireless originating networks that are non-IP as well as legacy Public
47 Safety Answering Points (PSAPs) that interconnect to the i3 solution architecture. NENA i3
48 introduces the concept of an Emergency Services IP network (ESInet), which is designed
49 as an IP-based inter-network (network of networks) that can be shared by all public safety
50 agencies that may be involved in any emergency and a set of core services that process
51 9-1-1 calls¹ on that network (NGCS – NG9-1-1 Core Services). The i3 PSAP is capable of
52 receiving IP-based signaling and media for delivery of emergency calls conformant to the i3
53 Standard.

54 Getting to the i3 solution from the current E9-1-1 infrastructure implies a transition from
55 existing legacy originating network and 9-1-1 PSAP interconnections to next generation
56 interconnections. This document describes how NG9-1-1 works after transition, including
57 ongoing interworking requirements for IP-based and Time Division Multiplexed (TDM)-
58 based PSAPs and originating networks². It does not provide solutions for how legacy
59 PSAPs, originating networks, Selective Routers (SRs), and Automatic Location Identification
60 (ALI) systems evolve. Rather, it describes the end state when transition is complete. At
61 that point, SRs and existing ALI systems are decommissioned and all 9-1-1 calls are routed
62 using the Emergency Call Routing Function (ECRF) and arrive at the ESInet/NGCS via

¹ As defined in **Document Terminology**, the term "call" includes text messages and non-interactive calls.

² "Originating networks" include service providers who send calls to ESInets/NGCS.

63 Session Initiation Protocol (SIP). NENA has produced documents covering transition options
64 and procedures.

65 TDM-based PSAPs are connected to the ESInet/NGCS via a gateway (the Legacy PSAP
66 Gateway). The definition of the Legacy PSAP Gateway is broad enough so this type of
67 gateway may serve both primary and secondary PSAPs that have not been upgraded.

68 Similarly, the scope includes gateways for legacy wireline and wireless originating networks
69 (the Legacy Network Gateway) used by originating networks that cannot yet create call
70 signaling matching the interfaces described in this document for the ESInet/NGCS. It is not
71 envisioned that legacy originating networks will evolve to IP interconnect in all cases, and
72 thus Legacy Network Gateways will be needed for the foreseeable future. This document
73 considers all wireline, wireless, and other types of networks with IP interfaces, including IP
74 Multimedia Subsystems (IMS) [49] networks, although the document only describes the
75 external interfaces to the ESInet/NGCS, which a conforming network must support. This
76 document describes a common interface to the ESInet/NGCS, to be used by all types of
77 originating networks or devices. How originating networks, or devices within them, conform
78 is not visible to the ESInet/NGCS and is out of scope. The interface conforms to the best
79 practice described in IETF RFC 6881 [46]. ATIS 0700015 [151], which in turn is based on
80 3GPP TS 24.229 [226] and TS 23.167 [49], describes how IMS originating networks deliver
81 calls to the ESInet/NGCS as defined in this document.

82 This specification defines a number of Functional Elements (FEs) with their external
83 interfaces. An implementation of one or more FEs in a single indivisible unit (such as a
84 physical box, or software load for a server) is compliant with this specification if it
85 implements the functions as defined, and the external interfaces as defined for the
86 assembly of FEs. Internal interfaces between FEs that are not exposed outside the
87 implementation are not required to meet the standards herein, although it is recommended
88 that they do.

89 This document describes the “end state” that has been reached after a migration from
90 legacy TDM circuit-switched telephony, and the legacy E9-1-1 system built to support it, to
91 an all IP-based communication system with a corresponding IP-based Emergency Services
92 IP network. To get to this “end state” it is critical to understand the following underlying
93 assumptions:

94 1. All calls entering the ESInet are SIP-based. Gateways, if needed, are outside of, or on
95 the edge of, the ESInet. Calls that are IP-based, but use a protocol other than SIP or
96 are not fully i3-compliant, must be interworked to i3-compliant SIP prior to being
97 presented to the ESInet.

98 2. Access Network Providers (e.g., cable providers, DSL providers, fiber network
99 providers, WiMax providers, Long Term Evolution (LTE) wireless carriers, etc.) have

- 100 installed, provisioned, and operated some kind of Location Determination and
101 dissemination function for their networks.
- 102 3. All emergency calls entering the ESInet/NGCS will normally have location information
103 (which might be coarse, e.g., cell site/sector location in civic or geo-coordinate format)
104 in the signaling with the call.
- 105 4. 9-1-1 Authorities have transitioned from the tabular Master Street Address Guide
106 (MSAG) and Emergency Service Numbers (ESNs) to a Geographic Information System
107 (GIS) based Location Validation Function (LVF) and Emergency Call Routing Function
108 (ECRF).
- 109 5. 9-1-1 authorities have sufficiently accurate and complete GIS data, which are used to
110 provision the LVF and ECRF. A change to the 9-1-1 Authority's GIS system
111 automatically propagates to the ECRF and LVF and affects routing.
- 112 6. All civic locations will be validated by the access network against the LVF prior to an
113 emergency call being placed. This is analogous to MSAG validation.
- 114 7. Periodic revalidation of civic location against the LVF will be performed to assure that
115 location remains valid as changes in the GIS system that affect existing civic locations
116 are made.
- 117 8. Since the legacy circuit-switched TDM network will very likely continue to be used for
118 the foreseeable future (both wireline and wireless), the i3 architecture defines a
119 Legacy Network Gateway (LNG) to interface between the legacy network and the
120 ESInet/NGCS.
- 121 9. Transition to i3 is complete when the existing SR and ALI are no longer used within a
122 jurisdiction. Even after that time, some PSAPs may not have upgraded to i3. The i3
123 architecture defines a Legacy PSAP Gateway (LPG) to interface between the
124 ESInet/NGCS and a legacy PSAP. The LPG supports the delivery of an emergency call
125 through the ESInet/NGCS to a legacy PSAP as well as the transfer of an emergency call
126 between i3-PSAPs and legacy PSAPs.
- 127 10. Federal, State/Provincial, and local laws, regulations, and rules (such as, for example,
128 those specifically referring to ALI and Selective Routers) may need to be modified to
129 support NG9-1-1 system deployment.
- 130 11. While NG9-1-1 is based on protocols that are international and are designed to allow
131 visitors and equipment not of North American origin to work with NG9-1-1, the specific
132 protocol mechanisms, especially interworking of legacy telecom and ESInet/NGCS
133 protocols are North American-specific and may not be applicable in other areas.

134

Table of Contents

135	1 EXECUTIVE OVERVIEW.....	2
136	DOCUMENT TERMINOLOGY	19
137	INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY	20
138	REASON FOR ISSUE/REISSUE	21
139	2 GENERAL CONCEPTS	22
140	2.1 IDENTIFIERS.....	22
141	2.1.1 <i>Agency Identifier</i>	22
142	2.1.2 <i>Agent Identifier</i>	22
143	2.1.3 <i>Element Identifier</i>	22
144	2.1.4 <i>URN Emergency Namespace</i>	22
145	2.1.5 <i>Services</i>	23
146	2.1.6 <i>Call Identifier</i>	23
147	2.1.7 <i>Incident Tracking Identifier</i>	23
148	2.1.8 <i>LogEvent Identifier</i>	24
149	2.1.9 <i>Queue Identifier</i>	24
150	2.1.10 <i>Secure Telephone Identity</i>	25
151	2.2 TIME.....	25
152	2.3 TIMESTAMP.....	25
153	2.4 EVENTS COMMON TO MULTIPLE FUNCTIONAL ELEMENTS.....	25
154	2.4.1 <i>Element State</i>	26
155	2.4.2 <i>Service State</i>	27
156	2.5 LOCATION REPRESENTATION	29
157	2.6 xCARD/jCARD	30
158	2.7 EMERGENCY SERVICES IP NETWORKS	30
159	2.8 SERVICE INTERFACES.....	32
160	2.8.1 <i>HTTP Transport</i>	33
161	2.8.2 <i>Status Codes</i>	33
162	2.8.3 <i>Versions</i>	33
163	2.9 REDUNDANCY	35
164	2.10 TELEPHONE NUMBERS.....	36
165	2.11 FUNCTIONAL ELEMENTS.....	36

[MM/DD/YYYY]

Page 5 of 675



166	3 INTERFACES	36
167	3.1 SIP CALL	37
168	3.1.1 <i>Minimal Methods needed to handle a call</i>	38
169	3.1.2 <i>Methods allowed to be initiated by any UA which MUST be supported by i3 elements</i>	41
170	3.1.3 <i>Methods used within the ESInet/NGCS</i>	43
171	3.1.4 <i>Response Codes</i>	44
172	3.1.5 <i>Header fields and Request URI supported at the interface to the NGCS</i>	46
173	3.1.6 <i>Header fields Accepted and also used internally</i>	48
174	3.1.7 <i>Resource Prioritization</i>	50
175	3.1.8 <i>History-Info and Reason Parameter</i>	51
176	3.1.9 <i>Media</i>	51
177	3.1.10 <i>Instant Messaging</i>	55
178	3.1.11 <i>Non-interactive calls</i>	55
179	3.1.12 <i>Bodies in messages</i>	56
180	3.1.13 <i>Transport</i>	56
181	3.1.14 <i>Call Routing</i>	57
182	3.1.15 <i>Originating Network Interface</i>	58
183	3.1.16 <i>PSAP Interface</i>	59
184	3.1.17 <i>Element Overload</i>	59
185	3.1.18 <i>Maintaining Connections and NAT Traversal</i>	59
186	3.1.19 <i>Advanced Automatic Crash Notification Calls</i>	59
187	3.2 LOCATION.....	61
188	3.3 POLICY (POLICIES).....	64
189	3.3.1 <i>Policy Store Web Service</i>	65
190	3.3.2 <i>Policy Store Replication</i>	73
191	3.3.3 <i>Route Policy Syntax</i>	74
192	3.4 LoST	106
193	3.4.1 <i>Emergency Call Routing using LoST</i>	107
194	3.4.2 <i>Location Validation</i>	108
195	3.4.3 <i><findService> Request</i>	108
196	3.4.4 <i><findService> Response</i>	109
197	3.4.5 <i>locationInvalidated</i>	112

198	<i>3.4.6 getServiceBoundary</i>	112
199	<i>3.4.7 listServices and listServicesByLocation</i>	112
200	<i>3.4.8 Error Responses.....</i>	112
201	<i>3.4.9 Warnings.....</i>	113
202	<i>3.4.10 LoST Extensions.....</i>	114
203	<i>3.4.11 LoSt Query Examples</i>	117
204	3.5 EVENT NOTIFICATION	119
205	3.6 SPATIAL INTERFACE FOR LAYER REPLICATION	119
206	3.7 DISCREPANCY REPORTING.....	120
207	<i>3.7.1 Discrepancy Report</i>	122
208	<i>3.7.2 Discrepancy Resolution.....</i>	124
209	<i>3.7.3 Status Update.....</i>	125
210	<i>3.7.4 Policy Store Discrepancy Report.....</i>	126
211	<i>3.7.5 LoST Discrepancy Report.....</i>	128
212	<i>3.7.6 BCF Discrepancy Report</i>	129
213	<i>3.7.7 Logging Service Discrepancy Report.....</i>	131
214	<i>3.7.8 PSAP Call Taker Discrepancy Report.....</i>	132
215	<i>3.7.9 SIP Discrepancy Report</i>	132
216	<i>3.7.10 Permissions/Security/Authentication Discrepancy Report</i>	134
217	<i>3.7.11 GIS Discrepancy Report.....</i>	135
218	<i>3.7.12 LIS Discrepancy Report</i>	137
219	<i>3.7.13 Policy Discrepancy Report.....</i>	138
220	<i>3.7.14 Originating Service Provider Discrepancy Report</i>	139
221	<i>3.7.15 Call Transfer Failure Discrepancy Report.....</i>	141
222	<i>3.7.16 MSAG Conversion Service (MCS) Discrepancy Report</i>	142
223	<i>3.7.17 ESRP Discrepancy Report</i>	143
224	<i>3.7.18 ADR/IS-ADR Discrepancy Report.....</i>	144
225	<i>3.7.19 Network Discrepancy Report.....</i>	145
226	<i>3.7.20 Interactive Media Response (IMR) Discrepancy Report</i>	146
227	<i>3.7.21 Test Call Generator Discrepancy Report.....</i>	147
228	<i>3.7.22 Log Signature/Certificate Discrepancy Report.....</i>	148
229	4 FUNCTIONS	150

[MM/DD/YYYY]

Page 7 of 675



230	4.1 BORDER CONTROL FUNCTION (BCF)	150
231	4.1.1 <i>Functional Description</i>	150
232	4.1.2 <i>Interface Description</i>	153
233	4.1.3 <i>Roles and Responsibilities</i>	155
234	4.1.4 <i>Operational Considerations</i>	155
235	4.2 EMERGENCY SERVICE ROUTING PROXY (ESRP)	156
236	4.2.1 <i>Functional Description</i>	156
237	4.2.2 <i>Interface Description</i>	169
238	4.2.3 <i>Policy Elements</i>	175
239	4.2.4 <i>Provisioning</i>	176
240	4.2.5 <i>Roles and Responsibilities</i>	176
241	4.2.6 <i>Operational Considerations</i>	176
242	4.3 EMERGENCY CALL ROUTING FUNCTION (ECRF) AND LOCATION VALIDATION FUNCTION (LVF)	178
243	4.3.1 <i>Functional Description</i>	179
244	4.3.2 <i>Interface Description</i>	180
245	4.3.3 <i>Data Structures</i>	183
246	4.3.4 <i>Coalescing Data and Gap/Overlap Processing</i>	186
247	4.3.5 <i>Replicas</i>	188
248	4.3.6 <i>Provisioning</i>	189
249	4.3.7 <i>Roles and Responsibilities</i>	189
250	4.3.8 <i>Operational Considerations</i>	190
251	4.3.9 <i>Internal and External ECRF/LVFs</i>	192
252	4.3.10 <i>Relationship Between ECRF and LVF</i>	192
253	4.4 MSAG CONVERSION SERVICE (MCS)	192
254	4.4.1 <i>PIDF-LO to MSAG Conversion</i>	193
255	4.4.2 <i>MSAG to PIDF-LO Conversion</i>	194
256	4.5 GEOFENCE SERVICE (GFS)	195
257	4.5.1 <i>GEOFENCERequest</i>	195
258	4.5.2 <i>ReverseGEOFENCERequest</i>	196
259	4.6 PSAP	197
260	4.6.1 <i>SIP Call interface</i>	197
261	4.6.2 <i>Media</i>	198

[MM/DD/YYYY]

Page 8 of 675



262	<i>4.6.3 LoST interface</i>	198
263	<i>4.6.4 LIS Interfaces</i>	199
264	<i>4.6.5 Bridge Interface</i>	200
265	<i>4.6.6 ElementState</i>	200
266	<i>4.6.7 ServiceState</i>	200
267	<i>4.6.8 AbandonedCall Event</i>	200
268	<i>4.6.9 DequeueRegistration</i>	200
269	<i>4.6.10 QueueState</i>	200
270	<i>4.6.11 SI</i>	201
271	<i>4.6.12 Logging Service</i>	201
272	<i>4.6.13 Security Posture</i>	201
273	<i>4.6.14 Policy</i>	201
274	<i>4.6.15 Additional Data Dereference</i>	201
275	<i>4.6.16 Time Interface</i>	202
276	<i>4.6.17 Test Call</i>	202
277	<i>4.6.18 Testing of Policy Rules</i>	203
278	<i>4.6.19 Call Diversion</i>	204
279	<i>4.6.20 Incidents</i>	205
280	4.7 BRIDGING AND TRANSFERS	205
281	<i>4.7.1 Attended Transfers</i>	205
282	<i>4.7.2 Blind Transfers</i>	233
283	<i>4.7.3 Premature abandonment of a transfer by the Primary PSAP</i>	233
284	<i>4.7.4 Passing Data to Agencies via Bridging</i>	234
285	<i>4.7.5 Interoperability Between Transfer Models</i>	235
286	<i>4.7.6 Conference Bridging for MSRP Text</i>	235
287	4.8 MEDIA MIXING	237
288	<i>4.8.1 Mixing of Real-time Text</i>	237
289	4.9 INTER-ESINET TRANSFERS	238
290	<i>4.9.1 Upstream Ad Hoc Method to Downstream Ad Hoc Method</i>	239
291	<i>4.9.2 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Ad Hoc Method</i>	240
292	<i>4.9.3 Upstream Ad Hoc Method to Downstream Route All Calls Via a Conference-aware UA Method</i>	240

[MM/DD/YYYY]

Page 9 of 675



293	<i>4.9.4 Upstream Route All Calls Via a Conference Aware UA Method to Downstream Route All Calls Via a Conference Aware UA Method</i>	244
295	4.10 LOCATION INFORMATION SERVER (LIS)	250
296	4.11 ADDITIONAL DATA REPOSITORY (ADR)	252
297	<i> 4.11.1 Identity Searchable Additional Data Repository (IS-ADR).....</i>	254
298	4.12 LOGGING SERVICE	255
299	<i> 4.12.1 Logging Introduction.....</i>	256
300	<i> 4.12.2 Media Recording Interface.....</i>	256
301	<i> 4.12.3 Log Recording</i>	267
302	<i> 4.12.4 Roles and Responsibilities.....</i>	288
303	<i> 4.12.5 Operational Considerations</i>	288
304	4.13 FOREST GUIDE.....	289
305	<i> 4.13.1 Functional Description</i>	289
306	<i> 4.13.2 Interface Description</i>	290
307	<i> 4.13.3 Data Structures.....</i>	290
308	<i> 4.13.4 Roles and Responsibilities.....</i>	290
309	<i> 4.13.5 Operational Considerations</i>	291
310	<i> 4.13.6 Security Considerations</i>	291
311	4.14 DNS	291
312	4.15 SERVICE/AGENCY LOCATOR.....	292
313	<i> 4.15.1 Service/Agency Locator Record Store</i>	293
314	<i> 4.15.2 Service/Agency Locator Search by Location</i>	293
315	<i> 4.15.3 Service/Agency Locator Search by Name</i>	294
316	<i> 4.15.4 Service/Agency Locator Record</i>	295
317	<i> 4.15.5 Service/Agency Locator Inter-ESInet Index.....</i>	296
318	4.16 POLICY STORE	298
319	<i> 4.16.1 Functional Description</i>	298
320	<i> 4.16.2 Interface Description</i>	298
321	<i> 4.16.3 Roles and Responsibilities</i>	298
322	4.17 TIME SERVER	298
323	4.18 ORIGINATING NETWORKS AND DEVICES.....	299
324	<i> 4.18.1 SIP Call Interface</i>	299

[MM/DD/YYYY]

Page 10 of 675



325	4.18.2	<i>Location by Reference</i>	299
326	4.18.3	<i>Additional Data Repository</i>	299
327	4.19	MAPPING DATA SERVICE (MDS)	299
328	4.20	OUTBOUND CALL INTERFACE FUNCTION (OCIF).....	301
329	4.21	SECURE TELEPHONE IDENTITY (STI).....	304
330	4.21.1	<i>STI Verification for Emergency 9-1-1 Calls</i>	307
331	4.21.2	<i>STI Authentication for PSAP-Originated Calls.</i>	308
332	4.21.3	<i>Call Validation Treatment</i>	308
333	4.21.4	<i>STI Secure Key Store</i>	309
334	4.22	INCIDENT DATA EXCHANGE (IDX)	309
335	5	SECURITY	309
336	5.1	IDENTITY.....	309
337	5.2	PSAP CREDENTIALING AGENCY.....	310
338	5.3	ROLES	310
339	5.4	AUTHENTICATION	313
340	5.5	TRUSTING ASSERTING AND RELYING PARTIES.....	314
341	5.6	AUTHORIZATION AND DATA RIGHTS MANAGEMENT.....	315
342	5.7	INTEGRITY PROTECTION.....	316
343	5.8	PRIVACY.....	316
344	5.9	ALGORITHM UPGRADES	316
345	5.10	JSON WEB SIGNATURES	317
346	6	GATEWAYS.....	318
347	6.1	LEGACY NETWORK GATEWAY (LNG)	319
348	6.1.1	<i>Protocol Interwork Function (PIF)</i>	321
349	6.1.2	<i>NG9-1-1-specific Interwork Function (NIF)</i>	330
350	6.1.3	<i>Location Interwork Function (LIF)</i>	341
351	6.2	LEGACY PSAP GATEWAY (LPG)	358
352	6.2.1	<i>Protocol Interwork Function (PIF)</i>	360
353	6.2.2	<i>NG9-1-1-Specific Interwork Function (NIF)</i>	371
354	6.2.3	<i>Location Interwork Function (LIF)</i>	391
355	6.2.4	<i>Timing at the Legacy PSAP Gateway</i>	392
356	6.2.5	<i>Trouble Detection/Reporting at the Legacy PSAP Gateway</i>	394

357	7 DATA AND THE EMERGENCY INCIDENT DATA OBJECT	394
358	7.1 ADDITIONAL DATA	394
359	7.2 ADDITIONAL DATA ASSOCIATED WITH A PSAP, THE EMERGENCY INCIDENT DATA OBJECT	396
360	8 3RD PARTY ORIGINATION	396
361	8.1 3RD PARTY CLIENT IS REFERRED TO PSAP; PSAP ESTABLISHES CONFERENCE	396
362	8.2 3RD PARTY CALL AGENT AND CALLER ADDED TO CONFERENCE	399
363	9 TEST CALLS	401
364	10 IANA ACTIONS.....	402
365	10.1 "URN:EMERGENCY" NAMESPACE	402
366	10.2 "URN:EMERGENCY:SERVICE" URN SUBREGISTRY.....	402
367	10.3 "URN:EMERGENCY:SERVICE:SOS" REGISTRY.....	402
368	10.4 "URN:EMERGENCY:SERVICE:TEST" REGISTRY	403
369	10.5 "URN:EMERGENCY:SERVICE:RESPONDER" REGISTRY	403
370	10.6 "URN:EMERGENCY:SERVICE:RESPONDER.POLICE" REGISTRY	404
371	10.7 "POLICE.FEDERAL" REGISTRY	404
372	10.8 "URN:EMERGENCY:SERVICE:RESPONDER.FIRE" REGISTRY	405
373	10.9 "URN:EMERGENCY:SERVICE:RESPONDER.EMS" REGISTRY.....	405
374	10.10 "URN:EMERGENCY:UID" REGISTRY	405
375	10.11 "SERVICE NAMES" REGISTRY	405
376	10.12 "SERVICE STATE" REGISTRY	406
377	10.13 "ELEMENT STATE" REGISTRY	407
378	10.14 "URN:EMERGENCY:SERVICE:SERVICEAGENCYLOCATOR" REGISTRY.....	407
379	10.15 "SIPHEADERISOPERATORCONDITIONS" REGISTRY	408
380	10.16 "URN:EMERGENCY:MEDIA-FEATURE" REGISTRY	408
381	10.17 "QUEUE STATE" REGISTRY	409
382	10.18 "SECURITY POSTURE" REGISTRY.....	409
383	10.19 "ESRP NOTIFY EVENT CODE" REGISTRY	410
384	10.20 "ROUTE CAUSE" REGISTRY.....	410
385	10.21 "LOG EVENT" REGISTRY.....	411
386	10.22 "LOG EVENT PROTOCOL" REGISTRY	414
387	10.23 "LOG EVENT CALL TYPES" REGISTRY.....	415
388	10.24 "CALL STATES" REGISTRY.....	415

[MM/DD/YYYY]

Page 12 of 675



389	10.25 "LOGEVENT ANNOUNCEMENT TYPES" REGISTRY	416
390	10.26 "NON-RTP MEDIA TYPES" REGISTRY	417
391	10.27 "AGENCY ROLES" REGISTRY	417
392	10.28 "AGENT ROLES" REGISTRY.....	418
393	10.29 "STATUS CODES" REGISTRY	420
394	10.30 "INTERFACE NAMES" REGISTRY	421
395	10.31 "MATCH TYPE" REGISTRY	422
396	10.32 "GIS LAYERS" REGISTRY.....	423
397	10.33 "POLICY TYPE" REGISTRY	424
398	10.34 "DISCREPANCY REPORT STATUS TOKEN" REGISTRY	426
399	10.35 "EVENT PACKAGE" REGISTRY.....	433
400	10.36 "AGENT STATES" REGISTRY	434
401	11 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS	434
402	11.1 OPERATIONS IMPACTS SUMMARY	434
403	11.2 TECHNICAL IMPACTS SUMMARY	434
404	11.3 SECURITY IMPACTS SUMMARY.....	435
405	11.4 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK.....	436
406	11.5 ANTICIPATED TIMELINE.....	438
407	11.6 COST FACTORS	438
408	11.7 COST RECOVERY CONSIDERATIONS	439
409	11.8 ADDITIONAL IMPACTS (NON-COST RELATED).....	439
410	11.9 ABBREVIATIONS, TERMS, AND DEFINITIONS	440
411	12 REFERENCES.....	470
412	APPENDIX A - MAPPING BETWEEN NG9-1-1 AND LEGACY ALI DATA STRUCTURES (INFORMATIVE)	487
414	APPENDIX B – SI PROVISIONING DATA MODEL (NORMATIVE)	499
415	B.1 CENTERLINES	500
416	B.2 STREET/ADDRESS STRUCTURES	504
417	B.2.1 COMPLETESTREETNAME	504
418	B.2.2 COMPLETEADDRESSNUMBER	505
419	B.2.3 STREETSEGMENT	505
420	B.2.4 COMPLETEADDRESS	506

[MM/DD/YYYY]

Page 13 of 675



421	B.3 SITE/STRUCTURE	507
422	B.4 STATE BOUNDARY	510
423	B.5 COUNTY BOUNDARY.....	511
424	B.6 INCORPORATED MUNICIPALITY BOUNDARY	511
425	B.7 UNINCORPORATED COMMUNITY BOUNDARY	512
426	B.8 NEIGHBORHOOD COMMUNITY BOUNDARY	514
427	B.9 SERVICE BOUNDARY	515
428	B.9.1 SERVICE RESPONSE.....	516
429	B.10 MSAG	517
430	B.10.1 MSAG STREET NUMBER EXCEPTION	518
431	APPENDIX C – SUPPORT FOR PSAP CALL CONTROL FEATURES (NORMATIVE)	519
432	C.1 ASSUMPTIONS REGARDING BEHAVIOR IN THE ORIGINATING NETWORK	519
433	C.1.1 ASSUMED BEHAVIOR IN A LEGACY ORIGINATING NETWORK	520
434	C.1.1.1 SS7 SIGNALING FROM ORIGINATING END OFFICE.....	520
435	C.1.1.2 MF SIGNALING FROM ORIGINATING END OFFICE	521
436	C.1.2 ASSUMED BEHAVIOR IN A SIP-BASED ORIGINATING NETWORK	522
437	C.2 BRIDGING CONSIDERATIONS.....	524
438	C.2.1 SIP AD HOC METHOD.....	525
439	C.2.2 ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD.....	525
440	C.3 CALLED PARTY HOLD/SWITCH-HOOK STATUS	526
441	C.3.1 PROCEDURES AT THE LEGACY NETWORK GATEWAY	526
442	C.3.1.1 SS7 SIGNALING FROM ORIGINATING END OFFICE.....	526
443	C.3.1.2 MF SIGNALING FROM ORIGINATING END OFFICE	529
444	C.3.2 PROCEDURES AT THE ESRP	531
445	C.3.3 PROCEDURES AT THE I3 PSAP.....	532
446	C.3.4 PROCEDURES AT THE LEGACY PSAP GATEWAY	533
447	C.3.4.1 PROCEDURES AT THE LPG-NIF COMPONENT	533
448	C.3.4.2 PROCEDURES AT THE LPG-PIF COMPONENT	534
449	C.3.5 PROCEDURES AT THE BRIDGE.....	534
450	C.3.5.1 USING THE SIP AD-HOC METHOD	535
451	C.3.5.2 USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD	535
452	C.4 RINGBACK	535

[MM/DD/YYYY]

Page 14 of 675



453	C.4.1	PROCEDURES AT THE PSAP	535
454	C.4.2	PROCEDURES AT THE LEGACY PSAP GATEWAY	536
455	C.4.2.1	PROCEDURES AT THE LPG-PIF COMPONENT	536
456	C.4.2.2	PROCEDURES AT THE LPG-NIF COMPONENT	536
457	C.4.3	PROCEDURES AT THE ESRP	537
458	C.4.4	PROCEDURES AT THE LEGACY NETWORK GATEWAY	537
459	C.4.4.1	PROCEDURES AT THE LNG-NIF COMPONENT	537
460	C.4.4.2	PROCEDURES AT THE PIF COMPONENT	538
461	C.4.5	PROCEDURES AT THE BRIDGE.....	538
462	C.4.5.1	USING THE AD HOC METHOD	538
463	C.4.5.2	USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD	539
464	C.5	ENHANCED CALLED PARTY HOLD.....	539
465	C.5.1	PROCEDURES AT THE LNG FOR CALLS RECEIVED OVER SS7 TRUNK GROUPS	540
466	C.5.1.1	PROCEDURES AT THE LNG-PIF COMPONENT	540
467	C.5.1.2	PROCEDURES AT THE LNG-NIF COMPONENT.....	540
468	C.5.2	PROCEDURES AT THE LNG FOR CALLS RECEIVED OVER MF TRUNK GROUPS	541
469	C.5.2.1	PROCEDURES AT THE LNG-PIF COMPONENT	541
470	C.5.2.2	PROCEDURES AT THE LNG-NIF COMPONENT.....	542
471	C.5.3	PROCEDURES AT THE BRIDGE.....	543
472	C.5.3.1	USING THE SIP AD HOC METHOD.....	543
473	C.5.3.2	USING THE ROUTE ALL CALLS VIA A CONFERENCE-AWARE UA METHOD	543
474	D	APPENDIX D – EXAMPLE CALL FLOWS (INFORMATIVE)	544
475	D.1	DATA BY VALUE SIP END-TO-END EXAMPLE CALL FLOW	544
476	D.1.1	STEP-BY-STEP DESCRIPTION	550
477	D.1.1.1	BOOT UP ACTIVITIES (STEPS NOT SHOWN)	550
478	D.1.1.2	PRE-CALL ACTIVITIES	550
479	D.1.1.3	CALL-RELATED ACTIVITIES	551
480	D.2	LOCATION BY REFERENCE / CELLULAR / HELD EXAMPLE CALL FLOW.....	560
481	D.2.1	STEP-BY-STEP DESCRIPTION	567
482	D.2.1.1	PROVISIONING ACTIVITIES (STEPS NOT SHOWN)	567
483	D.2.1.2	PRE-CALL ACTIVITIES	567
484	D.2.1.3	CALL-RELATED ACTIVITIES	567

[MM/DD/YYYY]

Page 15 of 675



485	APPENDIX E - REST/JSON DEFINITIONS (NORMATIVE)	582
486	E.1 POLICY STORE	582
487	E.1.1 OPENAPI INTERFACE DESCRIPTION	582
488	E.1.2 EXAMPLES	601
489	E.2 DISCREPANCY REPORT	601
490	E.2.1 OPENAPI INTERFACE DESCRIPTION	601
491	E.2.2 EXAMPLES	618
492	E.3 DEQUEUE REGISTRATION	618
493	E.3.1 OPENAPI INTERFACE DESCRIPTION	618
494	E.4 MSAG CONVERSION SERVICE	620
495	E.4.1 OPENAPI INTERFACE DESCRIPTION	620
496	E.4.2 EXAMPLES	623
497	E.5 GEOCODE CONVERSION SERVICE	623
498	E.5.1 OPENAPI INTERFACE DESCRIPTION	623
499	E.5.2 EXAMPLES	625
500	E.6 TEST CALL	625
501	E.6.1 OPENAPI INTERFACE DESCRIPTION	625
502	E.6.2 EXAMPLES	628
503	E.7 ADDITIONAL DATA REPOSITORY	628
504	E.7.1 OPENAPI INTERFACE DESCRIPTION	628
505	E.7.2 EXAMPLES	630
506	E.8 LOGGING SERVICE	630
507	E.8.1 OPENAPI INTERFACE DESCRIPTION	630
508	E.8.2 EXAMPLES	660
509	E.9 BAD ACTOR SERVICE	660
510	E.9.1 OPENAPI INTERFACE DESCRIPTION	660
511	E.10 SERVICE/AGENCY LOCATOR SERVICE	661
512	E.10.1 OPENAPI INTERFACE DESCRIPTION	661
513	E.11 NOTIFY BODIES	666
514	E.11.1 ESRP NOTIFY NOTIFY BODY	666
515	E.11.1.1 JSON SCHEMA	666
516	E.11.1.2 GAP-OVERLAP NOTIFY BODY	667

[MM/DD/YYYY]

Page 16 of 675



517	E.11.1.3 JSON SCHEMA	667
518	E.11.2 ABANDONED CALL NOTIFY BODY.....	668
519	E.11.2.1 JSON SCHEMA	668
520	E.11.3 ELEMENT STATE NOTIFY BODY	669
521	E.11.3.1 JSON SCHEMA	669
522	E.11.3.2 QUEUE STATE NOTIFY BODY	670
523	E.11.3.3 JSON SCHEMA	670
524	E.11.3.4 SERVICE STATE NOTIFY BODY	671
525	E.11.3.5 JSON SCHEMA	671
526	E.11.4 COMMON YAML.....	672
527	E.11.4.1 OPENAPI INTERFACE DESCRIPTION	672
528	ACKNOWLEDGEMENTS.....	674
529		
530		

[MM/DD/YYYY]

Page 17 of 675



531
532
533

**NENA
STANDARD DOCUMENT
NOTICE**

534 This Standard Document (STA) is published by the National Emergency Number Association
535 (NENA) as an information source for 9-1-1 System Service Providers, network interface
536 vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an
537 industry Standard it provides for interoperability among systems and services adopting and
538 conforming to its specifications.

539 NENA reserves the right to revise this Standard Document for any reason including, but not
540 limited to:

- 541 • Conformity with criteria or standards promulgated by various agencies,
542 • Utilization of advances in the state of the technical arts,
543 • Reflecting changes in the design of equipment, network interfaces, or services described
544 herein.

545 This document is an information source for the voluntary use of communication centers. It is
546 not intended to be a complete operational directive.

547 It is possible that certain advances in technology or changes in governmental regulations will
548 precede these revisions. All NENA documents are subject to change as technology or other
549 influencing factors change. Therefore, this NENA document should not be the only source of
550 information used. NENA recommends that readers contact their 9-1-1 System Service Provider
551 (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal
552 counsel, to ensure compliance with current regulations.

553 Patents may cover the specifications, techniques, or network interface/system characteristics
554 disclosed herein. No license is granted, whether expressed or implied. This document shall not
555 be construed as a suggestion to any manufacturer to modify or change any of its products, nor
556 does this document represent any commitment by NENA, or any affiliate thereof, to purchase
557 any product, whether or not it provides the described characteristics.

558 By using this document, the user agrees that NENA will have no liability for any consequential,
559 incidental, special, or punitive damages arising from use of the document.

560 NENA's Committees have developed this document. Recommendations for changes to this
561 document may be submitted to:

562 National Emergency Number Association
563 1700 Diagonal Rd, Suite 500
564 Alexandria, VA 22314
565 202.466.4911
566 or commleadership@nena.org

[MM/DD/YYYY]

Page 18 of 675



567 **NENA: The 9-1-1 Association** improves 9-1-1 through research, standards development,
568 training, education, outreach, and advocacy. Our vision is a public made safer and more
569 secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1
570 professionals. Learn more at nena.org.

571

572 Document Terminology

573 This section defines keywords, as they should be interpreted in NENA documents. The form
574 of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document.
575 Any of these words used in lower case and not emphasized do not have special significance
576 beyond normal usage.

- 577 1. **MUST, SHALL, REQUIRED:** These terms mean that the definition is a normative
578 (absolute) requirement of the specification.
- 579 2. **MUST NOT:** This phrase, or the phrase "SHALL NOT", means that the definition is an
580 absolute prohibition of the specification.
- 581 3. **SHOULD:** This word, or the adjective "RECOMMENDED", means that there may exist
582 valid reasons in particular circumstances to ignore a particular item, but the full
583 implications must be understood and carefully weighed before choosing a different
584 course.
- 585 4. **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" means that there
586 may exist valid reasons in particular circumstances when the particular behavior is
587 acceptable or even useful, but the full implications should be understood and the
588 case carefully weighed before implementing any behavior described with this label.
- 589 5. **MAY:** This word, or the adjective "OPTIONAL", means that an item is truly optional.
590 One vendor may choose to include the item because a particular marketplace
591 requires it or because the vendor feels that it enhances the product while another
592 vendor may omit the same item. An implementation which does not include a
593 particular option "must" be prepared to interoperate with another implementation
594 which does include the option, though perhaps with reduced functionality. In the
595 same vein an implementation which does include a particular option "must" be
596 prepared to interoperate with another implementation which does not include the
597 option (except, of course, for the feature the option provides.)

598 These definitions are based on IETF [RFC 2119](https://www.rfc-editor.org/rfc/rfc2119.html).

599 This document uses the word "call" to mean the following:

[MM/DD/YYYY]

Page 19 of 675



- 600 1. A session established by signaling with two-way real-time media. This type of call
601 usually involves a human making a request for help. This document sometimes uses
602 “voice call”, “video call”, or “text call” when specific media is of primary importance.
603 Real-time text and instant messaging using MSRP are examples of text calls of this
604 type.
605 2. A one-time notification or series of data exchanges without media. A call of this type
606 is referred to as a “non-interactive call”. Such calls often do not involve a human at
607 the calling end. Examples of non-interactive calls include a burglar alarm, an
608 automatically detected HAZMAT spill, or a flooding sensor.

609 All types of calls are handled the same way.

610 The term “Incident” is used to refer to a real-world event for which one or more calls may
611 be received.

612 The term Location Information Server (LIS) as listed in the NENA Master Glossary includes
613 functions out of scope for i3. This document only uses those functions of a LIS described in
614 Sections 3.2 and 4.10.

615 **Intellectual Property Rights (IPR) Policy**

616 NOTE – The user’s attention is called to the possibility that compliance with this
617 standard may require use of an invention covered by patent rights. By publication of this
618 standard, NENA takes no position with respect to the validity of any such claim(s) or of
619 any patent rights in connection therewith. If a patent holder has filed a statement of
620 willingness to grant a license under these rights on reasonable and nondiscriminatory
621 terms and conditions to applicants desiring to obtain such a license, then details may be
622 obtained from NENA by contacting the Committee Resource Manager identified on
623 NENA’s website at www.nena.org/ipr.

624 Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any
625 interested party to bring to its attention any copyrights, patents or patent applications, or
626 other proprietary rights that may cover technology that may be required to implement this
627 standard.

628 Please address the information to:

629 National Emergency Number Association
630 1700 Diagonal Rd, Suite 500
631 Alexandria, VA 22314
632 202.466.4911
633 or crm@nena.org

[MM/DD/YYYY]

Page 20 of 675



634 **Reason for Issue/Reissue**

635 NENA reserves the right to modify this document. Upon revision, the reason(s) will be
636 provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA 08-003	06/14/2011	Initial Document
NENA-STA-010.2-2016	09/10/2016	This document is issued to define a specification describing the functionality supported by elements associated with an ESInet and the interconnection of these functional elements. This second version of the Functional and Interface Standards for the NENA i3 Solution is intended to be used in Standards Development Organization (SDO) liaisons, and Request for Information (RFI)-like processes. It provides more detailed specifications for interfaces and functions, compared to the prior version and reflects experience with early implementations. The NENA i3 Architecture Working Group plans to release subsequent versions of the Standard as new work items are identified and resolved. Provide more detailed specification and reflect early implementation experience. Provisioning was taken out of scope and the section was removed.
NENA-STA-010.3-202Y	[MM/DD/YYYY]	Major re-write. This version substantively modifies and provides additional specification to many sections of this document.

637

[MM/DD/YYYY]

Page 21 of 675



638 **2 General Concepts**

639 **2.1 Identifiers**

640 To enable calls to be handled in an interconnected ESInet/NGCS, identifiers are
641 standardized in the subsections below.

642 **2.1.1 Agency Identifier**

643 An Agency is represented by a fully qualified domain name (FQDN) as defined in RFC 2664
644 [229]. Each Agency MUST use one FQDN consistently in order to correlate actions across a
645 wide range of calls and incidents. Any FQDN in the public Domain Name System (DNS) is
646 acceptable as long as each distinct Agency uses a different FQDN. This ensures that each
647 Agency Identifier (ID) is globally unique. An example of an Agency Identifier is
648 "police.allegheny.pa.us". FQDNs can be represented with or without a final terminating dot
649 (the final dot represents the DNS root). FQDNs are case-insensitive. FQDNs with and
650 without a terminating dot MUST be treated as equivalent (e.g., "police.allegheny.pa.us."
651 and "police.allegheny.pa.us" are equivalent).

652 **2.1.2 Agent Identifier**

653 An agent MUST be represented by an agent identifier that is a username, using the syntax
654 for "Dot-string" in RFC 5321 [133] (that is, the user part of an email address, without the
655 possibility of a "Quoted-String"). Usernames MUST be unique within the domain of the
656 agency, which implies that the combination of Agent and Agency IDs is globally unique.
657 Examples of this are "tom.jones@psap.allegheny.pa.us" and "tjones.atroop@state.vt.us".

658 **2.1.3 Element Identifier**

659 A logical name used to represent physical implementation of a functional element or set of
660 functional elements as a single addressable unit (Section 2.11). The external interfaces of
661 the element MUST adhere to the standards in this document. Elements are addressable via
662 an FQDN that MUST be globally unique. An example of an Element Identifier is
663 "esrp1.state.pa.us". Element Identifiers represent one instance of a replicated functional
664 element when redundant instances of a function are provided for reliability.

665 **2.1.4 URN Emergency Namespace**

666 This document uses the "emergency" Namespace Identifier (NID) for Uniform Resource
667 Name (URN) resources. Use of the "nena" NID is retained for backwards compatibility
668 when used with v2 interfaces, but v3 interfaces MUST use the "emergency" NID. The
669 lexical equivalence is the same as defined in *URN Syntax* (RFC 2141) [112]. Unless
670 otherwise specified, all FEs MUST treat these URNs as case insensitive when doing

671 comparisons in order to follow the lexical equivalency rules of *A Uniform Resource Name*
672 (*URN*) for Emergency and Other Well-Known Services (RFC 5031) [45].

673 **2.1.5 Services**

674 A set of functional element instances that provide the basic capabilities described in this
675 document is called a Service. Services defined in this document are known by a Service
676 Name which comes from the Service Name registry (Section 10.11).

677 A service can be implemented in one or more elements, and indeed for redundancy
678 purposes, nearly every service SHOULD be implemented by multiple elements. Regardless,
679 the external interfaces of the service MUST adhere to the standards in this document. A
680 Service Identifier refers to the collection of elements that define a service within an NGCS.
681 Service Identifiers are Fully Qualified Domain Names (FQDNs). An example of a Service
682 Identifier is "foo.allegheny.pa.us". The Service Name is not required to be part of the
683 FQDN.

684 **2.1.6 Call Identifier**

685 The term "call" is defined in Document Terminology and includes voice calls, video calls,
686 text calls, and non-interactive calls. The first element in the first ESInet/NGCS that handles
687 a call assigns the Call Identifier. The form of a Call Identifier is a Uniform Resource Name
688 (URN) (RFC 2141) [112] formed by the prefix "urn:emergency:uid:callid:", a unique string
689 containing alpha and/or numeric characters, the ":" character, and the Element Identifier of
690 the element that first handled the call. For example,

691 "urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us" is a properly formatted Call
692 Identifier. The unique string portion of the Call Identifier MUST be unique for each call the
693 element handles over time. The length of the unique string portion of the Call Identifier
694 MUST be a string of 10 to 32 characters. One way to create this unique string is to use a
695 timestamp with a suffix that differentiates multiple calls if they could be created by the
696 element in the same instant. Implementations using multiple physical devices to implement
697 a redundant element MAY need an additional component to guarantee uniqueness. The
698 Call Identifier is added to a Session Initiation Protocol (SIP) message using a Call-Info
699 header field with a purpose of "emergency-CallId". For example:

700 Call-Info: <urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us>;
701 purpose=emergency-CallId

702 Every call, including non-emergency calls, MUST have a unique Call Identifier.

703 **2.1.7 Incident Tracking Identifier**

704 A real-world event such as a heart attack, car crash, or a building fire for which one or
705 more calls may be received is an Incident. Examples include a traffic accident (including

706 subsequent secondary crashes), a hazardous material spill, etc. Multiple Calls MAY be
707 associated with an Incident. An Incident MAY include other Incidents in a hierarchical
708 fashion. The form of an Incident Tracking Identifier is a URN formed by the prefix
709 "urn:emergency:uid:incidentid:", a unique string containing alpha and/or numeric
710 characters, the ":" character, and the Element Identifier of the entity that first declared the
711 incident. For example, "urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us" is a
712 properly formatted Incident Tracking Identifier. The string MUST be unique for each
713 Incident the element handles over time. The length of the unique string portion of the
714 Incident Tracking Identifier MUST be a string of 10 to 32 characters. One way to create this
715 unique string is to use a timestamp with a suffix that differentiates multiple Incidents if
716 they could be created by an element in the same instant. Implementations using multiple
717 physical devices to implement a redundant element MAY need an additional component to
718 guarantee uniqueness. Incident Tracking Identifiers are globally unique. By definition, there
719 is an Incident associated with every emergency call. As a practical matter, there is at least
720 one call associated with every Incident, except those incidents declared by an agent (such
721 as a police officer observing a traffic incident). The Incident Tracking Identifier is locally
722 generated and assigned by an LNG, LSRG, or the first element in the first ESInet/NGCS
723 that handles an emergency call or declares an incident. Incident Tracking Identifiers MAY
724 be assigned to a call prior to determining the real-world incident to which it actually
725 belongs. (See Section 4.2.2.2). The Incident Tracking Identifier MUST be added to a SIP
726 message using a Call-Info header field with a purpose of "emergency-InstanceId". For
727 example:

728 Call-Info: <urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us>;
729 purpose=emergency-InstanceId

730 **2.1.8 LogEvent Identifier**

731 Each Logging Service MUST assign a globally unique identifier to each LogEvent. The form
732 of a LogEvent Identifier is a URI consisting of the string "urn:emergency:uid:logid:", a
733 unique string, the ":" character, and the FQDN of the Logging Service. The unique string
734 MUST be 10 to 36 characters long and unique to the Logging Service. An example
735 LogEvent Identifier is "urn:emergency:uid:logid:0013344556677-231:logger.state.pa.us".
736 The FQDN specified MUST be the domain of the Logging Service to which a corresponding
737 RetrieveLogEvent request can be sent to access the LogEvent.

738 **2.1.9 Queue Identifier**

739 The Queue Identifier, which is represented by a URI, MUST have the domain part of the
740 URI set to the domain in which the queue (the destination for calls) resides (ESRP or PSAP,
741 for example). An example of a PSAP URI is normalCalls@psap.allegeny.pa.us.

[MM/DD/YYYY]

Page 24 of 675



742 **2.1.10 Secure Telephone Identity**

743 The Secure Telephone Identity is defined as the identity provided in a SIP Identity header
744 field, constructed and formatted as per RFC 8224 [60]. When present, it is used to validate
745 the identity of the calling party.

746 **2.2 Time**

747 It is essential that all elements on the ESInet/NGCS have the same notion of time. To do
748 so, every element MUST implement Network Time Protocol (NTP) (RFC 5905) [216], and
749 access to a hardware clock MUST be provided in each ESInet/NGCS such that the absolute
750 time difference between any element on any ESInet/NGCS and another element in the
751 same or any other ESInet/NGCS is maintained within one tenth of a second³ of one
752 another. (See Section 4.17).

753 **2.3 Timestamp**

754 Any record that must be marked as to when it occurred (especially a log record, see
755 Section 4.12) includes a Timestamp. A Timestamp includes integer-valued year, month,
756 day, hour, minute, seconds, a decimal seconds value, and a timezone offset value. Time
757 MUST include seconds, and, if two or more Timestamps could be generated by the same
758 element within one second when the order of events matters, the seconds element MUST
759 include sufficient decimal places in the seconds field to differentiate the Timestamps.
760 Except when otherwise dictated by standards, all time within the ESInet/NGCS is
761 represented as local time with offset from Universal Coordinated Time (UTC). The offset
762 MUST be based on the local time of the creator. The offset is a REQUIRED component of
763 the Timestamp and consists of an integer number of hours and minutes.

764 Timestamps contained in JavaScript Object Notation (JSON) objects governed by this
765 specification SHALL be represented by the “date-time” datatype described in RFC 3339,
766 Section 5.6 [135], and SHALL be indicated in schema definitions accordingly. An example
767 of a Timestamp in this format is “2015-08-21T12:58:03.01-05:00”.

768 **2.4 Events Common to Multiple Functional Elements**

769 Events are described in Section 3.1.3.2. The following events MAY be implemented in any
770 functional element. Also see the Logging Service interface in Section 4.12, which is
771 implemented by any element that handles a call.

³ Some implementations MAY require more time accuracy than this specification within a domain such as an ESInet/NGCS.

772 **2.4.1 Element State**

773 The elementState event package provides the state of an element either determined
774 automatically or as determined by management. A registry (ElementState) of allowed
775 values is defined (see Section 10.13).

776 In addition, if the subscriber to an element is unable to contact that element, it MUST
777 assume the state of the element is "Unreachable".

778 A physical or virtual implementation that is separately addressable or differentiable
779 between other entities of the same type MUST implement elementState.

780 **Event Package Name:** emergency-ElementState

781 **Event Package Parameters: None**

782 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions filter specification MAY be
783 present

784 **Subscription Duration:** Default is one (1) hour. One (1) minute to 24 hours is
785 reasonable.

786 **NOTIFY Bodies:** MIME type Application/EmergencyCallData.ElementState+json

Name	Condition	Description
elementId	MANDATORY	Element identifier
state	MANDATORY	Enumeration of current state from Internet Assigned Numbers Authority (IANA) ElementState registry
reason	OPTIONAL	Text containing the reason state was changed, if available

787 **Notifier Processing of SUBSCRIBE Requests**

788 The notifier consults the policy (elementState) specifying the Element Identifier as the
789 target to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not
790 acceptable. If the request is acceptable, it returns 200 OK. Notifiers MUST implement event
791 rate filters as described in RFC 6446 [80].

792 **Notifier Generation of NOTIFY Requests**

793 When the state of the element changes, a new NOTIFY request is generated, adhering to
794 the filter requests. Filter requests MAY specify a minimum notification interval. The element

[MM/DD/YYYY]

Page 26 of 675



795 MUST generate a NOTIFY meeting this filter, if specified. This can be used as a watchdog
796 mechanism.

797 **Subscriber Processing of NOTIFY Requests**

798 No specific action required.

799 **Handling of Forked Requests**

800 Forking between elements MUST NOT be used.

801 **Rate of Notification**

802 State normally does not change often. Changes MAY occur every few seconds if the
803 network or systems are unstable. A minimal rate should be used to ascertain a subscription
804 is still valid.

805 **State Agents**

806 No special handling is required.

807 **2.4.2 Service State**

808 The serviceState event indicates the state of a service either automatically determined, or
809 as determined by management. It encompasses the state of the designated service,
810 inclusive of its security posture when supported. The Request-URI of the SUBSCRIBE
811 specifies the Service Identifier of the target Service.

812 Two IANA registries of allowed values are defined, one for "serviceState" (see Section
813 10.12) and one for "securityPosture" (see Section 10.18).

814 In addition, if the subscriber to a service is unable to contact that service, it MUST assume
815 the state of the service is "Unreachable".

816 Note that one or more elements MAY implement one or more service(s). Each addressable
817 element would have its own element state; each service would have an independent
818 service state.

819 **Event Package Name:** emergency-ServiceState

820 **Event Package Parameters:** None

821 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions filter specification MAY be
822 present

823 **Subscription Duration:** Default 1 hour. 1 minute to 24 hours is reasonable.

824 **NOTIFY Bodies:** MIME type Application/EmergencyCallData.ServiceState+json

[MM/DD/YYYY]

Page 27 of 675



Name	Condition	Description
service	MANDATORY	Service subscribed to
name	MANDATORY	Name of the service. Enumeration of current service name from the IANA service registry
serviceId	MANDATORY	Service Identifier
serviceState	MANDATORY	
state	MANDATORY	Enumeration of current state from the IANA serviceState registry
reason	MANDATORY	Text containing the reason state was changed, if available. Otherwise, empty
securityPosture	CONDITIONAL If the service maintains Security Posture, the field MUST be present. Otherwise, it is omitted.	
posture	MANDATORY	Mandatory if the securityPosture field is present. Enumeration of current security posture from the IANA securityPosture registry
reason	OPTIONAL	Text containing the reason posture changed, if available. Otherwise, empty.

825 Notifier Processing of SUBSCRIBE Requests

826 The notifier consults the policy (serviceState) specifying the ServiceIdentifier as the target to determine if the requester is permitted to subscribe. It returns 603 (Decline) if not acceptable. If the request is acceptable, it returns 200 OK. Notifiers MUST implement event rate filters, RFC 6446 [80].

830 Notifier Generation of NOTIFY Requests

[MM/DD/YYYY]

Page 28 of 675



831 When the state of the service changes, a new NOTIFY request is generated, adhering to
832 the filter requests. Filter requests MAY specify a minimum notification interval. The element
833 MUST generate a NOTIFY meeting this filter, if specified. This can be used as a watchdog
834 mechanism.

835 **Subscriber Processing of NOTIFY Requests**

836 No specific action required.

837 **Handling of Forked Requests**

838 Forking between elements MUST NOT be used.

839 **Rate of Notification**

840 State normally does not change often. Changes MAY occur every few seconds if the
841 network or systems are unstable.

842 **State Agents**

843 No special handling is required.

844 **2.5 Location Representation**

845 Location in NG9-1-1 is represented by content in a PIDF-LO⁴ document (RFC 4119 [6],
846 updated by RFC 5139 [53] and RFC 5491 [52]) with field use for the United States as
847 documented in the NENA Civic Location Data eXchange Format (CLDXF) [77]. An
848 equivalent definition for Canadian addresses will be referenced in a future version of this
849 document. Fields in the PIDF-LO must be used as defined; no local variation is permitted. A
850 function (PIDFLOtoMSAG) is provided as part of the MSAG Conversion Service (See Section
851 4.4) for translating PIDF-LO to a NENA-standard MSAG representation for backwards
852 compatibility. Geodetic location MUST be one of the shape listed in [69]. All geodetic data
853 in i3 uses WGS84 as the datum.

854 A PIDF-LO has an element called “retransmission-allowed”, which, when missing or set to
855 false, is meant to prohibit forwarding of the PIDF-LO. Handling of location when processing
856 an emergency call is controlled by law, and NG9-1-1 FEs normally would ignore
857 retransmission-allowed within the ESInet/NGCS for such calls. There are circumstances in
858 which data about an emergency call may be sent to entities not covered by existing law. In
859 those circumstances it is desirable that NG9-1-1 FEs honor the privacy wishes of the sender

⁴ In the IETF, location information (Location Object) is a subset of Presence information (Presence Information Data Format): PIDF-LO. While NG9-1-1 uses PIDF and the IETF mechanisms that are described in the Presence service, no other parts of Presence are used in emergency calls although Presence may be used in other parts of NG9-1-1.

860 as expressed in the retransmission-allowed field. FEs SHOULD honor the "retransmission-
861 allowed" element of the PIDF-LO when laws do not specify privacy is suspended. When
862 laws suspend privacy, FEs SHOULD send location regardless of the value of the
863 "retransmission-allowed" element. When handling non-emergency calls, retransmission-
864 allowed SHOULD be honored.

865 An entity conforming to this specification that supplies a PIDF-LO for an emergency call
866 MUST use the <provided-by> element to convey its Data Provider Additional Data block, as
867 specified in RFC 7852 [107] Section 4.1. Note that the PIDF-LO supplier's Data Provider
868 block MUST also be conveyed using a Call-Info header field as described in sections 3.1.15
869 and 4.11, unless the supplier is not in the call path. The <provided-by> element MUST
870 NOT be used to convey any other Additional Data blocks. The "dataProvider" schema [ref3]
871 of the "pidf:geopriv10:dataProvider namespace" [ref4] MUST NOT be used. It is
872 RECOMMENDED that the Data Provider Additional Data block be conveyed by value rather
873 than by reference, to avoid an additional operation to obtain the data.

874 **2.6 xCard/jCard**

875 In many interfaces defined in this and related NG9-1-1 documents, a common need is to
876 provide contact information. For example, in some blocks of Additional Data and in
877 Service/Agency Locator, the identity and contact information is part of the data structure.
878 When contact data is needed, i3 specifies the use of an xCard in eXtensible Markup
879 Language (XML) format per RFC 6351 [113] where the interface must be XML, and a jCard
880 as defined in RFC 7095 [215] when the interface is JSON.

881 **2.7 Emergency Services IP Networks**

882 ESInets are private, managed, and routed IP networks. An ESInet serves a set of PSAPs, a
883 region, a state/province, or a set of states/provinces. ESInets are interconnected to
884 neighboring ESInets so that traffic can be routed from any point in the ESInet to any point
885 in any other ESInet. States/Provinces MAY have a backbone ESInet either directly
886 connecting to all PSAPs in the state/province, or interconnected to all county/parish or
887 regional ESInets. Neighboring states/provinces or regions SHOULD interconnect their
888 ESInets. It is desirable to have a backbone national ESInet in each country to optimize
889 routing of traffic between distant ESInets. Each PSAP MUST be connected to an ESInet,
890 possibly through a Legacy PSAP Gateway.

891 ESInets MUST accept and route IPv4 and IPv6 packets. All services MUST support IPv4 and
892 IPv6 interfaces. IPv6 is RECOMMENDED for use throughout the ESInet, but cannot be
893 assumed. Within this document there are several interfaces that may require a text
894 representation of an IPv6 address, including in the specification of addresses for media in
895 the Session Description Protocol (SDP). In such interfaces the canonical representation

896 specified in RFC 5952 [196] MUST be used, including the use of brackets when specifying a
897 port number. Note that originating networks are outside the scope of this document and
898 they may not follow RFC 5952 conventions.

899 ESInets MUST be accessible from the global Internet, with calls going through the Border
900 Control Function (BCF). This Internet interconnect is RECOMMENDED at the state ESInet
901 level with local or regional ESInets getting Internet connectivity via the state ESInet.
902 Originating networks SHOULD be connected to any ESInet to which they regularly deliver
903 volume traffic via a private connection through the BCF of that ESInet.

904 An ESInet MUST be capable of withstanding the largest feasible Distributed Denial of
905 Service (DDoS)/Telephone Denial of Service (TDoS) attack. As of this version, that means
906 approximately at least a terabit of mitigation. Network and BCF bandwidth as well as
907 mitigation services may be used to achieve this requirement. DDoS/TDoS mitigation
908 typically requires that traffic be rerouted to a mitigation service. Private connections MUST
909 be able to be so re-routed if mitigation is needed. Connection through the Internet is
910 acceptable, PREFERABLY through a Virtual Private Network (VPN) with the same mitigation
911 caveat.

912 **Note:** The effect on emergency calls already in progress when mitigation is enabled will be
913 addressed in a future version of this document.

914 Access to ESInets MUST be controlled. Only public safety agencies and their service
915 providers may be connected directly to the ESInet. Call origination sources, gateways, and
916 similar elements are outside the ESInet and interconnected through the BCF. However, for
917 security reasons, the ESInet SHOULD NOT be assumed to be a "walled garden."

918 For Quality of Service (QoS) reasons, IP traffic within an ESInet MUST implement DiffServ
919 (RFC 2474 [218] and 2475 [134]). Differentiated Service Code Points (DSCPs) within the
920 ESInet are drawn from pool 2, with the exception of DSCP value "0000 00" which is the
921 default from Pool 1. Routers MUST respect code points: Functional Elements MUST mark
922 packets they create with appropriate code points. The ESInet edge router MUST perform
923 traffic conditioning for packets entering the ESInet. The following code points MUST be
924 used, so that packets transiting more than one ESInet can receive appropriate treatment.
925 The following Per Hop Behaviors (PHB) on ESInets are RECOMMENDED starting points and
926 MAY be changed based on operational experience:

927 This table specifies ESInet-specific traffic. Other traffic (e.g., DHCP, ICMP, BGP, etc.)
928 should be marked according to industry standards and best practices.

DSCP	Use	PHB
0000 00	Routine Traffic except as specified below	Default (Best Effort)

[MM/DD/YYYY]

Page 31 of 675



DSCP	Use	PHB
0000 11	9-1-1 Call (SIP) Signaling (including non-interactive calls) and emergency call related HTTP/S operations, DNS traffic	AF12
0001 11	9-1-1 Text Media (RTT and MSRP)	AF12
0010 11	9-1-1 Audio Media (9-1-1 Calls and admin calls)	EF
0011 11	9-1-1 Video Media	AF11

929 Interconnected ESInets represent a DS Region as defined in RFC 2475 [134] and connect
930 to other networks which are distinct DS Regions. The ESInet edge routers SHOULD re-mark
931 code points between the interconnected networks and the ESInet to match the traffic
932 classes ("Use") above as closely as possible, within the terms of any interconnect
933 agreements with such networks. An interconnected network might perform the re-marking
934 at its edge routers, in which case the ESInet edge router's re-marking is a null operation.

935 All elements in an ESInet SHOULD have a publicly addressable IP address. Network
936 Address Translations (NATs) SHOULD NOT be used within an ESInet. Although NAT use
937 within an ESInet is NOT RECOMMENDED, NATs may be needed in specific deployments,
938 and therefore all network elements MUST operate in the presence of NATs.

939 It is RECOMMENDED that elements connected to the ESInet not be referred to by their IP
940 address but rather through a hostname using DNS. Use of statically assigned IP addresses
941 SHOULD be limited, and SHOULD NOT be used with IPv6 addresses. Dynamic Host
942 Configuration Protocol (DHCP) (RFC 2131) [147] or Dynamic Host Configuration Protocol
943 for IPv6 (DHCPv6, RFC 8415 [233]) must be implemented on all network elements to
944 obtain IP address, gateway, and other services.

945 There SHALL NOT be any single point of failure for any critical service or function hosted
946 on the ESInet. Certain services designated as non-critical may be exempt from this
947 requirement. These MUST NOT include the BCF, internal ECRF, ESRP, Logging Service, and
948 security services. Services MUST be deployed to survive disasters, deliberate attacks, and
949 massive failures.

950 **2.8 Service Interfaces**

951 In this document, we make use of three kinds of interfaces:

- 952 • Web Services, typically using a Simple Object Access Protocol (SOAP) [148] interface
953 or using Representational State Transfer (REST),
- 954 • Simple HyperText Transfer Protocol Secure (HTTPS) (RFC 2818) [153] GET (and in
955 some cases, POST) with retrieval of JSON data structures based on a Uniform
956 Resource Identifier (URI), and
- 957 • SIP interfaces, including SIP Subscribe/Notify.

[MM/DD/YYYY]

Page 32 of 675



958 The term “web service”, when it appears in this document, unless otherwise specified as an
959 IETF-defined XML interface, means a REST interface using JavaScript Object Notation
960 (JSON) defined by a NENA-provided Open API 3.0 YAML (YAML Ain’t Markup Language) file
961 (Appendix E.).

962 The interface point for web services MUST be the server line of the YAML file, with the
963 Service Identifier of the appropriate service substituted for “localhost”.

964 The YAML file in Appendix E represents the normative definition of the interface; if there
965 are any discrepancies between the YAML file in the repository and the YAML file in the text
966 (Appendix E), the YAML file in the repository is authoritative.

967 **2.8.1 HTTP Transport**

968 i3 Services which use HTTP MUST support HTTP over TLS (HTTPS) (RFC 2818) [57]. The
969 services, unless specified otherwise, MUST support HTTP/1.1 (RFC 7230) [162] and
970 SHOULD support HTTP/2.0 (RFC 7540) [197]. Clients and servers MUST support TLS 1.2
971 [199], MAY support TLS 1.3 [200] or greater and MUST NOT offer or accept TLS 1.1 or TLS
972 1.0. Perfect forward secrecy MUST be used within the ESInet.

973 **2.8.2 Status Codes**

974 Each entry point lists status codes that are returned for expected situations. (For example,
975 Section 4.12.3.1.1 LogEvent response includes the codes 200 OK, 434 Signature
976 Verification Failure, and 463 LogEvent extension on disallowed list, as well as other codes.)
977 In some cases, an IANA-registered [222] status code is used (e.g., 200 OK in the above),
978 while in other cases, custom status codes are used (e.g., 434 Signature Verification Failure
979 and 463 LogEvent extension on disallowed list in the above). If a server encounters a
980 situation not listed, the most appropriate IANA-registered status code SHOULD be used (for
981 example, 500 Internal Server Error for a server fault or 507 Insufficient Storage if a server
982 is unable to store a resource).

983 Clients MUST appropriately handle all status codes listed for each supported entry point,
984 and MUST react appropriately to other status codes received, based on the first digit as per
985 RFC 7231 [223] Section 6.

986 **2.8.3 Versions**

987 Each web service has a version. A version consists of a major version and a minor version,
988 both integers. Versions are commonly expressed as a string with a period between the
989 major and minor version integers (e.g., "3.2"). The integer before the period represents
990 the major version, and the integer after the period represent the minor version. Any
991 change to the YAML file will change the version. If a set of changes to the YAML file is

992 backwards compatible, the minor version is incremented. If any of a set of changes to the
993 YAML file is not backwards compatible, the major version is incremented, and the minor
994 version reset to zero. Implementations MUST ignore elements of data structures they do
995 not understand and MUST return 404 errors to entry points to the web interfaces they
996 don't provide as a server. If a minor version introduces a backwards compatible change
997 that is not accommodated by existing implementations of the same major version solely by
998 ignoring elements it doesn't understand and returning 404 errors for entry points it doesn't
999 understand, the document describing the new minor version MUST describe precisely how
1000 implementations of that and succeeding minor versions accommodate prior minor versions.
1001 Other NENA standards MAY specify changes to the interface, and thus the version.
1002 Changes that are not backwards-compatible changes SHOULD only be made in future
1003 version of this document.

1004 Each Web Service MUST implement an entry point called "Versions". For example, the
1005 PolicyStore web service implements .../PolicyStore/Versions. Clients of Web Services MUST
1006 make an HTTPS GET request using the URI of the service's Versions entry point. The GET
1007 does not have any parameters. The server sends a response containing a data structure to
1008 inform the client which versions the server supports. The "Versions" entry point returns the
1009 following parameters:

Name	Condition	Description
fingerprint	MANDATORY	Vendor Info
versions	MANDATORY	One entry for each version supported at the server

1010 Status Codes
1011 200 OK Version information returned

1012 "versions" contains an array of objects, each consisting of:

Name	Condition	Description
major	Mandatory	Major version number
minor	Mandatory	Minor version number
vendor	Optional	Vendor extensions
serviceInfo	Conditional: required for services that specify this parameter, omitted for all others	Service-specific information. Some web services return additional service-specific information; for such services, this parameter is present and contains additional parameters as specified for the service; for services that do not specify the use of this parameter, it is omitted.

1013 The "vendor" string is not defined in this version of the document but is intended to
1014 indicate which vendor extensions the implementation supports.

[MM/DD/YYYY]

Page 34 of 675



1015 The “fingerprint” string is intended to contain a unique string for a particular code set (e.g.,
1016 a build identifier). The string is logged (in the “VersionsEvent” LogEvent) for debugging
1017 purposes but is otherwise not used.

1018 The Versions entry point MAY be used as a keep-alive mechanism for a service. Successful
1019 queries for this purpose SHOULD NOT be logged by the client. When a change in version is
1020 detected, however, this SHOULD be logged by the client.

1021 Note that the information returned by the Versions entry point can be different for different
1022 Web Services even if the IP addresses of the servers are the same, and that version
1023 information can change between requests (e.g., a server could fail-over).

1024 For example, assuming a hypothetical Web Service “Tantrums” that specifies a
1025 “maxScreamVolume” parameter in serviceInfo, an HTTPS GET request on
1026 .../Tantrums/Versions” returns a body containing a JSON data object similar to the
1027 following:

```
1028 {  
1029     "fingerprint": "Woof-FurrySuite-v8-8c439e",  
1030     "versions":  
1031         [  
1032             { "major": 6, "minor": 3,  
1033                 "vendor": "burby-magic",  
1034                 "serviceInfo": { "maxScreamVolume": 11 }  
1035             }  
1036         ]  
1037     }  
1038 }
```

1038 **2.9 Redundancy**

1039 Many methods are available to implementers to create reliable implementations. Some
1040 methods require clients to be aware of the redundancy model of the server in order to
1041 achieve the desired reliability model. Interoperability is affected if there is a mismatch in
1042 what the client assumes and what the server (or peer) assumes with respect to
1043 redundancy.

1044 The i3 architecture provides support for one model in which clients expressly support two
1045 (or optionally more) servers in an active-active (multi-master) configuration. Each client
1046 must be prepared to send its transactions to one of two (or optionally more) servers. One
1047 interface is considered “primary” with “secondary” interface(s) available to be used at any
1048 time by any client. Deployment of this mechanism is not a requirement.

1049 Servers may implement other models as long as it is transparent to the client. If the server
1050 has a redundancy model that hides redundancy from the client, only the primary interfaces
1051 would be used. This model does not support an active/standby failover paradigm – it is
1052 active-active. The burden of maintaining consistency of transactions when replicated

1053 databases are used rests on the server. Clients MUST retry transactions on redundant
1054 elements that that could not be completed on the initial element.
1055 Every implementation MUST be capable of using a DNS based implementation of redundant
1056 elements where more than one address may be returned for the URI provided.
1057 Implementations MUST be capable of preferring the first returned address, and using the
1058 second, third and optionally additional addresses returned as representing redundant
1059 elements for the service. Other mechanisms to achieve redundancy MAY be provided, but
1060 the DNS based mechanism MUST be supported by all services and clients of those services.
1061 Examples of how an active-active architecture is implemented at the server are beyond the
1062 scope of this document.

1063 **2.10 Telephone Numbers**

1064 When telephone numbers are used within the NGCS, full E.164 [120] numbers may be
1065 encountered on any call and all elements MUST be able to handle a full E.164 telephone
1066 number. Ten-digit numbers conforming to the North American Numbering Plan (NANP)
1067 may be assumed to be North American telephone numbers and telephone numbers that
1068 are not full E.164 numbers but contain a digit string with greater than 10 digits may be
1069 assumed to be non-North American telephone numbers, but missing the "+" prefix. Some
1070 systems may have more sophisticated methods of determining a full E.164 number from a
1071 digit sequence appearing in the signaling. Telephone numbers conveyed as part of a URI
1072 MUST be designated as such either by using a tel URI (RFC 3966) [150] or in a SIP URI
1073 using the user=phone parameter. SIP elements MUST conform to RFC 3824 [29]

1074 **2.11 Functional Elements**

1075 This document describes many functional elements. An implementation MAY combine any
1076 set of functional elements into a physical realization, provided that the assembly of
1077 functional elements provides all of the required functionality specified in this standard, as
1078 well as the external interfaces that the set of elements offer to other ESInet/NGCS
1079 elements. Interfaces between the FEs within a physical realization do not have to conform
1080 to the interfaces described in this document, provided that the set of elements behaves as
1081 if those interfaces conformed to this document.

1082 **3 Interfaces**

1083 This section describes the major interfaces used in NG9-1-1. Not every interface is
1084 described in this section; some of the web interfaces, for example, the Additional Data
1085 dereferencing interfaces, are described in other documents or in other sections of this
1086 document.

[MM/DD/YYYY]

Page 36 of 675



1087 **3.1 SIP Call**

1088 The i3 call interface is SIP (RFC 3261) [10]. All calls presented to the NGCS MUST be SIP
1089 signaled. Calls are potentially multimedia, and can include one or more forms of media
1090 (audio, video, and/or text⁵). See Section 3.1.11 for a discussion of “non-interactive calls”
1091 (also called “data-only emergency calls”) which are used for requests for help when there
1092 is no human caller. SIP MUST also be the protocol used to call a 9-1-1 caller back, and is
1093 the protocol for calls between agents within the ESInet.

1094 SIP is a complex protocol defined in a large number of standards documents. All NG9-1-1
1095 elements which process calls MUST implement all of the standards listed in Section 3 (Core
1096 Standards) of the "Hitchhiker's Guide to SIP" (RFC 5411) [9], and RFC 4320 [36].
1097 Implementations are cautioned to be "strict in what you send, and liberal in what you
1098 accept" with respect to such standards. It is generally unacceptable to drop a 9-1-1 call
1099 just because it doesn't meet some standard detail if it's reasonably possible to process the
1100 call anyway. This section does not describe a change to any normative text in any IETF
1101 standards-track document. If there is any conflict between this document and the IETF
1102 document concerning how the SIP protocol works, the IETF document is authoritative.
1103 Many elements of SIP have options, and this document may restrict an implementation's
1104 use of such options within an ESInet.

1105 **Note:** There are some conflicts between some of the documents mentioned in RFC 5411
1106 and this document. This will be addressed in a future version of this document.

1107 There are three primary entities in a SIP protocol exchange:

- 1108 1. The User Agent Client (UAC), which is the initiator of a “transaction” within SIP. In
1109 the origination of a 9-1-1 call, the calling party's end device could be the UAC.
- 1110 2. The User Agent Server (UAS), which is the target of a transaction within SIP. In the
1111 origination of a 9-1-1 call, the call taker's end device could be the UAS.
- 1112 3. A Proxy Server, which is an intermediary that assists in the routing of a call. Proxy
1113 servers are in the signaling path of a call, but not in the media path. A call may
1114 traverse several proxies. In a typical 9-1-1 call, the calling party's originating
1115 network may have two or more proxies. The NGCS has at least one proxy (an
1116 Emergency Service Routing Proxy) and typically has more than one.

1117 In addition, some implementations may make use of a Back-to-Back User Agent (B2BUA)
1118 which is an interconnected UAC and UAS.

⁵ All ESInet elements support all forms of media described in this document. Any given originating network or device may not support all media types, and support of specific media types by originating networks and devices may be subject to regulation.

1119 SIP message exchanges are defined in transactions, which are explicit sequences of
1120 messages. The transaction is named by the "method" in the SIP message that starts the
1121 transaction. For example, the SIP transaction that creates a call (termed a "session" in SIP)
1122 is the INVITE transaction.

1123 In this document, we use the terms "diversion" and "retarget" to mean that a call is sent to
1124 a PSAP other than the nominal PSAP, normally due to unusual conditions at the nominal
1125 PSAP. In SIP, these terms are used for behaviors with strict definitions that generally
1126 involve a change in the Request-URI. However, because emergency calls maintain a service
1127 urn in the Request-URI, changes in the destination are accomplished via the Route header.

1128 Forking between elements MUST NOT be used.

1129 Emergency call handling relies on the Service URN in the Request-URI being preserved. To
1130 avoid the Request-URI being rewritten, this document assumes loose routing (as defined in
1131 RFC 3261 [10]) is used for all SIP Calls end-to-end. Per RFC 3261, the "lr" parameter
1132 should be present in URIs used for routing. A future version of this document will
1133 normatively require this behavior.

1134 Complete emergency call examples are presented in Appendix D.

1135 **3.1.1 Minimal Methods needed to handle a call**

1136 The only SIP methods absolutely REQUIRED to handle a 9-1-1 call are the INVITE (for
1137 interactive calls) or MESSAGE (for non-interactive calls). The REFER method (defined in
1138 RFC 3515 [19]) MUST also be supported in order to conference and transfer calls. Call
1139 takers (and thus bridges that they may use) MUST be able to generate the BYE transaction
1140 to terminate the call.

1141 NG9-1-1 elements that process 9-1-1 calls MUST accept calls that do not strictly follow the
1142 SIP standards. As long as the messages can be parsed, and the method discerned, at least
1143 the first SIP element (the BCF) MUST be able to accept the call and forward the call
1144 onward (see Section 4.1), possibly rewriting non-conforming signaling messages. There are
1145 security concerns with accepting non-conforming calls; the BCF MAY reject calls that
1146 appear to be security risks.

1147 Support for the following SIP Methods is summarized and specified in the following table:

SIP Method	Mandatory/Must Not/ Conditional/Optional
INVITE	MANDATORY
REFER	MANDATORY
BYE	MANDATORY
CANCEL	MANDATORY
UPDATE	MANDATORY

SIP Method	Mandatory/Must Not/ Conditional/Optional
OPTIONS	MANDATORY
ACK	MANDATORY
PRACK	MANDATORY
MESSAGE	MANDATORY
INFO	MANDATORY (But must not be used to convey DTMF digits)
REGISTER	MUST NOT
SUBSCRIBE/NOTIFY	MANDATORY
PUBLISH	OPTIONAL

1148 **3.1.1.1 INVITE (initial call)**

1149 The INVITE method is used to initiate an interactive call. The standard INVITE/200 OK/ACK
1150 sequence MUST be followed, with allowance for provisional (1XX) responses.

1151 An emergency call has a Route header field containing next-hop data obtained from the
1152 ECRF (which should be augmented with the "lr" parameter to avoid Request-URI)
1153 rewriting based on the location of the call, and a Request-URI containing a Service URN.
1154 Nominally, the Service URN SHOULD be "urn:service:sos" or a subservice. In most
1155 jurisdictions, subservices such as "urn:service:sos.police", "urn:service:sos.fire" and
1156 "urn:service:sos.ambulance" appearing on a call presented to the Next Generation 9-1-1
1157 Core Services (NGCS) are routed as they would be without the subservice.

1158 The external (i.e., facing outside the ESInet/NGCS) ECRF returns a "PSAP URI" which is
1159 contained in the Route header field (which should be augmented with the "lr" parameter to
1160 avoid Request-URI rewriting) when the call enters the ESInet/NGCS. The content of this
1161 URI can vary depending on the policy of the 9-1-1 Authority. One strategy is simply to use
1162 a general URI that leads to a state level ESRP, for example "911@sos.tx.us". The state
1163 ESRP queries the internal ECRF (within the ESInet/NGCS) with the service URN found in
1164 the PRF policy for the incoming call, for example "urn:emergency:service:sos.psap", and
1165 receives the next hop route for the call. Alternatively, the external ECRF could return a
1166 more specific URI, for example, "harris.county@sos.tx.us". This URI still routes to the same
1167 state-level ESRP, which performs the same ECRF query. However, failures at the state
1168 ESRP (for example, a failure to obtain a route from the ECRF) may be able to be mitigated
1169 by using the information in the Route header field.

1170 Every call received by the NGCS gets some form of "call treatment". Minimal call
1171 treatments defined include:

- 1172 1. Route call to the PSAP serving the location of the caller
1173 2. Return Busy (600 Busy Everywhere)

[MM/DD/YYYY]

Page 39 of 675



1174 3. Answer at an Interactive Media Response (IMR) system
1175 4. Divert to another PSAP

1176 The ESRP determines, by evaluating PSAP policies, which treatment a call gets.

1177 An i3 PSAP SHOULD normally only return a 180 Ringing provisional response when a 9-1-1
1178 call is queued for answer. 183 Session Progress may be used in some specific
1179 circumstances. It is RECOMMENDED that no other 1XX response be used by the i3 PSAP
1180 due to uneven implementations of these responses. The provisional response SHOULD be
1181 repeated at approximately 3 second intervals if the call is not answered. When placing a
1182 call-back, elements MUST accept any 1XX intermediate response and provide an
1183 appropriate indication to the caller.

1184 The normal response to an answered call is 200 OK.

1185 9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used;
1186 however, 3XX MAY be used for calls initiated within the ESInet/NGCS. If a call is
1187 retargeted, History-Info and Reason header fields MUST be added to the INVITE/MESSAGE
1188 per section 3.1.8. NG9-1-1 elements that initiate calls within the ESInet/NGCS SHOULD
1189 appropriately respond as defined in RFC 3261 [10].

1190 Once a call is established, it may be necessary to modify some of the parameters of the
1191 call. For example, it may be necessary to change the media session parameters. In this
1192 case, an INVITE transaction on an existing session is used. This is termed a "re-INVITE" in
1193 SIP. A re-INVITE MAY be used on any call within the ESInet/NGCS, including a 9-1-1 call. A
1194 re-INVITE MAY be initiated from either end of the call. Note that when the called party
1195 initiates the re-INVITE it becomes the UAC, and the calling party becomes the UAS. A party
1196 MUST be able to accept a re-INVITE which changes the Contact header field. This may
1197 occur in the case of an element failure.

1198 SIP entities MUST support the Dialog Event, RFC4235 [68].

1199 **3.1.1.2 REFER (transfer)**

1200 The REFER method MUST be supported within the ESInet/NGCS for two purposes:

1201 • To transfer a call when the model is ad hoc, see Section 4.9 (transfer models)
1202 • To conference additional parties to a call

1203 REFER is defined in RFC 3515 [19]. The REFER method indicates that the recipient
1204 (identified by the Request-URI) should contact a third party using the contact information
1205 provided in the Refer-To header field of the request. The recipient of the REFER request
1206 sends an INVITE to the URI in the Refer-To header field.

1207 REFER creates an implicit subscription as described in RFC 6665 [14] to a REFER event
1208 package. As with all SIP subscriptions the recipient of the REFER sends an immediate
1209 NOTIFY confirming instantiation of the subscription. When the INVITE is answered or fails,
1210 another NOTIFY is sent with success or failure of the REFER operation.

1211 REFER is sometimes used with the Replaces header field, which is dubbed
1212 "REFER/Replaces". This is used to replace a call leg with another call leg, an example being
1213 replacing a two way call between the caller and call taker with a leg between the caller and
1214 the bridge, with another transaction used to create the leg between the call taker and the
1215 bridge. If an element receives a REFER with Replaces request when the Replaces SIP Call
1216 ID does not exist, it MUST be rejected.

1217 If the calling device supports the Replaces header field, which is signaled by having the
1218 "replaces" value in the Supported header field of the original INVITE, the Replaces header
1219 field can be sent to the calling device in the context of an emergency call transfer when the
1220 model is ad hoc. Section 4.7 discusses the problem of a calling device that is unable to
1221 support a Replaces transaction. Section 4.7.2 discusses blind transfer which uses REFER
1222 without Replaces.

1223 All SIP call processing entities within an NGCS, as well as PSAPs, MUST be able to send a
1224 REFER. Bridges MUST be able to receive a REFER. SIP entities implementing REFER MUST
1225 implement RFC 4508 [38] and the Replaces Header Field, RFC 3891 [27].

1226 **3.1.1.3 BYE (call termination)**

1227 The BYE method is used to terminate a call. BYE may be initiated from either end, unless
1228 the mechanism defined in Appendix C for implementing PSAP control of disconnect is used.

1229 **3.1.2 Methods allowed to be initiated by any UA which MUST be supported by i3 1230 elements**

1231 **3.1.2.1 CANCEL (cancel call initiation)**

1232 An attempt to create a call with INVITE MAY be cancelled before it is completed using the
1233 CANCEL method. CANCEL is used before the session is created (call establishment); BYE is
1234 used after the session is created. Of course, race conditions exist between the signaling of
1235 the session and the attempt to cancel it. These conditions are discussed in RFC 3261 [10].
1236 CANCEL would be the signaling used to abandon a call, and NGCS elements MUST treat a
1237 CANCELled call as such, including logging requirements.

1238 **3.1.2.2 UPDATE (update parameters)**

1239 UPDATE is defined in RFC 3311 [15] and is sometimes used during call establishment if
1240 needed to change the parameters of the call. RFC 3311 states that although UPDATE can

[MM/DD/YYYY]

Page 41 of 675



1241 be used on confirmed dialogs, it is RECOMMENDED that a re-INVITE be used instead.
1242 NGCS elements MUST NOT send UPDATE on a confirmed dialog but MUST accept one.
1243 UPDATE MAY be used on any call within an ESInet/NGCS (including 9-1-1 calls).

1244 **3.1.2.3 OPTIONS (option negotiation)**

1245 OPTIONS MAY be used by an external caller, or inside the ESInet/NGCS to determine the
1246 capabilities of the destination User Agent (UA). All endpoints within the ESInet/NGCS MUST
1247 be capable of responding to an OPTIONS request, as defined in RFC 3261 [10].

1248 Although Session Timers [32] MUST be supported by all SIP entities, an OPTIONS
1249 transaction is the preferred mechanism for maintaining a “keep alive” between two SIP
1250 elements. Periodic OPTIONS transactions MUST be used between ESRPs that normally pass
1251 calls between themselves, between the ESRP and the PSAPs, LNGs and LPGs it normally
1252 serves, and between the PSAP and the bridge it normally uses. The period between
1253 OPTIONS requests used for keep-alive SHOULD be provisioned, and default to one (1)
1254 minute (which MUST be less than the Transport Layer Security (TLS) timeout period)
1255 intervals during periods of inactivity. Since the OPTIONS method requires an exchange of
1256 messages, only one member of a pair of “adjacent” SIP elements needs to initiate an
1257 OPTIONS request towards the other. It is RECOMMENDED that the “upstream” element
1258 initiates the request. A Session Recording Client (SRC) sends OPTIONS requests to its
1259 Session Recording Service (SRS) for keep-alive purposes. Using an OPTIONS request from
1260 outside the ESInet/NGCS is NOT RECOMMENDED to determine if an emergency call would
1261 reach the PSAP. Instead, sparing use of the Test Call (RFC 6881) [46] mechanism is
1262 RECOMMENDED. If OPTIONS is received from an entity outside the ESInet/NGCS, it
1263 SHOULD receive a valid response from some entity inside the ESInet/NGCS. The ESRP
1264 SHOULD route the request to some entity that will respond affirmatively. The path taken by
1265 such a request need not be representative of what an actual or test call would take. The
1266 ESRP itself, if it had some UA capability, SHOULD respond.

1267 **3.1.2.4 ACK (acknowledgement)**

1268 The ACK request is used to acknowledge completion of a request. Strictly speaking, there
1269 are two cases of ACK: one used for a 2XX series response (which is actually part of a
1270 three-way handshake, typically INVITE/200 (OK)/ACK), and a non-2XX response, which is a
1271 separate transaction. All endpoints in an ESInet/NGCS MUST use ACK.

1272 **3.1.2.5 PRACK (reliable message acknowledgement)**

1273 The PRACK method MUST be used within systems that need reliable provisional responses
1274 (non 100). “Provisional” responses are part of the 1XX series responses, except the general
1275 100 (Trying) response. As an example of when an NGCS SIP element may see a PRACK,

1276 see the example in RFC 3311 [15] when PRACK is sent by the UAS to reliably send an SDP
1277 "offer" to a UAC in a 18X response.

1278 **3.1.2.6 MESSAGE (text message)**

1279 The MESSAGE method, an extension to SIP, allows the transfer of Instant Messages and is
1280 also used to carry a Common Alerting Protocol (CAP) message. In NG9-1-1, Message
1281 Session Relay Protocol (MSRP) is used to carry Instant Messages, but the MESSAGE
1282 method is used for non-interactive calls. Since the MESSAGE request is an extension to SIP,
1283 it inherits all the request routing and security features of that protocol. MESSAGE requests
1284 carry the content in the form of Multipurpose Internet Mail Extensions (MIME) body parts.
1285 MESSAGE requests do not themselves initiate a SIP dialog; each Instant Message stands
1286 alone, much like pager messages. While there is no known use case, ESInet elements
1287 MUST allow MESSAGE requests in the context of a dialog initiated by some other SIP
1288 request. For more information on MESSAGE please refer to RFC 3428 [17]. MESSAGE is
1289 part of the SIP/SIMPLE presence and messaging system.

1290 **3.1.2.7 INFO**

1291 The INFO method (RFC 6086) [149] is used for communicating mid-session signaling
1292 information along the signaling path for a call. See Appendix C for details related to the use
1293 of INFO in the context of PSAP call control features. INFO MAY also be used for backwards
1294 compatibility with some video systems that use RFC 5168 [122] to request Intra-frame
1295 refresh (see Section 3.1.9.2). INFO MUST NOT be used to convey DTMF digits.

1296 **3.1.3 Methods used within the ESInet/NGCS**

1297 **3.1.3.1 REGISTER**

1298 Use of REGISTER is not defined in this document, so REGISTER SHALL NOT be used.

1299 **3.1.3.2 SUBSCRIBE/NOTIFY (Events)**

1300 SUBSCRIBE/NOTIFY is a mechanism to implement asynchronous events notification
1301 between two elements. The mechanism is used in i3, for example, to request current state
1302 and updates to state from a remote element, and to obtain location from a SIP location
1303 reference. SUBSCRIBE requests SHOULD contain an "Expires" header field. This "Expires"
1304 value indicates the duration of the subscription. In order to keep subscriptions effective
1305 beyond the duration communicated in the "Expires" header field, subscribers MUST refresh
1306 subscriptions on a periodic basis using a new SUBSCRIBE message on the same dialog. The
1307 subscription also expires in the originating network when the associated SIP dialogue is
1308 terminated with a BYE.

1309 NOTIFY messages are sent to inform subscribers of changes (e.g., in state or location) to
1310 which the subscriber has a subscription. Subscriptions are typically put in place using the
1311 SUBSCRIBE method; however, it is possible for other means to be used. A NOTIFY
1312 message does not terminate its corresponding subscription. A single SUBSCRIBE request
1313 MAY trigger multiple NOTIFY requests.

1314 For further information, refer to RFC 6665 [14] section 8.1. Entities implementing a notifier
1315 MUST implement RFC 3857 [26].

1316 **3.1.3.3 PUBLISH (update of presence information to presence server)**

1317 Use of PUBLISH is not defined in this document.

1318 **3.1.4 Response Codes**

1319 Responses typically encountered in a SIP call SHOULD be handled as follows:

1320 (Only salient response codes are listed. Response codes not listed and not defined in RFC
1321 3261 [10] are not expected to be provided nor received by the NGCS but if present, MAY
1322 be treated as the equivalent X00 error code, or MAY be processed as defined in the
1323 corresponding RFC.)

SIP Response Codes from NGCS	Description
180 (Ringing)	A 9-1-1 call is queued for answer. It is RECOMMENDED that no other 1XX response be used due to uneven implementations of these responses. 180 Ringing should be repeated at approximately 3-second intervals if the call is not answered.
200 (OK)	Normal response to an answered call.
3XX	9-1-1 calls are usually not redirected, and thus 3XX responses are normally not used. 3XX MAY be used for calls within the ESInet. NG9-1-1 elements that initiate calls within the ESInet SHOULD appropriately respond as defined in RFC 3261 [10].
400 (Bad Request)	A 9-1-1 call is so malformed that the BCF cannot parse the message.
401 (Unauthorized)	MUST NOT occur for a 9-1-1 call.
402 (Payment Required)	SHOULD NOT occur for a 9-1-1 call or an internal call.

SIP Response Codes from NGCS	Description
403 (Forbidden)	Normally, 403 (Forbidden) SHOULD NOT occur, but if the BCF passes a malformed INVITE which downstream devices cannot handle, they may have no choice but to return 403.
404 (Not Found)	404 (Not Found) would normally not occur for a 9-1-1 call, but MAY be used within the ESInet.
406 (Not Acceptable)	The 406 (Not Acceptable) SHOULD NOT occur for a 9-1-1 call because the INVITE SHOULD NOT have an Accept header field that is unacceptable to the PSAP. If it does, 406 is the correct response.
407 (Proxy Authorization)	Proxy authorization is REQUIRED for all calls originated by entities within an ESInet/NGCS.
408 (Request Timeout)	MAY be issued in an unplanned circumstance. Normally, this SHOULD NOT happen to a 9-1-1 call.
413 (Request Entity too Large)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 413 (Request Entity Too Large).
414 (Request-URI Too Long)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 414 (Request-URI Too Long).
416 (Unsupported URI Scheme)	The BCF SHOULD accept any Request-URI, but downstream elements MAY return 416 (Unsupported URI Scheme).
486 (Busy Here)	PSAPs MAY limit the number of test calls, and if that limit is exceeded, the response SHALL be 486 Busy Here. 486 may also be generated by a race condition in the queue mechanism overload per section 4.2.1.3
500 (SIP Server Internal Error)	Indicates a failure in a system, or a failure to be able to process the call. Depending on the source of the failure, retry may succeed.
600 (Busy Everywhere)	If the BCF detects an active attack, it MAY respond with 600 (Busy Everywhere), rather than another 4XX response, although silent discard may be more effective. It is also returned by the Busy Policy Routing Rule "busy action"

1325 **3.1.5 Header fields and Request URI supported at the interface to the NGCS**

1326 The Best Current Practice for Communications Services in Support of Emergency Calling
1327 RFC 6881 [46] document referenced in this section contains normative text related to
1328 devices, originating network, and service providers. This document considers only the
1329 interface between an originating network and the NGCS with respect to the signaling of the
1330 emergency calls and callbacks between an OSP and the NGCS. References to RFC 6881 in
1331 this document are limited to requirement ED-62, the details of signaling for an emergency
1332 call. Accordingly, it shall be explicitly understood that all requirements referenced from RFC
1333 6881, regardless of wording and context in that document, SHALL apply only to the NGCS
1334 interface and SHALL NOT constrain or limit the signaling and procedures used by end
1335 devices, access networks, and originating networks when not interacting with the NGCS.
1336 The following table shows the SIP header fields required in the INVITE and MESSAGE
1337 methods for emergency calls, recalling that the Request-URI will contain "urn:service:sos"
1338 or a subservice of it as defined in RFC 6881 [46] Section 5.

1339 Only salient Header Fields are listed. Header Fields not listed and not defined in RFC 3261
1340 [10] are not expected to be provided nor received by the NGCS but if present, MAY be
1341 ignored, or MAY be processed as defined in the corresponding RFC.

Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
Identity	RFC 8224	[60]	Provides caller identity assertion using a cryptographically signed Personal Assertion Token (PASSporT) and associated parameters as defined in RFC 8225 [203]. Present on any call, added by STI-AS for outgoing calls.
Request-URI	RFC 3261 Section 8.1.1.1	ED62 1.	"urn:service:sos" or a subservice of it
To	RFC 3261 Section 8.1.1.2 & 20.39	ED62 2.	Usually sip:911 or "urn:service:sos" on an incoming call
From	RFC 3261 Section 8.1.1.3 & 20.20	ED62 3.	Content cannot be trusted unless protected by an Identity header field

[MM/DD/YYYY]

Page 46 of 675



Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
Via	RFC 3261 Section 8.1.1.7 & 20.42		Occurs multiple times, once for each SIP element in the path
CSeq	RFC 3261 Section 8.1.1.5 & 20.16		Defines the order of transactions in a session
Call-ID	RFC 3261 Section 8.1.1.4 & 20.8		This is the SIP call id, not the NG9-1-1 call id (e.g., " 1j9FpLxk3uxtm8tn@biloxi.example.com " not "urn:emergency:uid:callid:1j9FpLxk3uxtm8")
Call-Info	RFC 3261 Section 8.1.1.10 & 20.9		Contains Additional Data URIs, Call and Incident Tracking IDs and EIDO URIs
Contact	RFC 3261 Section 8.1.1.8 & 20.10	ED62 5.	Usually a "globally routable user agent URI" (gruu) (RFC 5627) [41]
Content-Length	RFC 3261 Section 20.14		
Content-Type	RFC 3261 Section 8.2.3 & 20.15		Used, for example, in RFC 4119 [6] and RFC 4566 ⁶ [12]
Geolocation	RFC 6442	ED62 8.	Only occurs in an emergency call
Geolocation-Routing	RFC 6442	ED62 8.	Specifies if the Geolocation header field can be used for routing. Only occurs in an emergency call

⁶ Examples may include application/pidf+xml to indicate a PIDF-LO in the body of the message and application/sdp to indicate use of Session Description Protocol (SDP) in the body of the message.

Header Field/Request	Defined In	See Section (or RFC 6881)	Notes
History-Info	RFC 7044		MAY indicate the call has been retargeted, MUST include a Reason header field per section 3.1.8
P-Access-Network-Info	RFC 3325		MAY contain cell site info in carrier specific formats in an incoming call
P-Asserted-Identity	RFC 3325		When present, typically overrides the From header field
P-Preferred-Identity	RFC 3325	3.1.15, 6.1.2.2	Used with unauthenticated (e.g., NSI) calls
Reason	RFC 3326		Included if an INVITE transaction is retargeted.
Route	RFC 3261 Section 20.34	ED62 4.	Usually the ESRP/PSAP URI on an incoming emergency call
Supported	RFC 3261 Section 8.1.1.9 & 20.37	ED62 7.	
Replaces	RFC 3891	4.7	Used in call transfer scenarios

1342 3.1.6 Header fields Accepted and also used internally

1343 Only salient Header Fields are listed. Header Fields not listed and not defined in RFC 3261 [10] are not expected to be provided nor received by the NGCS but if present, MAY be ignored, or MAY be processed as defined in the corresponding RFC.

Header Field	Defined In	Notes
Max-Forwards	RFC 3261 20.22	Specifies the maximum number of SIP elements that may be traversed before assuming a routing loop has occurred
Accept-Contact	RFC 3841	
Accept	RFC 3261 20.1	
Content-Encoding	RFC 3261 20.12	
Accept-Encoding	RFC 3261 20.2	

Header Field	Defined In	Notes
Content-Language	RFC 3261 20.13	
Accept-Language	RFC 3261 20.3	
Content-Disposition	RFC 3261 20.11	
Record-Route	RFC 3261 20.30	
Allow	RFC 3261 20.5	
Unsupported	RFC 3261 20.40	
Require	RFC 3261 20.32	
Proxy-Require	RFC 3261 20.29	
Expires	RFC 3261 20.19	
Min-Expires	RFC 3261 20.23	
Subject	RFC 3261 20.36	
Priority	RFC 3261 20.26	
Date	RFC 3261 20.17	
Timestamp	RFC 3261 20.38	
Organization	RFC 3261 20.25	
User-Agent	RFC 3261 20.41	
Server	RFC 3261 20.35	
Authorization	RFC 3261 20.7	
Authentication-Info	RFC 3261 20.6	
Proxy-Authenticate	RFC 3261 20.27	
Proxy-Authorization	RFC 3261 20.28	
WWW-Authenticate	RFC 3261 20.44	
Warning	RFC 3261 20.43	
Error-Info	RFC 3261 20.18	
Alert-Info	RFC 3261 20.4	
In-Reply-To	RFC 3261 20.21	
MIME-Version	RFC 3261 20.24	
Reply-To	RFC 3261 20.31	
Retry-After	RFC 3261 20.33	
RAck	RFC 3262 7.2	
RSeq	RFC 3262 7.1	
Event	RFC 6665 8.2.1	
Allow Events	RFC 6665 8.2.2	
Subscription-State	RFC 6665 8.2.3	

[MM/DD/YYYY]

Page 49 of 675



Header Field	Defined In	Notes
Resource-Priority	RFC 4412 3.1, Section 3.1.7	

1346 **3.1.7 Resource Prioritization**

1347 The Resource-Priority header field (RFC 4412 [37]) is used on SIP calls to indicate priority
1348 that proxy servers give to specific calls. All SIP user agents that place calls within the
1349 ESInet/NGCS MUST be able to set Resource-Priority. All SIP proxy servers in the
1350 ESInet/NGCS MUST implement Resource-Priority and process calls in priority order when a
1351 queue of calls is waiting for service at the proxy server and, when needed, preempt lower
1352 priority calls⁷. BCFs⁸ MUST police Resource-Priority of incoming SIP calls when the value
1353 comes from the “esnet” namespace. Any other namespace is ignored. BCFs MUST add a
1354 Resource-Priority header with an appropriate value from the “esnet” namespace if it is not
1355 present and should be included. BCFs MUST change or delete a value that is present on an
1356 incoming call that appears to be invalid or illegitimate. Those calls that appear to be
1357 emergency calls (such as those To: 911 but without a Request-URI of “urn:service:sos”)
1358 MUST be marked with a provisioned Resource-Priority, which defaults to “esnet.1”. PSAP
1359 callbacks during handling of an incident use “esnet.0”. Callbacks outside of an incident are
1360 not marked. ESInets normally use the “esnet” namespace.

1361 The use of the namespace in an ESInet is defined as:

Header	Description
esnet.0	Calls which relate to an incident in progress, but whose purpose is not critical
esnet.1	9-1-1 calls traversing the ESInet
esnet.2	Calls related to an incident in progress which are deemed critical
esnet.3-	not defined
esnet.4	

⁷ Mechanisms such as DiffServ are likely to be sufficient to assure that high priority traffic gets through an ESInet. Preemption is unlikely to be needed, even for very high priority responder traffic, and should not be used for 9-1-1 calls. However, if responders need resources, lower priority traffic may have to be cleared to provide such resources. Preemption is considered a necessary prerequisite to getting police and fire responders on an ESInet. Originating network operators have expressed concerns over preemption especially for 9-1-1 calls.

⁸ This function may be provided outside an SBC but within the BCF.

1362 **3.1.8 History-Info and Reason Parameter**

1363 When a call is not sent to the originally intended destination, for example when it is
1364 diverted by the ESRP to another PSAP, the final destination must have the ability to know
1365 why it got the call. For this reason, SIP elements in the NGCS MUST support the History-
1366 Info header field (RFC 7044 [35]) and a Reason header field. Elements that retarget a call
1367 MUST add a History-Info header field indicating the original intended recipient, and the
1368 reason why the call was retargeted. A 'text' parameter MUST also be supplied to further
1369 explain why the call was retargeted. NGCS elements MUST be prepared to handle a
1370 History-Info (and its associated Reason parameter) added by an element outside the
1371 ESInet before presentment to the 9-1-1 system. History-Info might be found in a call in
1372 other circumstances, such as a RouteAction with a cause code of "Normal-Next-Hop", code
1373 200. This document defines a new "Reason Protocol" to be used with the Reason header
1374 field for emergency call retargeting not due to normal SIP protocol mechanisms. The
1375 protocol value is 'emergency'. A registry is defined for cause codes (See Section 10.20)
1376 used for the SOS protocol value. The initial values of 1-10 are used for Policy Routing Rule
1377 (PRR) retargeting. The first time the ruleset is evaluated, the cause code SHALL be set to
1378 1. Every time the rule set is re-evaluated for the same call (such as when the targeted
1379 PSAP refuses the call), the cause code is incremented by one. When cause codes 1-10 are
1380 used, the 'text' parameter MUST be present, and must start with the ruleId followed by a
1381 colon and any other clarifying text the implementation wishes to add.

1382 **3.1.9 Media**

1383 All call handling elements MUST support media using Real-time Protocol (RTP) (RFC 3550
1384 [11]). Each SIP session initiation message or response SHOULD describe the media the
1385 User Agent is capable of supporting using Session Description Protocol (SDP) (RFC 4566
1386 [12]) in the body of the message. Support of any type of media (e.g., voice, video, text) in
1387 originating networks is based on regulatory requirements or business decisions. All
1388 elements in the ESInet/NGCS MUST support all media if offered, except that a legacy PSAP
1389 on a Legacy PSAP Gateway MAY only support audio, including Teletypewriter (TTY) tones
1390 when converted from Real Time Text (RTT).

1391 Media streams for voice, video, and text MUST be carried on RTP over UDP (User
1392 Datagram Protocol). All endpoints in an ESInet MUST implement media security with
1393 Secure Real Time Protocol (SRTP) using Datagram Transport Layer Security (DTLS) as
1394 specified in RFC 5763 [166] and RFC 5764 [167]. SRTP Security MUST be requested in all
1395 calls originated within an ESInet. If a call is presented to the ESInet with SRTP, SRTP

1396 MUST be maintained through the ESInet⁹. Since media are routinely logged, the Logging
1397 Service MUST maintain equivalent or better security on the logging (recording) session as
1398 that provided on the emergency call (communications) session. RTCP as defined in RFC
1399 3550 [11] and Secure Real Time Control Protocol (SRTCP) as defined in RFC 5764 [167]
1400 MUST be supported within the ESInet, and it is highly RECOMMENDED that all calls
1401 presented to the ESInet provide RTCP. Within the ESInet, all User Agents MUST support
1402 RTCP Extended Reports (RTCP XR) [65]. SIP User Agents within the ESInet SHOULD label
1403 all media

1404 Instant Messaging (IM) MUST be presented to the ESInet/NGCS using Message Session
1405 Relay Protocol (MSRP) [91] as the media stream.

1406 All elements in the ESInet/NGCS MUST support RFC 5888 [20], RFC 3605 [22], RFC 3581
1407 [21] and RFC 4574 [99]

1408 **3.1.9.1 Audio**

1409 To minimize transcoding requirements, it is desirable that User Agents in the ESInet/NGCS
1410 and in i3-PSAPs implement the maximum number of codecs used in the market.

1411 All User Agents in the ESInet/NGCS MUST support G.711 µ-law and A-law codecs. A-law
1412 support is REQUIRED in those cases in which devices manufactured primarily for non-North
1413 American markets are used within North America.

1414 The following table lists widely used audio codecs, whether they are available under license
1415 and their support requirements.

Name	Definition and Usage	Licensed	Support
G.711µ-law	Narrowband audio. Widely used by Voice over IP (VoIP) devices manufactured for North America and Japan. Supports North American DTMF tones inband.	No (free)	REQUIRED
G.711 A-law	Narrowband audio.	No (free)	REQUIRED

⁹ Some PSAPs may be subject to the Health Insurance Portability and Accountability Act (HIPAA), or a state equivalent. Maintaining privacy via SRTP MAY be required on all calls for such PSAPs, and media handling systems on the ESInets MAY need to support such capability by applying SRTP to those media regardless of whether SRTP was applied to the call when presented.

Name	Definition and Usage	Licensed	Support
	Widely used by VoIP devices manufactured for Europe and Asia. Note: DTMF tones are different in Europe & Asia; no support in the North American Market.		
EVS (Enhanced Voice Service)	Audio codec supporting Narrowband, Fullband, Wideband and Superwideband.	Yes	RECOMMENDED
AMR (a.k.a. AMR-NB)	Common Narrowband audio. Used in CDMA, GSM, 3G, LTE networks	Yes	RECOMMENDED
AMR-WB (G.722.2)	Common Wideband audio (HD Voice). Used in CDMA, GSM, 3G, LTE networks	Yes	RECOMMENDED
G.722	High Definition Voice (HD Voice). Wideband (high compression, high quality voice).	No (free)	RECOMMENDED
G.729AB	Wideband audio codec Used in VoIP networks.	Yes	OPTIONAL
OPUS	Open Source codec (RFC 6716 [212]). Being implemented by major providers.	No (free)	RECOMMENDED

1416 **3.1.9.2 Video**

1417 All User Agents in the ESInet/NGCS MUST support video compression format H.264/MPEG-
 1418 4 Version 10. The Baseline profile MUST be supported. Scalable baseline profile support is
 1419 RECOMMENDED. At least levels 1-3 MUST be supported. User Agents in the ESInet/NGCS
 1420 MUST support both RFC 5104 [121] and RFC 5168 [122] for full frame refresh requests.
 1421 The RFC 5104 Real-time Control Protocol (RTCP) method is preferred with fall back to RFC
 1422 5168 INFO method when the sender does not implement RFC 5104. To maintain the ability
 1423 to support rapid finger-spelling for sign language users, ESInet/NGCS elements must
 1424 attempt to maintain 30 frames per second video if offered by the sender. RTP/AVPF (RFC
 1425 4585 [123]) MUST be supported and is preferred in offers.

[MM/DD/YYYY]

Page 53 of 675



1426 **3.1.9.3 Real-Time Text**

1427 All call handling elements in the ESInet/NGCS MUST support RTP Payload for Text
1428 Conversation (RFC 4103) [85]. All except the LNG and LPG MUST also support the update
1429 for multi-party real-time text calls defined in draft-ietf-avtcore-multi-party-rtt-mix [219].
1430 Information on application of real-time text can be found in Framework for Real-Time Text
1431 over IP Using the Session Initiation Protocol (SIP) (RFC 5194 [84]).

1432 **3.1.9.4 TTY (Baudot tones)**

1433 NG9-1-1 anticipates that deaf and hard of hearing callers will migrate from TTY to other
1434 forms of communication including Real-Time Text devices and various forms of relay.
1435 Although use of TTY is expected to decline, it cannot be assumed that TTY will be
1436 completely gone by the time transition to NG9-1-1 is complete. Therefore, PSAPs MUST be
1437 capable of receiving calls from TTY devices.

1438 Handling Baudot tones within an IP (VoIP) network is very problematic. Baudot is much
1439 more sensitive to packet loss and other impairments than human voice. Transcoding from
1440 Baudot to RFC 4103 [85] Real-Time Text is usually the only practical way to send TTY
1441 messages across an IP network. If at all practical, transcoding SHOULD occur in the
1442 originating network as close to the TTY device as possible. However, it is very difficult to
1443 assure that all originating networks will do that transcoding. Therefore, ESInets/NGCS must
1444 have the ability to transcode. LNGs and LSRGs MUST transcode, and therefore it is the
1445 VoIP originating networks that are problematic in that they may present calls containing
1446 Baudot tones to the ESInet/NGCS. A transcoder MUST be placed as early in the media path
1447 as possible¹⁰, and the IP network between the originating network and the transcoder
1448 MUST be engineered to have very low packet loss and minimize other impairments. The
1449 transcoder MUST be compliant with RFC 5369 [86] and MUST be transparent to audio that
1450 is not Baudot tones. Transcoders SHOULD reduce the amplitude of detected Baudot tones
1451 but SHOULD NOT remove them entirely. PSAPs that receive calls from sources other than
1452 the ESInet/NGCS may need to handle TTY in another way, which is outside the scope of
1453 this document.

10 It would be desirable for the transcoder to be part of the BCF, but this may not be possible. If it is not part of the BCF it would be internal to the ESInet and the engineering of that part of the ESInet must assure that there is very low packet loss or other impairments.

1454 **3.1.10 Instant Messaging**

1455 Text-based communications for NG9-1-1 is supported by all call handling elements of an
1456 NG9-1-1 system in two ways: Real-Time Text (RTT) and Instant Messages (IM)¹¹, with
1457 location and the ability to support location updates.

1458 All call handling elements MUST support Message Session Relay Protocol (MSRP), RFC 4975
1459 [88], chat rooms, RFC 7701 [123], as well as RFC 4976 [89] and RFC 3994 [87]

1460 Location MUST be included in a Geolocation header field in the initiation of the MSRP
1461 session as with any other "call" to 9-1-1.

1462 Other Instant Messaging protocols such as XMPP MAY be supported by an originating
1463 network but MUST be interworked to MSRP prior to presentation to the ESInet/NGCS.

1464 **3.1.11 Non-interactive calls**

1465 Non-interactive calls, also called data-only emergency calls, are emergency calls that are
1466 initiated automatically, carry data, are not necessarily associated with a person, and do not
1467 establish two-way interactive media sessions.

1468 Non-interactive calls¹² presented to an ESInet are signaled with a SIP MESSAGE method
1469 containing a Common Alerting Protocol (CAP) [66] message (as described in RFC 8876
1470 [225]), possibly wrapped in an Emergency Data eXchange Language – Distribution Element
1471 (EDXL-DE) [78] wrapper. The <Area> element of the CAP message is copied, in PIDF-LO
1472 form, in a Geolocation header field of the SIP MESSAGE container. The CAP message is
1473 included in the body of the SIP MESSAGE, with a MIME type of application/common-
1474 alerting-protocol+xml.

1475 The MESSAGE MUST conform to section 3.1.15 with respect to Additional Data.

1476 The <Identifier> in the CAP message is not the same as the Call Identifier assigned in the
1477 ESInet/NGCS, but the log contains a record that correlates the two.

1478 The <Sender> SHOULD be the same as the From header field in the MESSAGE.

11 All ESInet elements support instant messaging using the specifications in this document. Any given originating network or device may not support instant messaging, and support of instant messaging by originating networks and devices may be subject to regulation.

12 All ESInet elements support non-interactive calls using the specifications in this document. Any given originating network or device may not support non-interactive calls, and support of non-interactive calls by originating networks and devices may be subject to regulation.

1479 If included, the <Addresses> element SHOULD contain “urn:service:sos”, the same as the
1480 Route header field for the Message.

1481 Automatic Crash Notification (AACN) calls (see Section 3.1.19) establish interactive media
1482 and are associated with human vehicle occupant(s), instead of non-interactive calls (which
1483 do neither). A non-interactive call from a vehicle might be placed by an element that is not
1484 designed to communicate with vehicle occupants (e.g., a sensor module embedded in the
1485 vehicle without speaker or microphone access) and does not provide interactive two-way
1486 media.

1487 If an <Area> element is included, at least one <Polygon> or <Circle> element MUST be
1488 included. Any <AreaDesc> and <Geocode> elements will not be used by the routing
1489 elements, although destination agencies may be able to make use of them. The
1490 Geolocation header field in the MESSAGE MUST have the PIDF-LO equivalent of the
1491 <Polygon> or <Circle> element(s).

1492 A digital signature SHOULD be included in the CAP message. The CAP message SHOULD
1493 NOT be encrypted.

1494 When the CAP message is enclosed in an EDXL-DE wrapper, the body of the SIP MESSAGE
1495 will contain a section application/emergency-data-exchange-language+xml.

1496 Non-interactive calls are routed and handled the same as voice, video, or text calls
1497 throughout the NG9-1-1 system. The routing mechanisms can route non-interactive calls
1498 differently from voice calls in the same way they can route video calls differently from voice
1499 calls. The parameters in the CAP message are available to the Policy Routing Function
1500 (PRF) as inputs to direct calls with specified characteristics to specific entities.

1501 **3.1.12 Bodies in messages**

1502 All SIP elements in an ESInet/NGCS MUST support multipart MIME as defined in RFC 2046
1503 [90]. For example, location, Additional Data blocks (RFC 7852) [107], and SDP may be
1504 present in a message body. All SIP elements in the NGCS MUST allow all mime types/body
1505 parts to pass to the PSAP.

1506 **3.1.13 Transport**

1507 All SIP elements MUST support TLS (See Section 2.8.1), TCP, and UDP transport. SIP
1508 signaling within the ESInet SHOULD be carried with TLS. If TLS transport fails or is not
1509 available, SIP elements SHOULD attempt to use TCP. If TLS and TCP transports both fail or
1510 are unavailable, SIP elements SHOULD fall back to UDP transport. It should be noted
1511 however that emergency call-related SIP messages have many large elements (for
1512 example, a PIDF-LO) and are more likely to be fragmented at the source when carried in

1513 UDP¹³. Packet fragmentation and defragmentation is fully supported in IPv4 however, in-
1514 transit fragmentation is not supported in IPv6. To avoid packets being dropped in transit
1515 because of size, IPv6 Path Maximum Transmission Unit Discovery (PMTUD) [234] MAY be
1516 used. It should be noted however that PMTUD utilizes Internet Control Message Protocol
1517 for IPv6 (ICMPv6) [235] to convey error responses back. Unfortunately, ICMP traffic is
1518 often blocked by firewalls in IP networks, which means the error response is never
1519 reaching the sender thus causing the packet to be lost and the sender not knowing that it
1520 has to reduce path MTU for the next packets it sends. Perfect Forward Security MUST be
1521 implemented and all SIP elements within the NGCS MUST support connection reuse, RFC
1522 5923 [217].

1523 Further, if the transport is not TLS, additional security weaknesses occur, and
1524 implementations MUST be prepared to deal with the security risks engendered when TLS
1525 protection is not available. Known attacks on incomplete fragmentation/reassembly
1526 implementations are another concern that MUST be addressed by all elements in the
1527 ESInet. Persistent TLS connections between elements that frequently exchange SIP
1528 transactions SHOULD be deployed.

1529 PSAPs are expected to detect the presence of RTP streams so they can distinguish RTP
1530 failure from real silence by the caller. Devices containing User Agents that are not part of a
1531 Back-to-Back User Agent (B2BUA) and that detect the loss of RTP SHOULD attempt to re-
1532 establish the streams by sending a re-INVITE to the other party. If that fails, the device
1533 SHOULD indicate a failure and provide a mechanism for taking action such as initiating
1534 disconnect. A call SHOULD NOT automatically be taken down if RTP streams fail. For
1535 example, a multimedia call which loses one of several streams SHOULD NOT be
1536 terminated, just for loss of some media.

1537 **3.1.14 Call Routing**

1538 All SIP elements MUST support routing of SIP messages per RFC 3261 [10] and RFC 3263
1539 [13]. Note particularly that URIs will often have the domain of the destination following the
1540 '@' rather than the hostname of a SIP server, and thus DNS SRV records (RFC 2782) [75]
1541 MUST be consulted to determine the hostname of the SIP server for that domain.
1542 Redundancy support for a SIP call MUST NOT depend on non-standard mechanisms in SIP
1543 elements. Only mechanisms such as UPDATE or re-INVITE with a modified Contact and
1544 out-of-dialog REFER, which only rely on aspects of standards this document requires of all

13 Note that the typical length of a SIP INVITE is around 1300 bytes including around 200 bytes for the SIP Header overhead. If, for example, a SIP INVITE contains a complete header, and a body containing both an SDP and a civic PIDF-LO, it is likely this SIP message may be too big for a single UDP packet; and may require fragmentation, which is sometimes problematic. TCP transport avoids such issues.

1545 SIP elements in the ESInet, MUST be used to perform re-home on an established SIP
1546 dialog in the case of host failure.
1547 Emergency call handling relies on the Service URN in the Request-URI being preserved. To
1548 avoid the Request-URI being rewritten, this document assumes loose routing (as defined in
1549 RFC 3261 [10]) is used for all SIP Calls end-to-end. Per RFC 3261, the "lr" parameter
1550 should be present in URIs used for routing. A future version of this document will
1551 normatively require this behavior.

1552 **3.1.15 Originating Network Interface**

1553 The originating call interface to the ESInet/NGCS is a SIP call interface as described above
1554 in Section 3.1. All calls MUST be routed the same way they would route if the location in
1555 the call was used to query the authoritative ECRF. Location MUST be included in the
1556 Geolocation header field (civic or geodetic) by reference or value. The location used to
1557 query the routing function MUST be included in the Geolocation header field of the
1558 outgoing INVITE or MESSAGE method. The call MUST be routed, using normal RFC 3261
1559 [10] procedures, to the URI obtained from the routing function using the "urn:service:sos"
1560 service URN (this URI should contain the "lr" parameter in the SIP INVITE to avoid
1561 Request-URI rewriting). A callback address MUST be included in the outgoing INVITE or
1562 MESSAGE method, with an immediate device callback in the Contact header field and an
1563 address of record for later callback in either the From header field (protected by the
1564 Identity header field) or a P-Asserted-Identity (P-A-I).

1565 A call from an unauthenticated device SHALL populate the P-Preferred-Identity header field
1566 in the INVITE request with an equipment identifier as a SIP URI and no P-Asserted-Identity
1567 SHALL be provided.

1568 The incoming INVITE or MESSAGE method to the ESInet/NGCS MUST include Call-Info
1569 header field values containing URIs that refer to Additional Data (RFC 7852) [107]
1570 "ProviderInfo" and "ServiceInfo" structures. This is indicated by "purpose" parameters of
1571 "purpose=EmergencyCallData.ProviderInfo" and "purpose=EmergencyCallData.ServiceInfo"
1572 (respectively). Additional Call-Info header field values MAY be included that contain a
1573 URI(s) that refers to other Additional Data blocks. Some providers MAY also include a
1574 "SubscriberInfo" block.

1575 Elements on an ESInet SHALL assume a SIP call entering the ESInet is an emergency call
1576 unless it can determine it is something else, such as a call to an administrative number.
1577 Even if the call does not have the emergency service URN in the Request-URI, the call
1578 SHOULD be assumed to be an emergency call and the Request-URI SHALL be rewritten to
1579 urn:service:sos by the BCF or originating ESRP.

[MM/DD/YYYY]

Page 58 of 675



1580 **3.1.16 PSAP Interface**

1581 The PSAP call interface is a SIP call interface as described in Section 3.1. All calls will be
1582 presented to the PSAP based on the terminating ESRP's Policy Routing Function (PRF),
1583 defined in Section 4.2.1.5. The Geolocation header field, Call-Info header fields and other
1584 header fields SHOULD be the same as above (Section 3.1.15). The call will be routed, using
1585 normal RFC 3261 [10] procedures, to the URI obtained from the ESRP's PRF. See Section
1586 4.6.1 for other information on the PSAP interface.

1587 **3.1.17 Element Overload**

1588 Any SIP element may encounter a condition in which it is asked to process more calls than
1589 it can handle. SIP element overload has been extensively studied (see RFC 6357 [81]).
1590 Simple mechanisms to handle overload are insufficient. This standard specifies methods to
1591 avoid overload of calls to specific agencies using the routing rule and queue mechanisms,
1592 but a given SIP element may still encounter overload. To cope with such overload, all SIP
1593 elements MUST implement the overload control mechanisms described in RFC 7339 [56].

1594 **3.1.18 Maintaining Connections and NAT Traversal**

1595 All elements in an ESInet that implement SIP interfaces MUST comply with RFC 5626 [42]
1596 (Outbound) to maintain connections from User Agents. PSAPs, IMRs, bridges and other
1597 elements that terminate calls from entities outside an ESInet that may be behind NATs
1598 MUST implement "Interactive Connectivity Establishment (ICE)", RFC 8445 [44] which
1599 includes support for "Session Traversal Utilities for NAT (STUN)", RFC 5389 [83].
1600 ESInets/NGCS SHOULD maintain a "Traversal Using Relays around NAT (TURN)" (RFC
1601 5766) [119] server for use by entities inside the ESInet placing outbound calls.

1602 **3.1.19 Advanced Automatic Crash Notification Calls**

1603 Advanced Automatic Crash Notification (AACN) calls, also called telematics calls, are
1604 emergency calls placed by vehicles or (Telematic Service Providers) (TSPs), initiated either
1605 automatically or manually, establishing interactive media channels, and conveying
1606 telematics data. The term "automatic crash notification" is used even though such calls are
1607 not necessarily in response to a crash and may be initiated manually as well as
1608 automatically; the telematics data they carry is often called "crash data" even though a
1609 crash has not necessarily occurred. In some older documents the word "collision" is used
1610 instead of "crash". The term Next Generation-Advanced Automatic Notification Calls (NG-
1611 AACN) is used to refer to AACN calls which conform to this document and the relevant IETF
1612 standards.

1613 Depending on implementation, the originator of an AACN call might be a vehicle or TSP on
1614 behalf of a vehicle. Communication between the vehicle and TSP is out of scope, but it is

[MM/DD/YYYY]

Page 59 of 675



1615 assumed that the TSP relays or passes information between the vehicle and PSAP (e.g.,
1616 requests for updated data or for the vehicle to perform an action such as flashing lights,
1617 providing access to a camera, unlocking doors, etc.).

1618 NG-AACN calls are specified in RFC 8148 [168]. As described there, vehicles (or TSPs)
1619 attach a Vehicular Emergency Data Set (VEDS) telematics dataset as described in VEDS,
1620 Version 3 [169] and a metadata/control object (RFC 8148) [168] containing vehicle/TSP
1621 capabilities information, to the SIP INVITE message that initiates an AACN call; the PSAP
1622 attaches a metadata/control object containing an acknowledgment that the dataset was
1623 received to its final response to the INVITE. When the vehicle (or TSP) receives the
1624 acknowledgement, it indicates not only that the PSAP received the VEDS data, but also that
1625 the call is a NG-AACN call end-to-end. If the vehicle (or TSP) receives the final response to
1626 an INVITE that lacks an acknowledgement of the VEDS data, this indicates that the call is
1627 not NG-AACN end-to-end (e.g., the call is being handled by a legacy PSAP or there is a
1628 legacy gateway at some point in the call path); the vehicle/TSP then falls back to legacy
1629 means of conveying crash and location data (e.g., text-to-speech, prerecorded audio, or
1630 verbal interaction with the TSP assistant).

1631 i3 PSAPs MUST support NG-AACN calls per RFC 8148 [168], including at least the VEDS
1632 dataset and the ability to send a telematics dataset acknowledgment. A PSAP MAY support
1633 additional telematics datasets (e.g., a PSAP might support the Pan-European eCall
1634 Minimum Set of Data (MSD) as described in RFC 8147 [202] to be prepared in case a
1635 vehicle sends the wrong dataset for North America), and MAY support enhanced
1636 capabilities of NG-AACN calls as described in RFC 8148 [168], (e.g., the ability to request a
1637 vehicle/TSP to send an updated or different dataset or to take some other action, such as
1638 flashing the lights, unlocking the doors, or accessing a vehicle camera feed).

1639 The VEDS dataset was created by a Joint Association of Public-Safety Communications
1640 Officials (APCO)/NENA working group to carry telematics data useful in handling
1641 emergency calls. Per RFC 8148 [168], the data is normally carried by value in the initial SIP
1642 INVITE message and therefore can be presented to the call taker when a call is assigned.
1643 An i3 PSAP MAY request a new VEDS dataset at any time during the call (e.g., if a call
1644 taker wants to check if the vehicle's condition, number of occupants, or location has
1645 changed). The vehicle/TSP MAY send an updated unsolicited VEDS dataset during the call
1646 as described in RFC 8148 [168] (e.g., if it is aware that data previously sent has changed).

1647 The VEDS dataset contains a comprehensive set of fields. It does not specify which fields
1648 vehicles must populate. Vehicle manufacturers and telematics vendors/providers are
1649 encouraged to populate as many fields as possible. The most critical fields are currently
1650 considered to be:

- 1651 • Vehicle VIN, year, make, model

[MM/DD/YYYY]

Page 60 of 675



- 1652 • Impact velocity
1653 • Vehicle location
1654 • Air bag deployment (i.e., indicating which airbags deployed)
1655 • Vehicle final resting orientation (e.g., on driver's side, on roof)
1656 • Number of occupants
1657 • Seat belt status
1658 • Hazardous cargo indicator(s)
1659 • Timestamp
1660 • Recent previous location
1661 • Call back number (e.g., to driver cellphone or vehicle cell number)
- 1662 The call taker may request the vehicle to perform an action (e.g., flashing lights, unlocking doors, view the feed from a vehicle camera). Such requests and responses are normally
1663 done during a call by using the SIP INFO method, as described in RFC 8148 [168]. It is
1664 OPTIONAL for vehicles and PSAPs to support actions (other than sending an updated
1665 dataset). It is RECOMMENDED that vehicles and PSAPs support such actions.
- 1666 The call routing mechanism defined in this document can route NG-AACN calls specially if
1667 desired (e.g., cooperating PSAPs might choose to have all NG-AACN calls handled by a
1668 designated PSAP). The parameters in the initial INVITE message that indicate that the call
1669 is an NG-AACN call are available to the Policy Routing Function [3.3] (e.g., the Request-
1670 URI, a Call-Info header field with a "purpose" parameter value of
1671 "EmergencyCallData.VEDS", and a MIME body part of
1672 "Application/EmergencyCallData.VEDS" each indicate an AACN call).

1674 **3.2 Location**

1675 Location is fundamental to the operation of the 9-1-1 system. Location is provided outside
1676 the ESInet/NGCS, and the generic functional entity that provides location is a Location
1677 Information Server (LIS). Since the LIS is external to the NGCS, the LIS is out of scope for
1678 i3. However, the entities inside the ESInet MUST interact with a source of location and thus
1679 the interfaces to that function are in scope and defined herein. For the purposes of this
1680 document, the only capabilities a LIS provides that are relevant to i3 are:

- 1681 a) A de-reference function defined below for location by reference
1682 b) Validation of location stored in the LIS by performing a validation query against the
1683 i3 LVF using the civic addresses, as described in Section 3.4.2.

1684 Any element that provides either or both of these two capabilities is considered a LIS
1685 within i3. Although a LIS is defined as a "server", as with all elements defined in this
1686 document, there may not be a physical server, and indeed, a LIS for some networks may
1687 only be a protocol interwork function to some other element in the network.

1688 The NG9-1-1 system supports location included by value in the body of a SIP message,
1689 with a pointer to it (i.e., a cid URL) in the Geolocation header field (RFC 6442) [8] of the
1690 SIP message. It also supports location by reference, when a location URI is populated in
1691 the Geolocation header field. All NGCS that receive location as a PIDF-LO must be prepared
1692 to receive location by reference and to use location by reference the NGCS MUST
1693 implement SIP and HTTP Enabled Location Delivery (HELD) (RFC 5985) [7] de-referencing
1694 protocols. A Location Information Server (LIS)¹⁴ MUST implement one or both of these
1695 protocols.

1696 Location by reference using SIP is an implied subscription to Presence (RFC 3856 [25]). An
1697 element needing location that has a SIP location URI MUST issue a SIP SUBSCRIBE (RFC
1698 6665 [14]) to the location URI. Filters (RFC 4661 [92], RFC 6446 [80] and RFC 6447 [72])
1699 MAY be used to control notification.

1700 An element needing location that has a HELD URI MUST de-reference per RFC 6753 [55].

1701 An access network that provides location by reference MUST supply either a SIP or a HELD
1702 location reference URI. Networks that use other protocols must interwork to SIP or HELD.
1703 NGCS that receive a location reference and forward location in SIP signaling to another
1704 element MUST pass the reference, and not any value that they determine by de-
1705 referencing (although the value should be logged). Each element MUST do its own de-
1706 reference operation, supplying its credentials to the LIS. It is RECOMMENDED that LISes
1707 cache location values and supply the cached values if multiple de-references occur in quick
1708 succession, such as when a call is being routed.

1709 In order for a LIS to be NG9-1-1 compliant, it MUST accept credentials traceable to the
1710 PSAP Credentialing Agency (PCA) when establishing the TLS connection as sufficient to
1711 deliver “dispatch” quality location. The credentials MAY be used by the LIS to authorize
1712 delivery of the caller’s location, with the required confidence/uncertainty information (when
1713 geodetic location is supplied) or civic/sub-civic address-level information (when civic
1714 location is supplied), when requested by a PSAP or other authorized entities.

1715 When location is passed by value, processing elements along the path MUST NOT change
1716 the location record. If additional location is acquired¹⁵, a new PIDF-LO with a different
1717 <Provided-by> element MUST be created and passed in addition to the original location. If
1718 the additional location is added before the call arrives at the PSAP, this additional location

¹⁴ A LIS, if it implements the SIP Subscribe/Notify mechanisms for location dereferencing, implements these portions of Presence server as defined in the IETF for the purposes of returning the location information only.

¹⁵ No mechanism to add location to a call within the NGCS before it is delivered to a PSAP is defined in this document.

1719 is added to the call signaling. If the additional location is added after the call is answered
1720 by a PSAP, it is included in an Emergency Incident Data Object (EIDO).

1721 Location Conveyance for the Session Initiation Protocol (RFC 6442 [8]) allows for multiple
1722 locations being passed so long as they relate to the same target however it does not
1723 provide guidance as to how to interpret multiple locations by entities processing such
1724 information. While it would be advisable to provide a unique location (or a reference to a
1725 unique location), there are nonetheless valid use cases for providing multiple locations in
1726 emergency calls presented to the ESInet/NGCS. For example, an Originating Network may
1727 provide a device-determined location and a network-determined location, after having
1728 performed a sanity check on the device-determined location. Another example is for an
1729 Originating Network providing a location information by-value and another location
1730 information by-reference. This could be useful for expediting call routing using the location
1731 by-value and leaving location updates being performed using the location by-reference. A
1732 third example is for an Originating Network providing location information in both civic and
1733 geodetic formats. This could be useful in cases where both formats are readily available at
1734 call setup time (RFC 5491 [52] should be followed in this case). This document provides
1735 guidance on how multiple location information could be presented to and processed in the
1736 ESInet/NGCS but does not prescribe how, nor does it assume that Originating Networks
1737 implement multiple location information on emergency calls.

1738 RFC 6442 [8] states "A SIP intermediary that adds a locationValue MUST position the new
1739 locationValue as the last locationValue within the Geolocation header field of the SIP
1740 request". Following this principle, it would be advisable that Originating Networks providing
1741 multiple location information in the original INVITE do so by making the top entry the
1742 preferred location to use for routing and put the other location information after. The order
1743 does not reflect whether the first entry is better, more reliable or more granular; it merely
1744 specifies the preferred choice of the Originating Network for location to use for routing. In
1745 such case, entities making routing decisions (like the ESRP) COULD simply use the top
1746 entry for routing and other downstream entities COULD use other entries for other
1747 purposes such as dispatch for example. In addition, an entity MAY opt to inspect the
1748 method token value and/or the provided-by token associated with each location object, if
1749 available, to make a determination on selecting the location information to use. An
1750 Originating Network may also provide a location-source parameter associated with each
1751 location information being passed, as defined in draft-ietf-sipcore-locparam [201]. This
1752 information MAY also be used by downstream entities to make a determination on selecting
1753 the location information to use. In addition, the confidence and uncertainty information
1754 which may be included in the location information (per RFC 7459) [145] could be
1755 considered when selecting from among multiple locations used.

1756 Multiple location information can be expressed in a number of ways. Here are a few
1757 examples.

1758 1. Multiple entries in the Geolocation header field

1759 Geolocation: <cid:target-a1w@orignet1.com>,
1760 <https://lis.orignet1.com:10236/flwprf232rfk>;loc-src=lrf.orignet1.com

1761 2. Multiple Geolocation header fields

1762 Geolocation: <cid:target-a1w@orignet1.com>
1763 Geolocation: <https://lis.orignet1.com:10236/flwprf232rfk>;loc-
1764 src=lrf.orignet1.com

1765 3. Multiple Location Information within a PIDF-LO

1766 Refer to the example in section 5.2 of RFC 6442 [8].

1767 There are multiple references to the Geolocation header field in this document. These
1768 references MUST be interpreted to include the possibility of multiple location information.

1769 Other than otherwise specified above, the implementation used within the origination and
1770 access networks for support of location is out of scope of i3¹⁶.

1771 **3.3 Policy (policies)**

1772 Policies are stored into and retrieved from a Policy Store using a web service. Section 3.3.1
1773 below describes the “Policy Store Web Service” that facilitates agencies uploading and
1774 retrieving policies. Policies are named for the function that the policy affects, (e.g., the
1775 RoutePolicy for a queue on an ESRP). A policy (or policy document or policy object)
1776 consists of a set of rules and is sometimes termed a “ruleset”. A specific Policy ruleset is
1777 uniquely identified by the combination of the policy name and the ID of the agency that
1778 owns (created) the policy and in some cases, the queue name. The client side of a web
1779 service authentication with the Policy Store identifies the agency storing or retrieving Policy
1780 rulesets.

1781 The Policy Store only accepts or delivers complete Policy rulesets, not individual rules
1782 within a Policy ruleset. The policy retrieved is valid until the expiration time. If the policy is
1783 needed for use after expiration, it MUST be retrieved again from the Policy Store. A policy
1784 retrieval request MAY return a referral to another Policy Store instead of the requested
1785 policy. The referred-to Policy Store might have the policy or might return another referral.

16 The roles of the access and originating networks in obtaining location for routing and delivery with an emergency call and interactions between such networks is out of scope and subject to SDO work outside NENA as well as regulatory policy.

- 1786 The standard i3 data rights management system can limit which agencies, agents, or
1787 functions are permitted to retrieve policies for another agency. The rights management
1788 policy (named "PolicyStore") can also allow an agency to store policies on behalf of another
1789 agency.
- 1790 Policies stored in the Policy Store MUST be signed by the owner of the Policy. A policy
1791 document MUST be a JSON Web Signature (JWS) object [171] per Section 5.10. For
1792 agencies within an ESInet, a credential traceable to the PCA MUST be used.

1793 **3.3.1 Policy Store Web Service**

1794 The Policy Store web service stores and retrieves policies (rulesets). The Policy Store
1795 accepts a policy document from a policy owner (an agency) or an agency authorized to
1796 store policies on behalf of the owner. Policies are identified by the policy type, the identity
1797 of the agency whose owns the policy and for Policy Routing Rules, a policyQueueName or
1798 an Id. Policy Types come from the Policy Type Registry 10.33 and consist of service names
1799 (which are policies that describe the access rights for the service), and policyTypes
1800 specified by this document or other NENA standards. The Policy Store provides the policy
1801 on request to a policy retriever. The Policy Store does not alter the policy document in any
1802 way; it stores it as an octet stream, without performing line-ending conversion, JSON or
1803 XML normalization, reformatting, or any other alteration. This allows the policy signature to
1804 be verified more efficiently, by avoiding the need to re-canonicalize the JSON.

1805 A policy is represented by a JWS which contains a Policy Object. The Policy Object consists
1806 of:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy. Restricted to the values in the Policy Types registry
policyId	CONDITIONAL, MUST NOT be specified unless policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", this is an arbitrary identifier for the policy

Name	Condition	Description
policyQueueName	CONDITIONAL, MUST NOT be specified unless policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For "OriginationRoutePolicy" or "NormalNextHopRoutePolicy", this is the policyQueueName
policyExpirationTime	OPTIONAL	Policy is not valid after this time
policyRules	MANDATORY	Array of Rules
policyLastModificationTime	CONDITIONAL, MUST be provided on retrieval, ignored on store	Date/Time policy was last modified
description	OPTIONAL	Text description of policy

1807

1808 3.3.1.1 Versions

1809 The Versions entry point of the Policy Store Web Service MUST include, in the "serviceInfo"
1810 parameter, the parameter "requiredAlgorithms" whose value is an array of JWS algorithms
1811 (as described in 5.10) acceptable to the policy store. The following example is from a policy
1812 store whose policy permits only the "EdDSA" algorithm:

```
1813 {
1814     "fingerprint": "Woof-FurrySuite-v8-8c439e",
1815     "versions":
1816     [
1817         {
1818             "major": 6, "minor": 3,
1819             "vendor": "burby-magic",
1820             "serviceInfo": { "requiredAlgorithms": [ "EdDSA" ] }
1821         }
1822     ]
}
```

1823 The OpenAPI definition of this interface can be found in Appendix E.1. This web service has
1824 the following functions:

1825 3.3.1.2 Policies

1826 Retrieves, Stores, Updates and Deletes a Policy ruleset from the common Policy Store.
1827 Policies are identified by the policy type, the identity of the agency whose policy is needed
1828 and for Policy Routing rules, a policyQueueName and possibly an Identifier. Policy Types
1829 come from the Policy Type Registry (Section 10.33) and consist of service names (which

[MM/DD/YYYY]

Page 66 of 675



1830 are policies that describe the access rights for the service), and types specified by this
1831 document or other NENA standards.

1832 For a GET operation the response is the Policy ruleset. The type, owner, id and/or
1833 policyQueueName can be omitted (at least one MUST be provided). This is a “wild-card”
1834 response where the set of policies that have the supplied parameter(s) is returned. Limit
1835 and start parameters are supported for pagination. The policies retrieved are valid until the
1836 expiration time. If the policy is needed for use after expiration, it MUST be retrieved again
1837 from the Policy Store.

1838 Instead of returning the policy requested, the response MAY return a referral to another
1839 Policy Store that might have the policy via an HTTP 307 Temporary Redirect.

1840 **3.3.1.2.1 Retrieve Policies**

1841 HTTP method: GET

1842 Resource name .../Policies

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
policyOwner	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	Type of the policy. Values are limited to names in the Policy Types registry
policyId	CONDITIONAL, at least one of policyType, policyowner, policyId or policyQueueName MUST be provided. If policyType is specified, MUST NOT be specified unless policyType is “OtherRoutePolicy”	For “OtherRoutePolicy”, this is the id mentioned in an InvokePolicyAction

Name	Condition	Description
policyQueueName	CONDITIONAL, at least one of policyType, policyowner, policyId or policyQueueName MUST be provided. If policyType is specified, MUST NOT be specified unless policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

1843 Status Codes

- 1844 200 Policies found
- 1845 307 Temporary Redirect
- 1846 451 Unknown or bad Policy Type
- 1847 452 Unknown or bad Agency Name
- 1848 453 Not available here, no referral available
- 1849 454 Unspecified Error
- 1850

1851 On a successful GET, a PolicyArray is returned:

1852 **PolicyArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
policies	MANDATORY	Array of Policy objects, each as a JWS

1853

1854 **3.3.1.2.2 Store Policy**

1855 Initiates the creation of a Policy ruleset in the Policy Store. The POST has a request body containing the Policy as a JWS.

1857 Following a POST, the Policy Store MUST confirm that the policyExpirationTime is in the future, the size of the received policy exactly matches the size specified in policySize, the structure and contents of the document is well-formed and conformant, for Policy Routing
1858 Rules that each rule has a unique id, and verify the signature of the JWS.
1859
1860

1861 HTTP method: POST

[MM/DD/YYYY]

Page 68 of 675



- 1862 Resource name .../Policies
1863 The request body contains the policy as a JWS
1864 Status codes
1865 201 Policy successfully created
1866 434 Signature Verification Failure
1867 436 Duplicate or Invalid Priority
1868 437 Bad Policy Structure
1869 451 Unknown or bad Policy Type
1870 452 Unknown or bad Agency Name
1871 454 Unspecified Error
1872 460 Bad PolicyExpirationTime

1873 **3.3.1.2.3 Update Policy**

1874 Initiates the update of a Policy ruleset in the Policy Store. This function's parameters
1875 include the name of the policy, the agency or service whose policy is being updated, for
1876 PRRs, the policyQueueName or policyId. The request body contains the replacement policy
1877 as a JWS.

1878 When processing an Update request, the Policy Store MUST confirm that the
1879 policyExpirationTime is in the future, the size of the received policy exactly matches the
1880 size specified in policySize, the structure and contents of the document is well-formed and
1881 conformant, for Policy Routing Rules that each file has a unique ID, and verify the
1882 signature of the JWS.

1883 HTTP method: PUT

1884 Resource name .../Policies

1885 The request body contains the replacement policy as a JWS

1886 Parameters:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service owning the policy(ies). MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy

Name	Condition	Description
policyId	CONDITIONAL, MUST be provided if policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, MUST be provided policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

1887 Status Codes

- 1888 200 Policy successfully updated
- 1889 404 Not found
- 1890 434 Signature Verification Failure
- 1891 436 Duplicate or Invalid Priority
- 1892 437 Bad Policy Structure
- 1893 451 Unknown or bad Policy Type
- 1894 452 Unknown or bad Agency Name
- 1895 454 Unspecified Error
- 1896 460 Bad PolicyExpirationTime

1897 **3.3.1.2.4 Delete Policy**

1898 Deletes a Policy ruleset in the Policy Store. The parameters are the name of the policy and
1899 the agency/service whose policy is being deleted and for PRRs, the policyQueueName or
1900 policyId.

1901 HTTP method: DELETE

1902 Resource name .../Policies

1903 Parameters:

Name	Condition	Description
policyOwner	MANDATORY	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	MANDATORY	Type of the policy

Name	Condition	Description
policyId	CONDITIONAL, MUST be provided if policyType is "OtherRoutePolicy"	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, MUST be provided policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy"	For PRRs, this is the policyQueueName

1904 Status Codes

1905 200 Policy successfully deleted
 1906 404 Not found
 1907 451 Unknown or bad Policy Type
 1908 452 Unknown or bad Agency Name
 1909 454 Unspecified Error

1910 3.3.1.3 Policy Enums

1911 Returns a list of policy names available in the store for a specific agency/service. The type, owner, policyId and/or policyQueueName can be omitted (at least one MUST be provided).
 1912 This is a "wild-card" response where the set of policies that have the supplied parameter(s)
 1913 is returned. Limit and start parameters are supported for pagination. The enumeration
 1914 includes only those policies that are actually stored in this specific instance of the Policy
 1915 Store.

1917 3.3.1.3.1 Enumerate Policies

1918 HTTP method: GET

1919 Resource name .../PolicyEnums

1920 Parameters

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.

Name	Condition	Description
policyOwner	CONDITIONAL, at least one of policyOwner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	ID of the agency or service whose policy is requested. MUST be a FQDN or URI that contains a FQDN
policyType	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	Type of the policy. MAY be "*" for all policy types
policyId	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	For "OtherRoutePolicy", the id of the policy mentioned in the InvokePolicyAction
policyQueueName	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	For PRRs, this is the policyQueueName
policiesUpdatedSince	CONDITIONAL, at least one of policyowner, policyType, policyQueueName, policyId or policiesUpdatedSince MUST be provided	Query returns all policies having the time of creation or last modification greater than policiesUpdatedSince

1921 On a successful GET, a PolicyEnumArray is returned:

1922 **PolicyEnumArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
policyEnums	MANDATORY	Array of PolicyEnum objects

1923 **PolicyEnum** (for each policy)

Name	Condition	Description
policyType	MANDATORY	The type of the policy.
policyOwner	MANDATORY	The policy owner of interest. MUST be a FQDN or URI that contains a FQDN
policyId	CONDITIONAL, MUST be provided for "OtherRoutePolicy"	Id of the policy
policyQueueName	CONDITIONAL, MUST be provided for "NominalNextHopRoutePolicy"	For "RoutePolicy", this is the policyQueueName
policyExpirationTime	MANDATORY	The expiration time of the policy
policyLastModificationTime	MANDATORY	Date/Time of last modification

1924 Status Codes

- 1925 200 Policies enumerations found
- 1926 404 Not found
- 1927 451 Unknown or bad Policy Type
- 1928 452 Unknown or bad Agency/Service Name
- 1929 454 Unspecified Error

1930 **3.3.2 Policy Store Replication**

1931 The Policy Store is replicated and distributed. There is a single authoritative master store for each agency (policy owner). There MAY be one or more replicas in other Policy Stores of the policies for any given agency. Each Policy Store that is authoritative for the policies of one or more agencies is provisioned with a list of replicas that are authorized to store policies from each agency. Each replica is provisioned with a list of agencies for which it serves as replica and the authoritative master policy store for each. A replica uses the

[MM/DD/YYYY]

Page 73 of 675



1937 RetrievePolicy function to get policies from the master Policy Store, and refreshes them
1938 automatically before they expire. EnumeratePolicy MAY be used to determine which
1939 agency's policies are stored in the Policy Store.
1940 As an optimization, the replica MAY make use of the policiesUpdatedSince parameter:
1941 policiesUpdatedSince MAY be used as a poll to maintain an up-to-date replica, rather than
1942 waiting for expiration times of individual policies (since a policy owner might update a
1943 policy prior to expiration). Use of policiesUpdatedSince is RECOMMENDED for replicas of
1944 policies that could reasonably be changed unexpectedly, such as in a disaster situation.
1945 The Policy Store is replicated and distributed. There is a single authoritative master store
1946 for each agency (policy owner). There MAY be one or more replicas in other Policy Stores
1947 of the policies for any given agency. Each Policy Store that is authoritative for the policies
1948 of one or more agencies is provisioned with a list of replicas that are authorized to store
1949 policies from each agency. Each replica is provisioned with a list of agencies for which it
1950 serves as replica and the authoritative master policy store for each. A replica uses the
1951 Policies GET function to get policies from the master Policy Store and refreshes them
1952 automatically before they expire. PolicyEnums MAY be used to determine which agency's
1953 policies are stored in the Policy Store.
1954 The PolicyEnums function is also useful to maintain a referral service to distribute the
1955 Policy Store. Policy Stores MAY refer queries to another Policy Store. To do so, they
1956 maintain a map of which Policy Stores have what policies. The mapping MAY be
1957 provisioned or learned via the PolicyEnums function (with a list of other Policy Stores
1958 provisioned in a specific Policy Store).

1959 **3.3.3 Route Policy Syntax**

1960 This section describes the syntax and semantics of the policy language used for making call
1961 routing decisions.

1962 A policy document is a JWS; the payload is a JSON object conformant to Appendix E.10.
1963 Policy documents are carried using the MIME type of Application/EmergencyCallData.auth-
1964 policy+json. A policy document is composed of a set of rules and an optional description.
1965 Each rule is a JSON object containing the following members:

- 1966 • “id” (REQUIRED): a string containing an ID for the rule; the value MUST be unique
1967 within the ruleset
- 1968 • “priority” (REQUIRED): an integer greater than or equal to zero that MUST be
1969 unique within the ruleset; this is the rule’s priority
- 1970 • “conditions” (OPTIONAL): an object that MAY contain one or more Condition objects
1971 (Section 3.3.3.1 below)

[MM/DD/YYYY]

Page 74 of 675



- 1972 • “actions” (REQUIRED): an object that MUST contain one or more Action objects
1973 (Section 3.3.3.1 below)
- 1974 • “description” (OPTIONAL): a string that describes the rule
- 1975 Within a rule, the “Conditions” object evaluates to ‘true’ or ‘false’. If it evaluates to ‘true’
1976 then the “actions” part of the rule is eligible to be executed. Because multiple rules might
1977 have “Condition” parts that evaluate to ‘true’, each rule has an associated priority value. A
1978 higher (numerically greater) value takes precedence over a rule with a lower value. When
1979 more than one rule has a “Conditions” section that evaluates to ‘true’, only the rule with
1980 the largest priority value has its actions section executed. Priority 0 is the lowest priority; a
1981 rule with priority 0 is only executed if no other rule’s “conditions” evaluate to ‘true’. Each
1982 rule also has an ID, which is a string unique to the ruleset.
- 1983 In a Route Policy, an omitted “Conditions” section evaluates to ‘true’; this permits
1984 constructing default or “catch-all” rules that are executed only if no other rule matches.
1985 Normally, such rules have an extremely low priority value, e.g., 0.
- 1986 A Route Policy document MUST be a JWS [171] as per Section 5.10 and MUST have a
1987 payload conforming to Appendix E.10.
- 1988 A routing element MUST verify the JWS signature before executing the rules. The Policy
1989 Store is REQUIRED to store and retrieve Route Policy documents byte-for-byte unaltered
1990 (so that the JWS extracted is the exact same octet stream stored, and calculates the exact
1991 same digest). If the JWS signature verification fails, the policy MUST NOT be executed. Any
1992 element encountering a failed JWS signature verification SHOULD file a Policy Discrepancy
1993 Report (Section 3.7.13) against the policy owner and MAY file a Policy Store Discrepancy
1994 Report (Section 3.7.4) against the Policy Store.
- 1995 **3.3.3.1 Conditions**
- 1996 This section describes the “Conditions” part of the rule. “Conditions” is an array of zero or
1997 more condition objects (listed in the following subsections), that MAY contain a “negation”
1998 member that inverts the condition sense. Several conditions require that the ESRP use the
1999 SIP-based notification mechanism described in RFC 6665 [14] to be aware of the state or
2000 condition of an external entity (such as a service or queue), or perform a L0cation to
2001 Service Translation (LoST) query and store the resulting URI in a variable.
- 2002 A condition object contains the following members:
- 2003 • conditionType: a string which MUST exist and be set to the specific condition type.
2004 • negation: an OPTIONAL Boolean that when set to ‘true’ inverts the condition sense.
2005 When “negation” exists and is set to ‘true’, it reverses the evaluation of the
2006 “Conditions” object; when set to ‘false’ or omitted it has no effect.

- 2007 • description: an OPTIONAL string containing a description of the condition.
2008 • Other condition-specific members as described in the below subsections.
- 2009 When "Conditions" contains more than one condition object, they are evaluated using a
2010 logical AND: if they all evaluate as 'true', the "Conditions" evaluates as 'true'; if any
2011 evaluate as 'false', the "Conditions" evaluates as 'false'. The exception is
2012 "TimePeriodCondition": all "TimePeriodCondition" objects in a rule are evaluated with an
2013 implicit OR. Logically, each condition other than "TimePeriodCondition" in a rule is
2014 evaluated; if they all evaluate as 'true' and any "TimePeriodCondition" within the rule
2015 evaluates to 'true', then the "Conditions" evaluates to 'true'.
- 2016 After evaluation of the contained condition object(s), if the "negation" member is present
2017 and set to 'true', the evaluation is reversed.
- 2018 If a ruleset has no conditions that evaluate to 'true', the ESRP MUST treat this as a fatal
2019 error (see Section 4.2.1.6).
- 2020 **3.3.3.1.1 Time Period Condition**
- 2021 "TimePeriodCondition" allows a rule to make decisions based on the time, date, and time
2022 zone. The following members are defined for use within a "TimePeriodCondition" object:
- 2023 dateStart: Start of interval (Timestamp, see Section 2.3). This member is MANDATORY.
- 2024 dateEnd: End of interval (Timestamp). This member is MANDATORY.
- 2025 timeStart: Start of time interval in a particular day. It uses the partial-time data type as
2026 described in Section 5.6 of RFC 3339 [135], interpreted as having the same
2027 offset from UTC as found in dateStart and dateEnd. This member is
2028 OPTIONAL. The default value is "00:00:00".
- 2029 timeEnd: End of time interval in a particular day. It uses the partial-time data type as
2030 described in Section 5.6 of RFC 3339 [135], interpreted as having the same
2031 offset from UTC as found in dateStart and dateEnd. This attribute is
2032 OPTIONAL; if specified MUST be greater than the value of timeStart. The
2033 default value is 23:59:59.
- 2034 weekdayList: List of days of the week. This member is optional. The "weekdayList" member
2035 specifies a comma-separated list of days of the week:
- 2036 • "MO" indicates Monday,
2037 • "TU" indicates Tuesday,
2038 • "WE" indicates Wednesday,
2039 • "TH" indicates Thursday,
2040 • "FR" indicates Friday,

[MM/DD/YYYY]

Page 76 of 675



- 2041 • "SA" indicates Saturday, and
2042 • "SU" indicates Sunday.

2043 These values are not case-sensitive. Whitespace after a comma is permitted.

2044 An ESRP or other entity executing a policy MUST ignore an invalid value in a member (e.g.,
2045 a timeStart or timeEnd with an hour greater than 24, or minutes or seconds greater than
2046 60, or hour set to 24 with minutes or seconds greater than 0) but SHOULD generate a
2047 Discrepancy Report against the policy owner (Section 3.7.13) and MAY file a DR against the
2048 Policy Store (Section 3.7.4). A Policy Store MUST reject as an error an attempt to store or
2049 update a policy containing an invalid value. A Policy Store MAY also file a Discrepancy
2050 Report against the policy owner.

2051 **3.3.3.1.1.1 Examples of "TimePeriodCondition"**

2052 The following examples illustrate the "TimePeriodCondition" object:

```
2053 {  
2054     "conditionType": "TimePeriodCondition",  
2055  
2056     "description": "Example Time Rule 1  
2057     Rule applies on weekdays (Monday through Friday)  
2058     between 8:00 AM and 6:00 PM during the period  
2059     from January 12th, 2017 8:30 AM Eastern Standard Time  
2060     until January 1st, 2018 6:30 PM Eastern Standard Time  
2061     NOT accounting for Daylight Saving Time:",  
2062  
2063     "dateStart": "2017-01-12T08:30:00-05:00",  
2064     "timeStart": "08:00",  
2065     "timeEnd": "18:00",  
2066     "weekdayList": "MO, TU, WE, TH, FR",  
2067     "dateEnd": "2018-01-01T18:30:00-05:00"  
2068 }  
2069  
2070 {  
2071     "conditionType": "TimePeriodCondition",  
2072  
2073     "description": "Example Time Rule 2  
2074     Rule applies on weekdays (Monday through Friday)  
2075     between 8:00 AM and 6:00 PM during the period  
2076     from January 1st, 2018 12:01 AM Eastern Standard Time  
2077     until December 31st, 2019 11:59 PM Eastern Standard Time  
2078     adjusting for Daylight Saving Time (2:00 AM on the second  
2079     Sunday in March until 2:00 AM on the first Sunday of  
2080     November) during the period:  
2081  
2082     Standard Time period at start of 2018:",  
2083  
2084     "dateStart": "2018-01-01T00:01:00-05",  
2085 }
```

```
2086          "timeStart":      "08:00",
2087          "timeEnd":        "18:00",
2088          "weekdayList":    "MO,TU,WE,TH,FR",
2089          "dateEnd":        "2018-03-11T01:59:59-05:00"
2090      }
2091
2092
2093      {
2094          "conditionType": "TimePeriodCondition",
2095
2096          "description":  "Daylight Saving Time period of 2018:",
2097
2098          "dateStart":     "2018-03-11T02:00:00-04:00",
2099          "timeStart":     "08:00",
2100          "timeEnd":       "18:00",
2101          "weekdayList":  "MO,TU,WE,TH,FR",
2102          "dateEnd":       "2018-11-04T01:59:59-04"
2103      }
2104
2105
2106      {
2107          "conditionType": "TimePeriodCondition",
2108
2109          "description":  "Standard time period winter 2018-2019:",
2110
2111          "dateStart":     "2018-11-04T02:00:00-05:00",
2112          "timeStart":     "08:00",
2113          "timeEnd":       "18:00",
2114          "weekdayList":  "MO,TU,WE,TH,FR",
2115          "dateEnd":       "2019-03-10T01:59:59-05:00"
2116      }
2117
2118
2119      {
2120          "conditionType": "TimePeriodCondition",
2121
2122          "description":  "Daylight Saving Time period of 2019:",
2123
2124          "dateStart":     "2019-03-10T02:00:00-04",
2125          "timeStart":     "08:00",
2126          "timeEnd":       "18:00",
2127          "weekdayList":  "MO,TU,WE,TH,FR",
2128          "dateEnd":       "2019-11-03T01:59:59-04:00"
2129      }
2130
2131
2132      {
2133          "conditionType": "TimePeriodCondition",
2134
2135          "description":  "Standard time period late 2019:",
2136      }
```

```
2137          "dateStart": "2019-11-03T02:00:00-05:00",
2138          "timeStart": "08:00",
2139          "timeEnd": "18:00",
2140          "weekdayList": "MO,TU,WE,TH,FR",
2141          "dateEnd": "2019-12-31T23:59:59-05:00"
2142      }
```

2143 The following aspects need to be considered:

- 2144 1. By default, if all the OPTIONAL members are omitted, the TimePeriodCondition is
2145 valid for the whole duration from "dateStart" to "dateEnd" inclusive.
- 2146 2. The "weekdayList" member comes into effect only if the period from "dateStart"
2147 until "dateEnd" is long enough to accommodate the specified values, otherwise it is
2148 ignored.
- 2149 3. Any "weekdayList" values that do not correspond to expected values MUST be
2150 ignored.
- 2151 4. Each "timeStart" and "timeEnd" member MUST contain a single value. If "timeStart"
2152 is later than "timeEnd", both "timeStart" and "timeEnd" SHALL be ignored.
- 2153 5. Multiple "TimePeriodCondition" objects MAY be included in a rule. If multiple
2154 "TimePeriodCondition" objects are present, each is evaluated independently (an
2155 implicit "or").
- 2156 6. The time is specified with a timezone offset (i.e., in local time with the offset from
2157 UTC); rules need to consider any local daylight-saving changes. Multiple time period
2158 specifications MAY be used for this purpose.
- 2159 7. Since rules with time elements may have an end time, updates to rules may be
2160 required occasionally to maintain the desired effect.

2161 **3.3.3.1.2 SIP Header Condition**

2162 "SipHeaderCondition" tests a SIP header field in the INVITE or MESSAGE of a call (such as
2163 "From", "To", "Contact", etc.).

2164 The "SipHeaderCondition" object has three members:

- 2165 • "field", which MUST exist and be set to the name of a SIP header field (e.g.,
2166 "Recv-Info"); note that the value does not include the colon which follows a
2167 header field name in a message. The value MUST be the full name of the header
2168 field; it matches the full or abbreviated name of the header field in the SIP
2169 message.
- 2170 • "operator", which MUST exist and be set to one of:
 - 2171 ○ "EQ" for an equality match,
 - 2172 ○ "SS" for a substring match, or

- 2173 ○ “IS” for a registry-defined match.
- 2174 • “content”, which MUST be present. If “operator” is set to “EQ” or “SS”, this
2175 member contains a string against which the specified header field value is
2176 compared, either for equality or as a substring. If “operator” is set to “IS”, this
2177 member MUST be set to an entry in the “SIPheader ‘Is’ Operator conditions”
2178 registry (Section 10.15).
- 2179 An equality match compares the value of the “content” member against the value of the
2180 specified header field, including any parameters. A substring match tests if the value of the
2181 “content” member is present anywhere in the header field value, including parameters.
2182 Both equality and substring matches are case-insensitive.
- 2183 The “IS” operator uses a registry (See “SIPheader ‘Is’ Operator conditions”, Section 10.15)
2184 The “content” member is set to a value contained in the registry. This operator tests the
2185 header field for the condition is specified by the “content” value per the registry.
- 2186 “SipHeaderCondition” evaluates to ‘false’ if “operator” is “EQ” or “SS” and the specified
2187 header field is not found in the SIP INVITE or MESSAGE.

2188 **3.3.3.1.3 Additional Data Condition**

2189 “AdditionalDataCondition” tests the SIP INVITE or MESSAGE of the call to check if it
2190 contains an Additional Data block that meets a specified condition. At minimum, ESRPs
2191 access and evaluate against the condition criteria all Additional Data blocks that are
2192 conveyed by value or by reference via Call-Info header fields. It is
2193 implementation dependent if the ESRP also performs an ECRF query for URIs for Additional
2194 Data associated with a location and then dereferences those URIs, or queries IS-ADRs,
2195 to access and evaluate further Additional Data blocks against the Additional Data condition.
2196 No mechanisms currently exist, however, for differentiating these data blocks in the rule.
2197 This will be subject to review in a subsequent version of this document. See Sections
2198 4.2.2.3 ECRF interface, 4.2.2.5 Additional Data Interface, 4.3.3.4 Service to access
2199 Additional Data for a location, and 4.11.1 Identity Searchable Additional Data Repository
2200 (IS-ADR).

2201 The “AdditionalDataCondition” object has four members:

- 2202 • “type”, which MUST exist and be set to a value consisting of “EmergencyCallData”, a
2203 dot, and a block type contained in the IANA Emergency Call Data Types Registry
2204 [179].
- 2205 • “element” which value is the name of one of the elements in the specified Additional
2206 Data block; this member MUST be omitted when “operator” is set to “exists” or
2207 “missing” and is MANDATORY otherwise.
- 2208 • “operator”, which MUST exist and be set to one of:

2209 ○ “exists”, which evaluates as ‘true’ if the specified Additional Data block exists
2210 in the incoming message;
2211 ○ “missing”, which evaluates as ‘true’ if the specified Additional Data block does
2212 not exist in the incoming message;
2213 ○ “EQ” (equals), which checks for equality (case-insensitive) between the string
2214 in “content” and the element contents;
2215 ○ “SS” (substring), which checks if the string in “content” is contained in the
2216 element (case-insensitive);
2217 ○ “NE” (not equal to), which is the inverse of “EQ”;
2218 ○ “GT” (greater than), which checks if the string in “content”, treated a numeric
2219 or date value, is greater than the element contents;
2220 ○ “LT” (less than), which checks if the string in “content”, treated a numeric or
2221 date value, is less than the element contents;
2222 ○ “GE” (greater than or equal to), which checks if the string in “content”,
2223 treated a numeric or date value, is greater than or equal to the element
2224 contents;
2225 ○ “LE” (less than or equal to), which checks if the string in “content”, treated a
2226 numeric or date value, is less than or equal to the element contents;
2227 If the value in the Additional Data Block element being processed does not
2228 evaluate to a number or a date, GT/LT/GE/LE evaluate to ‘false’. String
2229 comparisons are case-insensitive. If the specified Additional Data Block does
2230 not exist or does not contain the specified element, all operators other than
2231 “missing” evaluate to ‘false’.

- 2232 • “content”, the value of which is compared with the value of the specified element of
2233 the specified Additional Data block, using the test specified by “operator”; this
2234 member MUST be omitted when “operator” is “present” or “missing” and is
2235 MANDATORY otherwise.

2236 A typical use for this condition is to route based on the class of service components, or to
2237 route VEDS calls to a VEDS-equipped PSAP.

2238 **3.3.3.1.3.1 Examples of “AdditionalDataCondition”**

2239 The following example tests if the “EmergencyCallData.ServiceInfo” block’s <ServiceType>
2240 element (analogous to Class of Service in legacy E9-1-1) indicates the call was placed via a
2241 relay service (which would be the case if the call was placed via a sign language
2242 relay/interpretation service or a telematics service that provides a human on the call):

```
2243 {  
2244   "conditionType": "AdditionalDataCondition",  
2245   "type": "EmergencyCallData.ServiceInfo",  
2246   "operator": "EQ",
```

```
2247         "element":      "ServiceType",
2248         "content":       "relay"
2249     }
2250
```

2251 The following example tests if a call contains an <EmergencyCallData.VEDS> block,
2252 indicating the call is an NG-AACN call:

```
2253     {
2254         "conditionType": "AdditionalDataCondition",
2255         "type":          "EmergencyCallData.VEDS",
2256         "operator":      "exists",
2257     }
```

2258 The following example tests if a call contains an <EmergencyCallData.VEDS> block (which
2259 indicates the call is an NG-AACN call) containing a
2260 'VehicleFinalRestOrientationCategoryCode' attribute with a value other than 'Normal'
2261 (indicating that the vehicle's final resting orientation is abnormal, e.g., on a side or roof or
2262 end):

```
2263     {
2264         "conditionType": "AdditionalDataCondition",
2265         "type":          "EmergencyCallData.VEDS",
2266         "operator":      "NE",
2267         "element":       "VehicleFinalRestOrientationCategoryCode",
2268         "content":       "Normal"
2269     }
```

2270 **3.3.3.1.4 MIME Body List Condition**

2271 “MimeBodyCondition” tests if an incoming call’s SIP INVITE or MESSAGE has a body part
2272 with a specified MIME type.

2273 The “MimeBodyCondition” object MUST contain a “mimeList” member, which is an array of
2274 strings. Each string is a MIME media type and subtype (e.g., “text/plain”) from the IANA
2275 registry [181]. The values in the array are compared with the content types in the body of
2276 the SIP INVITE or MESSAGE. A “MimeBodyCondition” object evaluates to ‘true’ if any of the
2277 call’s body parts is of a type contained in the array (i.e., the MIME type and subtype of
2278 each body part of the SIP INVITE or MESSAGE is compared against each value in the array
2279 using a logical OR).

2280 **3.3.3.1.5 Location Condition**

2281 The location used for the routing of a call can be tested using the “LocationCondition”
2282 object, which is derived from the location-based condition elements specified in RFC 6772
2283 [108].

2284 The “LocationCondition” object MUST contain at least one “location” child object. The
2285 “LocationCondition” object evaluates to ‘true’ if any of its child “location” objects evaluate
2286 to ‘true’ when tested against the location used for routing of the call; i.e., multiple
2287 “location” child objects in a “LocationCondition” object are combined using a logical OR.

2288 Four members are defined for use in a “location” child object:

- 2289 • “lo”: A “location” child object MUST contain a “lo” member. The value is a PIDF-LO
2290 (properly escaped for inclusion in a JSON object).
- 2291 • “profile”: The “profile” member MUST exist and be set to “geodetic” or “civic”. This
2292 member indicates the location profile of the “location” object in which it appears.
2293 The semantics of the two location profiles, “geodetic” and “civic”, are derived from
2294 RFC 6772 [108], Sections [4.1](#) and [4.2](#). The profile describes under what conditions a
2295 “location” child object evaluates to ‘true’ (i.e., the “profile” value specifies how to
2296 test the PIDF-LO contained in the “lo” member against the location used for routing
2297 of the call).

- 2298 ○ “geodetic”: Using the semantics described in RFC 6772 [108] Section [4.1](#), this
2299 profile tests if the location used for routing the call is entirely within a
2300 specified circle.

2301 Note that if the location used for routing is provided in geodetic form, it could
2302 be specified as a point, arc-band, circle, or other shape, which must be
2303 entirely contained in the circle specified in the “lo” member for the “location”
2304 object to evaluate to ‘true’. If the call’s location for routing is not specified in
2305 geodetic form, the “location” object evaluates to ‘false’.

- 2306 ○ “civic”: Using the semantics described in RFC 6772 [108], Section [4.2](#), this
2307 profile tests the location used for routing the call against a set of civic address
2308 elements. The civic address elements of the PIDF-LO contained in the “lo”
2309 member are compared against the same elements of the location used for
2310 routing the call. Per RFC 6772 [108], Section [4.2](#), each civic address element
2311 in the “lo” member MUST exist in the location used for routing the call, and
2312 the values MUST be identical on an octet-by-octet basis (case-sensitive, no
2313 normalizations of abbreviations, prefixes, suffixes, etc.) If the call’s location
2314 for routing is not specified in civic form, the “location” object evaluates to
2315 ‘false’.

- 2316 • “label”: This member allows a human-readable description to be added to each
2317 “location” child object. It is OPTIONAL.
- 2318 • “lang”: This member contains a language tag providing further information for
2319 rendering of the content of the “label” member. It is OPTIONAL. The “lang” member
2320 MUST NOT be present unless the “label” member is also present.

2321 The “LocationCondition” and the “location” objects both allow extension points by using an
2322 embedded “extension” child object. If an extension is not understood by the entity
2323 evaluating the conditions, then this condition evaluates to ‘false’. A “LocationCondition” is
2324 considered ‘true’ if any of the “location” objects understood by the condition evaluator is
2325 ‘true’.

2326 **3.3.3.1.6 Call Suspicion Condition**

2327 “CallSuspicionCondition” tests the suspicion score of the call.

2328 If the SIP INVITE or MESSAGE contains a Call-Info header field with a ‘purpose’ parameter
2329 set to “emergency-CallSuspicion”, the value specified in the header field is considered an
2330 integer suspicion score.

2331 “CallSuspicionCondition” evaluates this suspicion score. The “CallSuspicionCondition” object
2332 has two members: “scoreFrom” and “scoreTo”, both of which MUST be present and MUST
2333 contain an integer value. The “CallSuspicionCondition” object evaluates to ‘true’ if the call’s
2334 suspicion score is greater than or equal to the value of “scoreFrom” and less than or equal
2335 to the value of “scoreTo”.

2336 If the call does not have a suspicion score, or the suspicion score cannot be determined as
2337 an integer, the suspicion score is considered to be zero.

2338 **3.3.3.1.7 Security Posture Condition**

2339 “SecurityPostureCondition” tests the current security posture of a service or agency.
2340 Security Posture is one part of Service State.

2341 The “SecurityPostureCondition” object has three members:

- “service”, which MUST exist. It contains one of Service Name, Service Identifier, or Agency Identifier. If specified by Service Name, it MUST be an entry in the Service Names Registry (Section 10.11) and MUST NOT be PSAP. The address to subscribe for Service State can be found using the Service/Agency Locator, which contains the subscription address for ServiceState.
- “condition”, which MUST exist and be set to “EQ” (equals) or “NE” (not equal to).
- “value”, which MUST exist and be set to an entry in the Security Posture Registry (see Section 10.18).

2350 The “SecurityPostureCondition” compares the current state of the Security Posture for the
2351 specified service or agency against the value specified in the “value” member. It evaluates
2352 to ‘true’ if the values are the same and the “condition” member is “EQ”, or the values are
2353 not the same and the “condition” member is “NE”, and ‘false’ otherwise. If the ESRP is

2354 unable to subscribe to the Service State of the specified service or agency at the specified
2355 FQDN, the security posture is treated as "Green".

2356 Presence of this condition implies that the ESRP subscribes to the Service State event
2357 package for the specified service or agency at the specified domain. Implementations MAY
2358 preprocess rulesets to arrange these subscriptions in advance.

2359 **3.3.3.1.8 Queue State Condition**

2360 "QueueStateCondition" tests the current state of a queue.

2361 The "QueueStateCondition" object has three members:

- 2362 • "queue": The "queue" member MUST exist and be set to a queue URI. The entity
2363 identified by the URI MUST support the QueueState event package (see Section
2364 4.2.1.3).

- 2365 • "condition": The "condition" member MUST exist and be set to "EQ" or "NE".

- 2366 • "value": The "value" member MUST exist and be set to an entry in the Queue State
2367 Registry (see Section 10.17).

2368 "QueueStateCondition" compares the current state of the specified queue against the
2369 value specified in the "value" member. It evaluates to 'true' if the values are the same and
2370 the "condition" member is "EQ", or the values are not the same and the "condition"
2371 member is "NE", and 'false' otherwise. If the ESRP is unable to subscribe to a queue's
2372 state, it is treated as "unreachable".

2373 Presence of this condition implies that the ESRP subscribes to queue state notification
2374 for the specified queue. Implementations MAY preprocess rulesets to arrange
2375 these subscriptions in advance.

2376 **3.3.3.1.9 LoST Service URN Condition**

2377 "LostServiceUrnCondition" causes a route query to be performed for a specified service
2378 URN using the location for routing of the call, and as a side effect sets the "Normal-
2379 NextHop" variable.

2380 The "LostServiceUrnCondition" object MUST contain one "urn" member, which MUST be set
2381 to a Service URN (e.g., starting with either "urn:service:" or "urn:emergency:service:").
2382 The condition causes a LoST query to be sent to the ECRF using the location for routing in
2383 the call and the specified Service URN. The "LostServiceUrnCondition" object evaluates to
2384 'true' if the query is successful and 'false' if not. If the query succeeds, the resulting URI is
2385 stored in the "Normal-NextHop" variable. The value of "Normal-NextHop" is available to the
2386 rule evaluation system in the Normal-NextHop Condition (Section 3.3.3.1.14) and the
2387 Invoke Policy Action (Section 3.3.3.2.5). If the LoST query fails, then the evaluation of this

[MM/DD/YYYY]

Page 85 of 675



2388 rule stops and the value of "Normal-NextHop" is undefined. (Since this rule's conditions
2389 evaluate to 'false', the next lower priority rule that evaluates to 'true' is performed.).
2390 When the LostServiceURN condition is used, the rule SHOULD contain an Invoke Policy
2391 Action (Section 3.3.3.2.5) using a PolicyType of "NormalNexthopRoutePolicy" (see section
2392 3.3.3.2.5).
2393 If the LoST response specifies an 'Expires' attribute of 'NO-CACHE', the ESRP MAY retain
2394 the value of "Normal-NextHop" for the entirety of rule evaluation for the call instead of re-
2395 querying the ECRF for every rule evaluation containing a LostServiceURN condition with the
2396 same query parameters. Otherwise, the ESRP MUST respect the expiry of the LoST
2397 response in processing this condition.

2398 Entirety of rule evaluation for the call means while the ESRP is evaluating the call, i.e., until
2399 the ESRP receives a 200 OK in response to its forward of the INVITE or MESSAGE, or until
2400 it generates a 600 Busy Everywhere towards the caller. Rule evaluation includes an Invoke
2401 Policy Action.

2402 **3.3.3.1.10 Service State Condition**

2403 The "ServiceStateCondition" tests the current Service State of service.

2404 The "ServiceStateCondition" object has three members:

- 2405 • "service", which MUST exist. It contains one of Service Name, Service Identifier or
2406 Agency Identifier. If specified by Service Name, it MUST be an entry in the Service
2407 Names Registry (Section 10.11) and MUST NOT be PSAP. The address to subscribe
2408 for Service State can be found using the Service/Agency Locator, which contains
2409 the subscription address for ServiceState.
- 2410 • "condition": The "condition" member MUST exist and be set to "EQ" or "NE".
- 2411 • "value": The "value" member MUST exist and be set to an entry in the Service State
2412 Registry (see Section 10.12).

2413 "ServiceStateCondition" compares the current service state of the specified service at the
2414 specified FQDN against the value specified in the "value" member. It evaluates to 'true' if
2415 the values are the same and the "condition" member is "EQ", or the values are not the
2416 same and the "condition" member is "NE", and 'false' otherwise. If the ESRP is unable to
2417 subscribe to the service state of the specified service at the specified FQDN, it is treated
2418 as "unreachable".

2419 Presence of this condition implies that the ESRP subscribes to Service state notification for
2420 the specified service. Implementations MAY preprocess rulesets to arrange these
2421 subscriptions in advance.

2422 **3.3.3.1.11 Call Source Condition**

2423 “CallSourceCondition” tests the call’s source network. CallSource (as defined in the Via
2424 header fields of the INVITE) is interpreted by the ESRP to ignore intra-ESInet Vias and
2425 other intermediaries. CallSource SHOULD be the ESRP’s best determination of the domain
2426 of the originating network that handled the call. If there is more than one, the last
2427 originating network or service provider prior to the ESInet SHOULD be used. If there are no
2428 originating networks, the ESRP uses the domain of the caller as the Call Source. Note that
2429 if the call is routed through multiple ESInets, it may be difficult to determine the CallSource
2430 within downstream ESInets. Since routing through multiple ESInets normally only occurs in
2431 misroute situations, rules using CallSource are unlikely to be effective in these
2432 circumstances.

2433 The “CallSourceCondition” object contains two members:

- 2434 • “operator” which MUST exist and be set to “EQ” (equals), “SS” (substring), or “NE”
2435 (not equal to). String comparisons are case-insensitive.
- 2436 • “content” which MUST exist. This is the value to be compared with the ESRP’s
2437 determined Call Source value using the test indicated by “operator”.

2438 **3.3.3.1.12 Body Part Condition**

2439 “BodyPartCondition” tests an element or member within an XML or JSON-formatted body
2440 part. This capability MAY be used to route based on parameters within a CAP message.
2441 (see also the CAP Condition in Section 3.3.3.1.17, which tests for specific CAP elements)

2442 “BodyPartCondition” contains four members:

- 2443 • “contentType” which MUST exist and be set to a MIME media (content) type and
2444 subtype (e.g., “text/plain”) in the IANA registry [181], although the condition is only
2445 effective for types that contain data formatted using XML or JSON.
- 2446 • “element” which MUST exist. This is the name of an element or member in the
2447 specified body part; this member is omitted when “operator” is “exists” and
2448 MANDATORY otherwise.
- 2449 • “operator” which MUST exist and be set to one of:
 - 2450 ○ “exists”,
 - 2451 ○ “missing”,
 - 2452 ○ “EQ” (equals),
 - 2453 ○ “SS” (substring),
 - 2454 ○ “NE” (not equal to),
 - 2455 ○ “GT” (greater than),
 - 2456 ○ “LT” (less than),
 - 2457 ○ “GE” (greater than or equal to), or

2458 ○ “LE” (less than or equal to).

2459 The “exists” operator evaluates to ‘true’ if the element or member specified in
2460 the “element” member exists in a body part of the specified type in the incoming
2461 message, and ‘false’ otherwise. The “missing” operator evaluates to ‘true’ if the
2462 element or member specified in the “element” member does not exist in any
2463 body part of the specified type in the incoming message, and ‘false’ otherwise. If
2464 the value in the body part element or member being processed does not
2465 evaluate to a number or date, GT/LT/GE/LE evaluate to ‘false’. String
2466 comparisons are case-insensitive.

2467 • “content”, which MUST exist. This is the value to be compared with the value of the
2468 specified element or member of the first body part of the specified type, using the
2469 specified comparison operator; this member is omitted when “operator” is “present”
2470 or “missing” and MANDATORY otherwise.

2471 Note that the operators “missing” and “exists” potentially test every body part of the
2472 specified type, while the comparison operators only test the first occurrence of the
2473 specified element or member in the first body part of the specified type in which the
2474 element or member appears.

2475 Example Body Part test:

2476 The following example tests an incoming message to see if the body contains a CAP
2477 payload with a <msg_status> element set to “Actual”, and a <severity> element set to
2478 “Extreme”, and a <certainty> element set to “High”:

```
2479           {
2480            {
2481              "conditionType": "BodyPartCondition",
2482              "contentType": "application/common-alerting-protocol+xml",
2483              "element": "msg_status",
2484              "operator": "EQ",
2485              "content": "Actual"
2486           },
2487           {
2488              "conditionType": "BodyPartCondition",
2489              "contentType": "application/common-alerting-protocol+xml",
2490              "element": "severity",
2491              "operator": "EQ",
2492              "content": "Extreme"
2493           },
2494           {
2495              "conditionType": "BodyPartCondition",
2496              "contentType": "application/common-alerting-protocol+xml",
2497              "element": "certainty",
2498              "operator": "EQ",
2499              "content": "High"
```

2499 }

2500 **3.3.3.1.13 Request URI Condition**

2501 “RequestUriCondition” tests the Request-URI in the call’s SIP INVITE or MESSAGE. A call’s
2502 Request-URI is most frequently “urn:service:sos”, but can contain child elements (e.g.,
2503 “urn:service:sos.ecall.automatic for a VEDS call placed due to a crash) or may be different
2504 for calls to an admin line, etc.

2505 The “RequestUriCondition” object contains two members:

- 2506 • “operator”, which MUST be present and MUST be set to one of “EQ” (equals), “SS”
2507 (substring), or “NE” (not equal to). String comparisons are case-insensitive.
- 2508 • “content”, which MUST be present. This is the value to be compared with the call’s
2509 Request-URI value using the test specified in “operator”.

2510 “RequestUriCondition” evaluates to ‘true’ if “operator” is “EQ” and the call’s Request-URI
2511 exactly matches the value in “content” aside from case, or “operator” is “SS” and the call’s
2512 Request-URI contains the value in “content” ignoring case, or “operator” is “NE” and the
2513 call’s Request-URI does not exactly match the value in “content” ignoring case. Otherwise,
2514 it evaluates to ‘false’.

2515 **3.3.3.1.14 Normal-NextHop Condition**

2516 “NormalNextHopCondition” tests the current value of the “Normal-NextHop” variable. The
2517 LoST Service URN Condition (Section 3.3.3.1.9) sets “Normal-NextHop” to the URI returned
2518 by the LoST query or marks it as undefined.

2519 The “NormalNextHopCondition” object contains two members:

- 2520 • “operator”, which MUST exist and be set to one of “EQ” (equals), “SS” (substring),
2521 or “NE” (not equal to). String comparisons are case-insensitive.
- 2522 • “content”, which MUST exist. This value is compared against the current value of the
2523 NormalNextHop variable using the test specified by the “operator”.

2524 “Normal-NextHop” is undefined at the start of every call, and remains undefined until a
2525 LoST Service URN Condition (Section 3.3.3.1.9) succeeds. When undefined, it evaluates to
2526 an empty string.

2527 **3.3.3.1.15 Incoming Queue Condition**

2528 “IncomingQueueCondition” tests the URI of the queue the call was received on.

2529 The “IncomingQueueCondition” object contains two members:

- 2530 • “operator” which MUST exist and be set to one of “EQ” (equals), “SS” (substring), or
2531 “NE” (not equal to). String comparisons are case-insensitive.

[MM/DD/YYYY]

Page 89 of 675



- 2532 • “content” which MUST exist. This is the value to be compared with the queue URI
2533 using the test indicated by “operator”.

2534 **3.3.3.1.16 SDP Offer Condition**

2535 This condition supports routing policy based on SDP offers. This allows construction of
2536 rules that route calls based on the media requested as well as the human interactive
2537 language of a media stream, as indicated in the SDP. SDP is used to negotiate media and
2538 optionally includes a list of human languages and directionality for each media line in the
2539 offer; the answer optionally contains a language per media line, typically a language from
2540 the media line in the offer.

2541 The “SdpOfferCondition” object has multiple members, which test for various media and
2542 languages in the SDP offer, and evaluate to ‘true’ or ‘false’.

2543 The tests “video”, “audio”, “rtt”, and “im” evaluate to ‘true’ if the message contains an SDP
2544 offer and the offer includes the corresponding media. In addition, “text” is equivalent to
2545 “rtt” or “im” (that is, true if either RTT or IM is offered). Within an “SdpOfferCondition”
2546 object, these tests are Boolean members that are set to ‘true’ to perform the test; they are
2547 omitted or set to ‘false’ to not perform the test. If the member is set to ‘true’, then the test
2548 evaluates to ‘true’ if the SIP INVITE contains an SDP offer and the offer includes the
2549 corresponding media, and evaluates to ‘false’ if the INVITE does not contain an SDP offer,
2550 or contains an SDP offer that does not include the corresponding media, or the call is a SIP
2551 MESSAGE (which does not contain SDP). If the member is set to ‘false’ or omitted, it is not
2552 evaluated.

2553 Note that session mode instant messaging uses SDP, while pager mode does not.

2554 SDP offers may include human interactive language attributes (RFC 8373) [173] containing
2555 language subtags listed in the IANA Registry [180]. In an SDP offer, each media offered
2556 may contain an ‘hlang-send’ and/or an ‘hlang-recv’ attribute. The ‘hlang-send’ attribute
2557 contains a list of one or more language(s) the offerer is willing to use when sending the
2558 media; ‘hlang-recv’ contains a list of one or more language(s) the offerer is willing to use
2559 when receiving the media. The list of languages is in preference order (first is most
2560 preferred). A media may be intended for interactive communication using a language in
2561 both directions or in one direction only.

2562 PSAPs can natively support more than one language (i.e., the PSAP may have bi- or multi-
2563 lingual call takers), and might be able to conference in external translation services for
2564 other languages. PSAPs natively support audio and text, and might natively support video

2565 or be able to conference in external relay services in cases in which a call requests video
2566 with sign language that did not originate via a relay service¹⁷.

2567 Communication with the caller is optimized when the caller's most-preferred language can
2568 be supported in each requested media. Using a caller's less-preferred language may hinder
2569 communication, but using an external translation service has its own set of non-optimal
2570 aspects.

2571 Languages are indicated by their subtag entry in the IANA registry [180]. While languages
2572 may include multiple subtags (allowing specification of various aspects such as dialects and
2573 writing system), matching uses the subtags specified in the conditions tests, which
2574 optimally use just the major subtag (such as "en" for English). For example, a rule with a
2575 condition testing for "en" would match an offer indicating "en-US" (for English as generally
2576 used in the U.S.), "en-UK" (for English as generally used in the U.K.), and "en-CA" (for
2577 English as generally used in Canada), while a rule testing for "en-scotland" (for the Scottish
2578 dialect of English) would not match any of the three.

2579 The "langAudio", "langText", "langVideo", "langRtt", and "langIm" members are arrays of
2580 strings; each array element contains one human interactive language (humintlang) (RFC
2581 8373) [173] subtag. A member evaluates as 'true' if any of its language subtags matches
2582 one of the languages (for either direction) in the offer for the corresponding media (audio,
2583 text, video, RTT, IM). This allows the rule to ask, "Does the offer request audio using
2584 Spanish?" for example, and it will evaluate to 'true' if, in the example, the offer requests
2585 audio using Greek, Spanish, French, or German. These conditions allow creating language-
2586 specific queues and routing to the appropriate queue based on the humintlang (RFC 8373)
2587 [173] marking of the offer.

2588 The "langAudioPref", "langTextPref", "langVideoPref", "langRttPref", and "langImPref" child
2589 objects test if a specific language is the most-preferred of the languages that match a set
2590 of languages offered for the corresponding media. Each of these objects contains two
2591 members: "langTest" is a string containing one language subtag; "langList" is an array of
2592 strings, each array element is a string containing one language subtag. The condition tests
2593 if the corresponding media (audio, text, video, RTT, IM) contains any of the "langList"
2594 languages (for either direction) and, if so, whether the "langTest" language is the most-
2595 preferred of the matching languages. This allows the rule to ask, "Is French the most-
2596 preferred language of the set (English, French, Spanish) for audio in the offer?" It
2597 evaluates to true, in this example, if the offer specifies that Algonquian, French, and
2598 English (in that order) are available for an audio media stream. If, in contrast, the offer

¹⁷ While calls requiring relay service normally originate via the service, a call might originate directly, (e.g., in the case of a visitor from a country in which calls are placed directly).

2599 specified that English, Algonquian, and French (in that order) were available, the test
2600 would evaluate to false, since of the set (English, French, Spanish), English and French
2601 match, but of those, French is not the most-preferred. These conditions allow creating
2602 language-specific queues and routing to the appropriate queue based on the humintlang
2603 (RFC 8373) [173] marking of the offer, matching the most-preferred language of the caller
2604 with the languages natively supported at the PSAP.

2605 The "SdpOfferCondition" object has the following members:

2606 Boolean members: when set to 'true', evaluates as 'true' if the SDP contains the
2607 indicated media, and as 'false' if the SDP does not contain the indicated media:

- 2608 ○ "video": for video media
- 2609 ○ "audio": for audio media
- 2610 ○ "rtt": for RTT
- 2611 ○ "im": for IM
- 2612 ○ "text": for either RTT or IM

2613 The "video", "audio", "rtt", and "im" members MAY each occur; the "text" member
2614 MAY occur only if neither "rtt" nor "im" occurs.

2615 String array members: each member is an array of strings, each element of which is a
2616 single language subtag; the member evaluates as 'true' if the SDP contains the
2617 indicated media using any of the languages in the array, and 'false' otherwise:

- 2618 ○ "langVideo": for video
- 2619 ○ "langAudio": for audio
- 2620 ○ "langRtt": for RTT
- 2621 ○ "langIm": for IM
- 2622 ○ "langText": for either RTT or IM

2623 Child objects: each MUST contain the following two members:

- 2624 ○ "langList": array of strings, each element is a language subtag.
- 2625 ○ "langTest": string containing a language subtag.

2626 The child objects tests if the SDP includes the corresponding media using any of a set
2627 of languages of which the specified language is the most preferred:

- 2628 ○ "langVideoPref": for video
- 2629 ○ "langAudioPref": for audio
- 2630 ○ "langRttPref": for RTT
- 2631 ○ "langImPref": for IM
- 2632 ○ "langTextPref": for either RTT or IM

2633 Each of the above "lang...Pref" child objects evaluates as 'true' if:

- 2634 ○ the SDP includes the corresponding media, and
2635 ○ the corresponding media uses any of the “langList” languages, and
2636 ○ the “langTest” language tag is the most-preferred of the matching languages

2637 Multiple members and/or child objects MAY occur in a single “SdpOfferCondition” object;
2638 they are interpreted with an implicit logical OR: if any evaluate to ‘true’, the condition
2639 evaluates to ‘true’.

2640 **3.3.3.1.17 CAP Condition**

2641 CAP message parameters may be tested with the CAP Condition. (In addition to the tests in
2642 this condition, which test for certain specific CAP elements, any CAP element can also be
2643 tested using the more general Body Part Condition described in Section 3.3.3.1.12).

2644 The following child objects are defined for use within a “CapCondition” object:

- 2645 • “Identifier”,
2646 • “Sender”,
2647 • “Address”,
2648 • “InfoEventCode”,
2649 • “InfoValueName”.

2650 Each of these child objects contains two members:

- 2651 • “operator”, which MUST exist and be set to one of “EQ” (equals), “SS” (substring),
2652 or “NE” (not equal to). String comparisons are case-insensitive.
2653 • “content”, which MUST exist. This is the string that is compared with the
2654 corresponding element of the CAP component using the test indicated by “operator”.

2655 The above child objects are OPTIONAL, but at least one MUST occur. Multiple child objects
2656 MAY occur within a “CapCondition” object; they are interpreted with an implicit logical
2657 AND: if any evaluate to ‘false’, the condition evaluates to ‘false’.

2658 The “CapCondition” object MAY contain the “NonInteractive” Boolean member. If this
2659 member exists and is set to ‘true’, it evaluates as ‘true’ if the CAP occurs in a non-Interactive
2660 call (i.e., a SIP MESSAGE with CAP body), and as ‘false’ if the call is a SIP INVITE. If
2661 “NonInteractive” does not occur or is set to ‘false’, it has no effect on the evaluation of the
2662 “CapCondition” object. If “NonInteractive” evaluates to ‘false’ (i.e., it occurs and is set to
2663 ‘true’ but the CAP is in an INVITE), the “CapCondition” object evaluates to ‘false’ (even if all
2664 child objects evaluate to ‘true’).

2665 If the message does not contain a CAP body, or the CAP does not contain the indicated
2666 element, the “CapCondition” object evaluates to ‘false’.

2667 **3.3.3.1.18 CallingNumberVerificationStatus condition**

2668 This condition allows testing the outcome of any validation of the calling number that may
2669 have been done by the Secure Telephone Identity Verification Service (STI-VS) FE.

2670 The "CallingNumberVerificationStatusCondition" object has two members:

- 2671 • "operator", which MUST exist and be set to either "EQ" or "NE"
2672 • "value", which MUST exist and be set to an entry from the 3GPP 7.2A.20 "verstat"
2673 tel URI parameter definition (currently defined values "TN-Validation-Passed", "TN-
2674 Validation-Failed" and "No-TN-Validation")

2675 The evaluation of this condition compares the result of calling number verification with the
2676 state contained in "value", using the test indicated by "operator".

2677 If the call does not contain a "verstat" parameter, the call's verification status is considered
2678 to be "No-TN-Validation".

2679 **3.3.3.2 Actions**

2680 The conditions specified above are the "if" part of rules; the actions specified below are the
2681 "then" part. The actions within a rule determine which operations the ESRP performs in
2682 handling a call. Actions cause various operations to be executed. As described above, more
2683 than one rule might match; of the rules whose conditions match, the rule with the highest
2684 priority value is executed. Some actions do not directly affect the call (e.g., looking up a
2685 route, sending notifications, logging messages); other actions forward a call to its next
2686 point (the Route action), reject a call (the Busy action), or switch control to a different rule
2687 set (the Invoke Policy action, which then evaluates that set of rules). Rules MUST NOT
2688 contain more than one Route, Busy or Invoke Policy action, or a combination of Route,
2689 Busy or Invoke Policy actions.

2690 "Actions" is an array of action objects, as described below. An action object contains the
2691 following members:

- 2692 • "actionType": a string which MUST exist and be set to the specific action type.
2693 • "description": an OPTIONAL string containing a description of the action.
2694 • Other action-specific members as described in the below subsections.

2695 **3.3.3.2.1 Route Action**

2696 This action forwards the call (as its SIP message) to a specific URL. If the final response to
2697 this forwarded INVITE/MESSAGE is not 200 OK, then the rule MUST be treated as if it
2698 evaluated to 'false'.

2699 The "routeAction" object has three members:

- 2700 • “recipientUri”, which MUST exist and contain a URI that will become the Route
2701 header field for the outgoing SIP message (the Request-URI is normally a service
2702 URN such as “urn:service:sos”)
2703 • “rnaTimer”, which is OPTIONAL. This is the Ring No Answer timer; it is the time in
2704 seconds the ESRP will wait for a final response. If this member is omitted, the ESRP
2705 MUST use a provisioned value; a suggested default for the provisioned value is 20
2706 seconds.
2707 • “cause”, which is OPTIONAL. This contains the value to be used within the Reason
2708 parameter of the topmost History-Info header field for the outgoing SIP message.
2709 The value MUST be an entry from the RouteCause Registry (Section 10.20)
- 2710 The ESRP SHALL implement a Ring No Answer timer, which SHALL be set to the “rnaTimer”
2711 value if present, or the provisioned default if omitted. If the timer expires before the final
2712 response to the forwarded SIP message is received, the Route action fails and is treated as
2713 if the rule condition evaluated to ‘false’ (i.e., the rule set is reevaluated and the highest
2714 priority rule whose conditions evaluated to ‘true’ is executed).
- 2715 A Route Action can fail for reasons other than Ring No Answer timeout (e.g., because the
2716 destination queue becomes unreachable, the next hop rejected the call with an error
2717 status, or the call times-out before it is answered). In such cases, the ESRP MUST set its
2718 queue state for the target queue to “Unreachable” and MUST reevaluate the ruleset for the
2719 call. Note that its queue state remains “Unreachable” until a queue state notification resets
2720 it. The ESRP SHOULD set a minimum rate for queue state notifications to refresh state
2721 frequently.
- 2722 When routing a call (as a result of a RouteAction or other reason), a RouteLogEvent is
2723 generated to note the route, and an optional text string “cause” stating why it chose the
2724 route.
- 2725 **3.3.3.2.2 Busy Action**
- 2726 The “BusyAction” object causes a final status of 600 Busy Everywhere to be sent toward
2727 the caller.
- 2728 **3.3.3.2.3 Notify Action**
- 2729 This action sends a NOTIFY message to entities subscribing to the ESRP’s “ESRPnotify”
2730 event package for the specified “eventCode”. This may be used, for example, to advise
2731 other entities that calls are being diverted, etc.
- 2732 The “NotifyAction” object has the following members:

- 2733 • “recipient”, which is OPTIONAL. When present, it MUST be either a URI or a service
2734 URN. This member is used to notify a single entity registered for the “eventCode”. If
2735 “recipient” is a URI, notification is generated for that specific recipient. If “recipient”
2736 is a service URN, the ECRF is used to map the service URN to a URI, and a
2737 notification is generated for that URI. Recipients MUST have subscribed for the
2738 “eventCode” to get the notification. If “recipient” is omitted, notification is generated
2739 for all subscribers to the “eventCode”. In all cases, notifications are subject to per-
2740 recipient throttling.
- 2741 • “eventCode”, which MUST exist and be set to a value contained in the
2742 EsrpNotifyEventCodes registry (Section 10.19).
- 2743 • “urgency”, which MUST exist and be set to an integer value from 0 and 100 where 0
2744 is no urgency and 100 is the highest possible urgency.
- 2745 • “comment”, which is OPTIONAL. If present, it is a text string that is included in the
2746 “Comment” field of the NOTIFY message.

2747 **3.3.3.2.4 Log Message Action**

2748 This action causes a RouteRuleMsgLogEvent to be generated. This is primarily useful for
2749 debugging; implementations MAY provide a mechanism to switch logging of such messages
2750 on or off (i.e., when the mechanism is switched off, all occurrences of “LogAction” are
2751 ignored).

2752 The “LogAction” object contains one member: “message”, which is OPTIONAL.

2753 The generated RouteRuleMsgLogEvent contains the policy owner, policy type, policy ID if
2754 policyType is “OtherRoutePolicy”, policy queue name if policyType is
2755 “OriginationRoutePolicy” or “NormalNextHopRoutePolicy”, rule ID, rule priority, and the
2756 contents of the “message” member if present.

2757 **3.3.3.2.5 Invoke Policy Action**

2758 Invoke Policy Action causes the specified policy routing ruleset to be evaluated. It is
2759 typically used to evaluate the policy ruleset associated with the URI received from a LoST
2760 query, allowing calls to be processed according to the policy of the next hop. This action
2761 may also be used to structure the routing rules of an entity as desired (e.g., into general
2762 and specific rulesets).

2763 The “InvokePolicyAction” object has the following members:

- 2764 • “policyType”, which MUST exist and be set to one of the following subset of
2765 values from the Policy Types Registry Section 10.33:
 - OrginationRoutePolicy

- 2767 ○ NormalNexthopRoutePolicy
2768 ○ OtherRoutePolicy
2769 • “policyId”, which MUST exist when “policyType” is “OtherRoutePolicy” and MUST
2770 NOT exist otherwise.
2771 • “policyQueueName”

2772 The ESRP fetches a policy from the Policy Store using the specified “policyType”, no owner,
2773 and a policyQueueName/policyId dependent on “policyType”:

- 2774 • For “OriginationRoutePolicy”, policyQueueName is the queue the call arrived on and
2775 policyId is not used.
2776 • For “NormalNexthopRoutePolicy”, the policyQueueName is the value of the “Normal-
2777 NextHop” variable (as a result of a LostServiceUrnCondition evaluation as described
2778 in Section 3.3.3.1.9) and policyId is not used.
2779 • For “OtherRoutePolicy”, the policyId is the content of the “policyId” specified in the
2780 Invoke Policy Action and policyQueueName is not used.

2781 If “Normal-NextHop” is undefined when an Invoke Policy action specifying
2782 “NormalNexthopRoutePolicy” is evaluated, or if the policy cannot be retrieved for any
2783 reason, the rule fails and is treated as if the rule condition evaluated to ‘false’. “Normal-
2784 NextHop” is undefined if there is no Lost Service URN Condition in the rule, or the LoST
2785 query from the Lost Service URN Condition failed to result in a route.

2786 3.3.3.3 PRR Ruleset Examples

```
2787 {  
2788   "description": "Call is probably spam.",  
2789   "id": "AA56i12",  
2790   "priority": 7,  
2791  
2792   "conditions":  
2793   [  
2794     {  
2795       "conditionType": "CallSuspicionCondition",  
2796       "scoreFrom": 70,  
2797       "scoreTo": 100  
2798     }  
2799   ],  
2800  
2801   "actions":  
2802   [  
2803     {  
2804       "actionType": "RouteAction",  
2805       "recipientUri": "sip:special-treatment@psap.example.gov"  
2806     }  
]
```

[MM/DD/YYYY]

Page 97 of 675



```
2807     ]
2808 }
2809
2810
2811 {
2812     "description": "Rule for handling a SIP msg containing a CAP
2813     payload.",
2814     "id": "AA56i11",
2815     "priority": 6,
2816
2817     "conditions":
2818     [
2819         {
2820             "conditionType": "MimeTypeCondition",
2821             "mimeTypeList": [ "application/common-alerting-protocol+xml" ]
2822         }
2823     ],
2824
2825     "actions":
2826     [
2827         {
2828             "actionType": "routeAction",
2829             "recipientUri": "sip:psap@home.example.gov"
2830         }
2831     ]
2832 }
2833
2834
2835 {
2836     "description": "Rule to consider time and queue state.",
2837     "id": "AA56i10",
2838     "priority": 5,
2839
2840     "conditions":
2841     [
2842         {
2843             "conditionType": "QueueStateCondition",
2844             "queue": "sip:answering-machine@home.foo-bar.com",
2845             "condition": "EQ",
2846             "value": "Active"
2847         },
2848         {
2849             "conditionType": "TimePeriodCondition",
2850             "dateStart": "19970105T083000",
2851             "timeStart": "2200",
2852             "timeEnd": "0800",
2853             "weekdayList": "MO, TU, WE, TH, FR",
2854             "dateEnd": "19991230T183000"
2855         }
2856     ],
2857 }
```

```
2858     "actions":  
2859     [  
2860         {  
2861             "actionType": "routeAction",  
2862             "recipientUri": "sip:answering-machine@home.foo-bar.com"  
2863         }  
2864     ]  
2865 }  
2866  
2867
```

2868 The following example ruleset assumes a PSAP that natively supports voice and text, for
2869 both English and French. The ruleset checks if calls request a language and media
2870 supported natively; if so, calls are sent to specific queues for language and media; if not,
2871 calls are sent to a queue where an agent can authorize the use of third-party translation
2872 and/or relay services.
2873
2874
2875 {
2876 "description": "
2877 ; -----
2878 ; If call requires language not supported natively,
2879 ; send to the translation approval queue:
2880 ; -----",
2881
2882 "id": "BB67m100",
2883 "priority": 100,
2884
2885 "conditions":
2886 [
2887 {
2888 "negation": true,
2889 "conditionType": "SdpOfferCondition",
2890 "langAudio": "en",
2891 "langText": "en",
2892 "langAudio": "fr",
2893 "langText": "fr"
2894 }
2895],
2896
2897 "actions":
2898 [
2899 {
2900 "actionType": "routeAction",
2901 "recipientUri": "sip:trans-approv@psap.example.gov"
2902 },
2903 {
2904 "actionType": "logAction",
2905 "message": "Call requires language not natively supported"
2906 }
2907 }

```
2907     ]
2908 }
2909
2910
2911 {
2912     "description": "
2913     ; -----
2914     ; If call receives translation approval, send to
2915     ; the Policy Routing Rules queue:
2916     ; -----",
2917
2918     "id":      "AA56i222",
2919     "priority": 10,
2920
2921     "conditions":
2922     [
2923         {
2924             "conditionType": "LostServiceUrnCondition",
2925             "urn":          "urn:emergency:service:sos.psap"
2926         }
2927     ],
2928
2929     "actions":
2930     [
2931         {
2932             "actionType":   "InvokePolicyAction",
2933             "policyType":  "NormalNexthopRoutePolicy"
2934         }
2935     ]
2936 }
2937
2938
2939
2940 {
2941     "description": "
2942     ; -----
2943     ; If call requires media not supported natively, it
2944     ; should have been initiated via a third-party relay
2945     ; service; since it wasn't, send to the special
2946     ; handling queue:
2947     ; -----",
2948
2949     "id":      "BB67m090",
2950     "priority": 90,
2951     "negation": true,
2952
2953     "conditions":
2954     [
2955         {
2956             "conditionType": "SdpOfferCondition",
2957             "audio":        true,
2958             "text":         true
2959         }
2960     ]
2961 }
```

```
2958         }
2959     ],
2960
2961     "actions":
2962     [
2963         {
2964             "actionType": "routeAction",
2965             "recipientUri": "sip:special-handling@psap.example.gov"
2966         },
2967         {
2968             "actionType": "logAction",
2969             "message": "Call requires media not natively supported"
2970         }
2971     ]
2972 }
2973
2974
2975 {
2976     "description": "
2977     ; -----
2978     ; If French is the most-preferred of (English, French),
2979     ; send to French queue
2980     ;
2981     ; -----",
2982
2983     "id": "BB67m080",
2984     "priority": 80,
2985
2986     "conditions":
2987     [
2988         {
2989             "conditionType": "SdpOfferCondition",
2990             "langAudioPref":
2991                 {
2992                     "langTest": "fr",
2993                     "langList": [ "en", "fr" ]
2994                 },
2995             "langTextPref":
2996                 {
2997                     "langTest": "fr",
2998                     "langList": [ "en", "fr" ]
2999                 }
3000     ],
3001
3002     "actions":
3003     [
3004         {
3005             "actionType": "routeAction",
3006             "recipientUri": "sip:french@psap.example.gov"
3007         },
3008         {
```

```
3009             "actionType": "logAction",
3010             "message":     "French is most-preferred among English and
3011             French"
3012         }
3013     ]
3014 }
3015
3016
3017 {
3018     "description": "
3019     ; -----
3020     ; If English is the most-preferred of (English, French),
3021     ; send to English queue
3022     ; -----
3023
3024     "id":          "BB67m070",
3025     "priority": 70,
3026
3027     "conditions":
3028     [
3029         {
3030             "conditionType": "SdpOfferCondition",
3031             "langAudioPref":
3032             {
3033                 "langTest": "en",
3034                 "langList": [ "en", "fr" ]
3035             },
3036             "langTextPref":
3037             {
3038                 "langTest": "en",
3039                 "langList": [ "en", "fr" ]
3040             }
3041         }
3042     ],
3043
3044     "actions":
3045     [
3046         {
3047             "actionType": "routeAction",
3048             "recipientUri": "sip:english@psap.example.gov"
3049         },
3050         {
3051             "actionType": "logAction",
3052             "message":     "English is most-preferred among English and
3053             French"
3054         }
3055     ]
3056 }
3057
3058
3059 }
```

```
3060     "description": "  
3061         ; -----  
3062         ; Can't-get-here rule that should never be executed.  
3063         ;  
3064         ; If this rule executes, we have an error, since the  
3065         ; previous rules should have caught all cases. This rule  
3066         ; has no <conditions> element, hence is considered  
3067         ; to have a <conditions> that evaluates to true.  
3068         ; -----"  
3069  
3070     "id": "BB67m000",  
3071     "priority": 0,  
3072  
3073     "actions":  
3074     [  
3075         {  
3076             "actionType": "routeAction",  
3077             "recipientUri": "special-handling@psap.example.gov"  
3078         },  
3079         {  
3080             "actionType": "logAction",  
3081             "message": "ERROR: can't-get-here rule triggered"  
3082         },  
3083         {  
3084             "actionType": "logAction",  
3085             "message": "===== File discrepancy report ====="  
3086         }  
3087     ]  
3088 }  
3089  
3090
```

3091 To illustrate the effects of these rules, here are a few example SDP offers (only the most
3092 directly relevant portions of the SDP block are shown):

3093 An offer requesting spoken Spanish both ways (most preferred), spoken Basque both ways
3094 (second preference), or spoken English both ways (third preference):

```
3095 m=audio 49250 RTP/AVP 20  
3096 a=hlang-send:es eu en  
3097 a=hlang-recv:es eu en
```

3098
3099 In the immediately preceding ruleset:

- 3100 • The conditions of rule BB67m100 are 'false':
 - 3101 o "langAudio" for "en" is 'true' (since audio is offered and "en" is one of the
3102 offered languages for audio);
 - 3103 o "langText" for "en" is 'false' (since text is not offered)
 - 3104 o "langAudio" for "fr" is 'false' (since "fr" is not one of the offered languages for
3105 audio);
 - 3106 o "langText" for "fr" is 'false' (since text is not offered)

- 3107 ○ the SDP Offer condition evaluates to 'true'
3108 ○ The "conditions" evaluation is reversed by the "negation" element;
3109 • The conditions of rule AA56i222 are 'true' (assuming the LoST query succeeds);
3110 • The conditions of rule BB67m090 are 'false':
3111 ○ "audio" is 'true' (since audio is offered)
3112 ○ "text" is 'false' (since text is not offered)
3113 ○ the SDP Offer condition evaluates to 'true'
3114 ○ The "conditions" evaluation is reversed by the "negation" element;
3115 • The conditions of rule BB67m080 are 'false':
3116 ○ "langAudioPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to
3117 'false' (since the offer for audio does not contain "fr");
3118 ○ "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to
3119 'false' (since the offer does not contain text);
3120 • The conditions of rule BB67m070 are 'true':
3121 ○ "langAudioPref" with "langTest" "en", and "langList" "en and "fr" evaluates to
3122 'true' (since the offer requests "es eu en" in that order and the only offered
3123 language for audio in the set ("en", "fr") is "en", it is first (and only) in the
3124 matching set of "en");
3125 ○ "langTextPref" with "langTest" "fr", and "langList" "en fr" evaluates to 'false'
3126 (since the offer does not contain text);
3127 • The conditions of rule BB67m000 are 'true', as the conditions are omitted;

3128 So, three rules have conditions that evaluate to 'true':

- 3129 • BB67m070: "priority" 70
3130 • AA56i222: "priority" 10
3131 • BB67m000: "priority" 0.

3132 Since the highest (largest) priority matching value rule is executed, BB67m070 is
3133 executed, sending the call to the "sip:english@psap.example.gov" queue, and logging a
3134 message of "English is most-preferred among English and French".

3135 An offer requesting written Greek both ways:

3136 m=text 45020 RTP/AVP 103 104
3137 a=hlang-send:gr
3138 a=hlang-recv:gr

3139 In the immediately preceding ruleset:

- 3140 • The conditions of rule BB67m100 are 'true':
3141 ○ "langAudio" for "en" is 'false' (since audio is not offered);
3142 ○ "langText" for "en" is 'false' (since "en" is not one of the offered languages for
3143 text)
3144 ○ "langAudio" for "fr" is 'false' (since audio is not offered languages);
3145 ○ "langText" for "fr" is 'false' (since "fr" is not one of the offered languages for
3146 text)

- 3147 ○ the SDP Offer condition evaluates to 'false'
3148 ○ The "conditions" evaluation is reversed by the "negation" element;
3149 • The conditions of rule AA56i222 are 'true' (assuming the LoST query succeeds);
3150 • The conditions of rule BB67m090 are 'false':
3151 ○ "audio" is 'false' (since audio is not offered)
3152 ○ "text" is 'true' (since text is offered)
3153 ○ the SDP Offer condition evaluates to 'true'
3154 ○ The "conditions" evaluation is reversed by the "negation" element;
3155 • The conditions of rule BB67m080 are 'false':
3156 ○ "langAudioPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to
3157 'false' (since audio is not offered);
3158 ○ "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to
3159 'false' (since the text offer does not include "en" nor "fr");
3160 • The conditions of rule BB67m070 are 'false':
3161 ○ "langAudioPref" with "langTest" "en", and "langList" "en" and "fr" evaluates to
3162 'false' (since the offer does not include audio);
3163 ○ "langTextPref" with "langTest" "fr", and "langList" "en" and "fr" evaluates to
3164 'false' (since the text offer does not include "en" nor "fr");
3165 • The conditions of rule BB67m000 are 'true', as the conditions are omitted.

3166 So, two rules have conditions that evaluate to 'true':

- 3167 • BB67m100, "priority" 100
- 3168 • AA56i222, "priority" 10
- 3169 • BB67m000, "priority" 0.

3170 Since the highest (largest) priority matching value rule is executed, BB67m100 is executed,
3171 sending the call to the "sip:trans-approv@psap.example.gov" queue, and logging a
3172 message of "Call requires language not natively supported".

3173 An offer requesting spoken Cree both ways (most preferred), spoken English both ways
3174 (second preference), or spoken French both ways (third preference):

```
3175 m=audio 49250 RTP/AVP 20
3176 a=hlang-send:cr en fr
3177 a=hlang-recv:cr en fr
```

3178 In the immediately preceding ruleset:

- 3179 • The conditions of rule BB67m100 are 'false':
 - 3180 ○ "langAudio" for "en" is 'true' (since "en" is one of the offered languages for
3181 audio);
 - 3182 ○ "langText" for "en" is 'false' (since text is not offered)
 - 3183 ○ "langAudio" for "fr" is 'true' (since "fr" is one of the offered languages for
3184 audio);
 - 3185 ○ "langText" for "fr" is 'false' (since text is not offered)
 - 3186 ○ the SDP Offer condition evaluates to 'true'

- 3187 ○ The “conditions” evaluation is reversed by the “negation” element;
- 3188 • The conditions of rule AA56i222 are ‘true’ (assuming the LoST query succeeds);
- 3189 • The conditions of rule BB67m090 are ‘false’:
- 3190 ○ “audio” is ‘true’ (since audio is offered)
- 3191 ○ “text” is ‘false’ (since text is not offered)
- 3192 ○ the SDP Offer condition evaluates to ‘true’
- 3193 ○ The “conditions” evaluation is reversed by the “negation” element;
- 3194 • The conditions of rule BB67m080 are ‘false’:
- 3195 ○ “langAudioPref” with “langTest” “fr”, and “langList” “en” and “fr” evaluates to ‘false’ (since the offer for audio contains both “en” and “fr”, but lists “fr” second among those two);
- 3196 ○ “langTextPref” with “langTest” “fr”, and “langList” “en” and “fr” evaluates to ‘false’ (since the offer does not contain text);
- 3197 • The conditions of rule BB67m070 are ‘true’:
- 3198 ○ “langAudioPref” with “langTest” “en”, and “langList” “en and “fr” evaluates to ‘true’ (since the offer requests “cr en fr” in that order, the offered language for audio in the set (“en”, “fr”) are both “en” and “fr”, and “en” is first in the matching set of (“en”, “fr”);
- 3199 ○ “langTextPref” with “langTest” “fr”, and “langList” “en fr” evaluates to ‘false’ (since the offer does not contain text);
- 3200 • The conditions of rule BB67m000 are true, as the conditions are omitted;

3201 So, three rules have conditions that evaluate to true:

- 3202 • BB67m070: “priority” 70
- 3203 • AA56i222: “priority” 10
- 3204 • BB67m000: “priority” 0.

3205 Since the highest (largest) priority matching value rule is executed, BB67m070 is executed, sending the call to the “sip:english@psap.example.gov” queue, and logging a message of, “English is most-preferred among English and French”.

3206 3.4 LoST

3207 LoST (RFC 5222 [48]) is the protocol that is used for several functions:

- 3208 • Call routing: LoST is used by the ECRF as the protocol to route all emergency calls
- 3209 both to¹⁸ and within the ESInet.

18 LoST must be used within an ESInet to route calls. It is RECOMMENDED that originating networks also use LoST to route calls to the entry ESRP, but they MAY use appropriate local functions provided that calls are routed to the same ESRP as they would be if LoST were used to the authoritative ECRF.

- 3220 • Location validation: LoST is used by the LVF as the protocol to validate civic location
3221 information for every call origination end device prior to any potential use for
3222 emergency call routing.
3223 • Retrieving URIs to support the retrieval of information based on a location such as
3224 Additional Data about that location and Agency Locator records.
3225 • Retrieving lists of services available at a location.

3226 The normative reference that defines the protocol is RFC 5222 [48], extended by draft-
3227 ercit-lost-planned-changes [178]. The text in this section that defines LoST protocol
3228 operations should be considered informative, and any discrepancies are resolved by RFC
3229 5222 text. The text below does contain limitations and specific application of LoST
3230 operations that are normative.

3231 **3.4.1 Emergency Call Routing using LoST**

3232 All SIP-based emergency calls pass location information either by value (PIDF-LO) or by
3233 reference (Location URI) plus a Service URN to an Emergency Service Routing Proxy
3234 (ESRP) to support routing of emergency calls. The ESRP passes the Service URN and
3235 location information¹⁹ via the LoST interface to an Emergency Call Routing Function
3236 (ECRF), which determines the next hop in routing a call to the requested service. The ECRF
3237 performs the mapping of the call's location information and requested Service URN to, for
3238 example, a "PSAP URI" by querying its data and then returning the URI provided. Using the
3239 returned URI and other information (time of day, PSAP state, etc.), the ESRP then applies
3240 policy from a Policy-based Routing Function (PRF) to determine the appropriate routing
3241 URIs. This URI is the "next hop" in the call's routing path that could be an ESRP URI
3242 (intermediate hop), a PSAP URI (final hop), or even a call-taker (see Section 4.3 for a more
3243 detailed functional explanation of the i3 ECRF).

3244 The service URN used to query the ECRF by an ESRP is obtained by provisioning of the
3245 "origination policy" of the queue that the call is received on at the ESRP (see Section
3246 4.2.1.1). The response of the ECRF is determined by provisioning of the service boundary
3247 layers, which specify the URN they apply to (see Section 4.3.1). Thus, ECRFs (and ESRPs)
3248 are not hard-coded with any specific URNs, but the provisioning of the policy in the ESRP
3249 MUST match the provisioning of the service boundaries in the ECRF.

3250 A single emergency call can be routed by one or more ESRPs within the ESInet, resulting in
3251 use of the LoST interface once per hop as well as once by the terminating PSAP.

19 If an element using LoST receives location by reference, it MUST dereference the URI to obtain the value prior to querying the LoST server. The LoST server does not accept location by reference.

3252 Note that the term “PSAP URI” is used within the LoST protocol definition to refer to the
3253 URI returned from the service URN “urn:service:sos”. In NG9-1-1, the URI returned may
3254 not be that of a PSAP, but instead may route to a BCF or ESRP.

3255 **3.4.2 Location Validation**

3256 Location validation is the validation of civic address-based location information against an
3257 authoritative GIS database containing only valid civic addresses obtained from 9-1-1
3258 Authorities. Location validation is performed by the i3 LVF. “Validating” a location in
3259 NG9-1-1 means querying the Location Validation Function (Section 4.3) to determine if the
3260 location is suitable for use (specifically, if the location can be used to accurately route the
3261 call and dispatch responders). To be “LVF-Valid”, thus “routable”, a queried location using
3262 “urn:service:sos”, or “urn:emergency:service:sos”, or subservices of them MUST: 1) return
3263 a valid indication (i.e., no fields in the <invalid> list) from an LVF query with the location;
3264 and, 2) MUST yield a single <mapping> element in the LoST response. In general, this
3265 means the fields supplied in the LoST query match exactly one location (one address point
3266 in the site/structure layer, or a valid house number in a road segment layer).

3267 We differentiate between the ECRF and LVF even though they have identical provisioning
3268 and identical interfaces because the ECRF query is made at call time while the LVF query is
3269 made during provisioning of a location in a LIS, and thus is non-real-time. LoST servers
3270 discovered using the ‘LoST’ service tag might refuse to perform location validation (e.g.,
3271 when under stress). The ‘LoST-Validation’ service tag [224] provides a way to identify LoST
3272 servers designated to perform location validation.

3273 The LVF MUST support the validation of location around planned changes as defined by
3274 draft-ecrit-lost-planned-changes [178].

3275 **3.4.3 <findService> Request**

3276 The “civic” and “geodetic-2d” profiles are baseline profiles defined in RFC 5222 [48].
3277 Emergency calls are expected to use only these profiles. NG9-1-1 conformant LoST servers
3278 are NOT REQUIRED to support any location profiles beyond the baseline profiles defined in
3279 RFC 5222.

3280 The ECRF/LVF SHOULD expect to receive any of the PIDF-LO elements described in the
3281 NENA Civic Location Data Exchange Format (CLDXF) [77] document within a civic location.

3282 The LoST interface allows a geo-location to be expressed as a point or one of a number of
3283 defined “shapes” such as circle, ellipse, arc-band, or polygon. ECRFs MUST be able to
3284 handle all of these shapes.

3285 The “service” element identifies the service requested by the client. Valid service names
3286 MUST be “urn:service:sos” or one of its sub-services for ECRF and LVF queries used by

3287 originating networks or devices for emergency calls. For internal ECRFs used by entities
3288 within the ESInet to route calls, the <service> element MAY be a service URN beginning
3289 with "urn:emergency:service". ECRF implementations MUST support
3290 "urn:emergency:service". The use of such service URNs is dependent on provisioning of
3291 service boundary layers in the GIS. Service URNs are defined in Section 10.2.

3292 The optional attribute to request validation occurs in a query and indicates whether
3293 location validation should be performed and is currently conditioned on the <location>
3294 element containing a civic address; (i.e., it is an error to request location validation for a
3295 geodetic coordinates-based location in RFC 5222). A request for validation MAY include
3296 elements defined in draft-ecrit-lost-planned-changes [178] to allow clients to validate
3297 locations against planned changes in the GIS data. Entities inside the ESInet MUST specify
3298 recursion by setting the recursive attribute in the <findService> request to 'true' and all
3299 ECRFs and LVFs MUST implement and perform recursion when requested to help mitigate
3300 the effect of an attack on the Internal Forest Guide (see Section 4.13.6). The internal
3301 ECRFs and LVFs (see Section 4.13), when they are under stress from attack, MAY refuse
3302 queries from entities they do not know. External queries MAY use either recursion or
3303 iteration, as the external Forest Guide will be publicly available.

3304 **3.4.4 <findService> Response**

3305 LoST servers MAY operate in recursive mode or iterative mode if the server being queried
3306 is not authoritative for the location supplied.

- 3307 • The use of recursion by the ECRF or LVF initiates a query on behalf of the requestor
3308 that propagates through other ECRFs to an authoritative ECRF/LVF that returns the
3309 PSAP URI back through the intervening ECRFs to the requesting ECRF.
- 3310 • The use of iteration by the ECRF/LVF simply returns a FQDN of the next ECRF to
3311 contact.

3312 The ECRF MAY operate in a recursive mode or an iterative mode, depending on local
3313 provisioning and the value of the 'recursive' attribute of the <findService> request. All
3314 ECRF and LVF implementations MUST support both recursive and iterative modes. It is
3315 strongly RECOMMENDED that ECRFs and LVFs use recursion when the query allows it. This
3316 minimizes the time to complete a request, especially when ECRFs and LVFs make use of
3317 persistent TCP connections to parents and children within the common hierarchy of these
3318 services.

3319 When the i3 ECRF successfully processes a LoST <findService> message, it returns a LoST
3320 <findServiceResponse> message containing a <mapping> element that includes the "next
3321 hop" ESRP or final PSAP URI in the <uri> element. If the ECRF cannot successfully process
3322 a LoST <findService> message, it returns a LoST <errors> message indicating the nature

3323 of the error or a LoST <redirect> message indicating the ECRF that can process the
3324 <findService> message.

3325 The <uri> returned specifies either the next hop URI of the PSAP or the ESRP that is
3326 appropriate for the location sent in the query message. This MUST be a globally routable
3327 URI with a scheme of "sip" for "urn:service:sos". Some other service URNs MAY return
3328 values with HTTP/HTTPS schemes. For example, for the
3329 "urn:emergency:service:additionalData" service URN, LoST servers SHOULD return SIPS
3330 and HTTPS URIs in addition to the SIP and HTTP (when appropriate) URIs.

3331 The 'expires' attribute in the <mapping> element provides an ECRF or LVF with a way to
3332 control load, balancing that against the time required to completely implement a routing
3333 change when circumstances require. By increasing the expiration time, fewer queries to the
3334 server may be received if upstream LoST servers or clients implement caching.

3335 Adjusting the expiration time near the scheduled change time can better accommodate
3336 planned changes, especially for clients that do not implement [178].

3337 Responses from ECRFs SHOULD have very short expiration times, typically measured in
3338 minutes or at most a few hours. This would allow routes to change quickly if failures
3339 resulted in an inability of the normal route to work. While this should be a very unlikely
3340 event, because other mechanisms to redirect calls without changing the URI retrieved from
3341 the LoST query should provide adequate backup, it may still happen when significant
3342 disasters occur and pre-planned backups are not available. It is NOT RECOMMENDED to
3343 return the "NO-EXPIRATION" value. The OPTIONAL "NO-CACHE" expires value may
3344 increase the load experienced by the ECRF and should be used only with due care.

3345 The LoST response contains <via> elements in the <path> element that name the LoST
3346 servers visited to obtain the answer. Vias MUST be returned to be compliant with RFC 5222
3347 and are essential for use in error resolution.

3348 The <displayName> element of the <mapping> response is a text string that provides an
3349 indication of the serving agency(ies) for the location provided in the query. This
3350 information might be useful to PSAPs that query an ECRF. This capability could be used to
3351 provide English Language Translation (ELT)-type information that PSAPs receive from ALI
3352 databases today.

3353 The <service> element in the query identifies the service for which this mapping is valid.
3354 An ECRF outside the ESInet is REQUIRED to support the "urn:service:sos" service. Service
3355 substitution, as described in RFC 5222 [48], SHALL be used to substitute "urn:service:sos"
3356 for all subservices such as "urn:service:sos.police", which would cause the call to be routed
3357 the same as a call to "urn:service:sos". ECRFs inside the ESInet MUST support both
3358 "urn:service:sos" and "urn:emergency:service:sos". Support for other services will depend

3359 on local implementation. Routing of services inside the ESInet may depend on the (TLS)
3360 credentials of the client; routes for two services using the same service URN may receive
3361 different PSAP URIs. Note that if recursion is used, the credentials of the recursive server
3362 would be used, rather than the credentials of the original client.

3363 The <serviceNumber> element in the <mapping> response contains the emergency
3364 services number appropriate for the location provided in the query. This allows a foreign
3365 end device to recognize a dialed emergency number. The service number returned by an
3366 ECRF or LVF for an emergency call MUST be "911".

3367 A <mapping> element MAY contain a service boundary. See Section 4.3.3.3.

3368 The <locationValidation> element in <findServiceResponse> identifies which elements of
3369 the received civic address were "valid" and used for mapping, which were "invalid", and
3370 which were "unchecked" when validation is requested. Since the ECRF is not responsible
3371 for performing validation, this parameter may not be returned, subject to local
3372 implementations. LVFs would always return <locationValidation> if <validateLocation> was
3373 set to "True" in the <findService> request.

3374 To understand the validation portion of the response, follow these rules:

- 3375 1. The combination of all elements appearing in the <valid> list defines the scope.
- 3376 2. The combination of all elements appearing in the <invalid> list is not valid within
3377 the scope.
 - 3378 a. No meaning can be inferred regarding the status of any individual element unless
3379 it is the only invalid element listed.
 - 3380 b. The combination of elements may be valid in other scopes.
 - 3381 c. One or more elements may appear as invalid even if they were not used in the
3382 original query, but could be used to resolve an ambiguity.
- 3383 3. Any individual element appearing as unchecked (or used in the query but not
3384 appearing in any of lists) was not checked or could not be determined to be either
3385 valid or invalid.

3386 If any element appears in the <invalid> list, the location information is invalid and SHOULD
3387 NOT be entered in the LIS unless, for example, there is no reasonable prospect of
3388 obtaining better information before an emergency call could be placed, or the location is
3389 believed correct (and thus the ECRF data is believed incorrect, and a discrepancy report
3390 has been filed).

3391 Provisioning of the LoST server is defined by Section 3.6 and Appendix B. Two of the
3392 "layers" provisioned in the servers are the Centerline and Site/Structure layers. The former
3393 describes segments of a road, and may include address ranges. The latter describes a
3394 single addressable location and has a single address number. If both are provisioned, with

3395 the range overlapping the address points, any PIDF-LO containing a number in the range
3396 will be accepted as valid (address number not in the invalid list) regardless of which
3397 address points are present.

3398 **3.4.5 locationInvalidated**

3399 A LoST server operating as an LVF MUST support draft-ecrit-lost-planned-changes [178]. If
3400 it receives a URI for a location from a client, the LVF server MUST execute an HTTPS POST
3401 containing the <locationInvalidated> object against that URI when a change in GIS data
3402 will make that record invalid at a known future date. The “AsOf” attribute of the
3403 <locationInvalidated> object SHOULD be set to the date and time the GIS data will make
3404 the proffered location invalid. Note that if “AsOf” is used, expired and effective dates must
3405 be present in the data.

3406 **3.4.6 getServiceBoundary**

3407 If a LoST server returns a service boundary by reference, it MUST handle
3408 getServiceBoundary requests.

3409 **3.4.7 listServices and listServicesByLocation**

3410 All ECRFs and LVFs MUST implement listServices and listServicesByLocation. The response
3411 to this request may depend on the (TLS) credentials of the querier. A query with no
3412 <service> element in the request SHOULD result in “urn:service:sos” and possibly
3413 “urn:emergency:service” (the top level services) being returned in the response. A query
3414 with <service> specified as “urn:service:sos” SHOULD result in all the subservices of sos
3415 (sos.police, sos.fire, ...) that are available in the jurisdiction being returned in the response.
3416 Entities inside the ESInet MUST specify recursion by setting the recursive attribute in the
3417 <listServicesByLocation> request to true.

3418 **3.4.8 Error Responses**

- 3419 • <badRequest> Element
3420 This element indicates the ECRF/LVF could not parse or otherwise understand the
3421 request sent by the requesting entity (e.g., the XML is malformed).
- 3422 • <forbidden> Element
3423 This element indicates an ECRF/LVF refused to send an answer. This generally only
3424 occurs for recursive queries, namely, if the client tried to contact the authoritative
3425 server and was refused.
- 3426 • <internalError> Element
3427 This element indicates the ECRF/LVF could not satisfy a request due to a bad
3428 configuration or some other operational and non-LoST protocol-related reason.

- 3429 • <locationProfileUnrecognized> Element
3430 None of the profiles in the request were recognized by the server.
3431 • <locationInvalid> Element
3432 This element indicates the ECRF/LVF determined the geodetic or civic location is
3433 invalid (e.g., geodetic latitude or longitude value is outside the acceptable range).
3434 The only time this would normally be returned is if there was a malformed location
3435 such as profile="geodetic-2d" and <civicAddress> element present. If there is no
3436 authoritative server for the location, that would be coded as "notFound".
3437 • <SRSInvalid> Element
3438 This element indicates the ECRF/LVF does not recognize the spatial reference
3439 system (SRS) specified in the <location> element or it does not match the SRS
3440 specified in the profile attribute (e.g., not WGS84 2D, EPSG Code 4326 for
3441 profile="geodetic-2d"). Note that this error is not present in the RFC 5222 schema,
3442 has been reported as an errata, and thus may not be implemented by all LoST
3443 servers or clients. Use of this error may be problematic.
3444 • <loop> Element
3445 During a recursive query, the server was about to visit a server that was already in
3446 the server list in the <path> element indicating a request loop.
3447 • <notFound> Element
3448 The ECRF/LVF cannot find an answer to the query. This occurs if the authoritative
3449 server cannot find the location and has no applicable default mapping, or if no
3450 authoritative server exists.
3451 • <serverError> Element
3452 An answer was received from another LoST server, but it could not be parsed or
3453 otherwise understood. This error occurs only for recursive queries.
3454 • <serverTimeout> Element
3455 This element indicates the ECRF timed out waiting for a response (e.g., another
3456 ECRF for a recursive query, etc.).
3457 • <serviceNotImplemented> Element
3458 This element indicates the ECRF detected the requested service URN is not
3459 implemented and it found no substitute for it. This normally would not occur for a
3460 service beginning "urn:service:sos" unless 9-1-1 service is not available in that area.

3461 **3.4.9 Warnings**

3462 A LoST response MAY contain one or more of the following warnings. Each warning comes
3463 with a "message" attribute with content in a human-readable format.

- 3464 • locationValidationUnavailable
3465 A LoST server MAY return this element in the response to indicate it cannot fulfill a
3466 validation request.
3467 • serviceSubstitution
3468 A LoST server MAY return this element in the response to indicate that it cannot
3469 fulfill a <findService> request for the service URN specified.
3470 • defaultMappingReturned
3471 A LoST server MAY return this element in the response to indicate it cannot fulfill a
3472 <findService> request for the specified location but is able to respond with a default
3473 URI.
3474 • uriNotStored
3475 A LoST server operating as an LVF supporting draft-ecrit-lost-planned-changes [178]
3476 MUST return this element in the response if the URI provided by the LoST client in
3477 the <plannedChange> element was not stored.

3478 **3.4.10 LoST Extensions**

3479 The standard information returned within the <locationValidation> element of a LoST
3480 <findServiceResponse> is somewhat limited. In order to aid a consumer of the response in
3481 assessing the quality and validity of the queried location, it may be helpful to indicate what
3482 type of match was used by the LVF's geocoding logic. It may also be helpful if the LVF can
3483 explicitly warn when such a match is of lesser quality than might be expected. Therefore,
3484 two extensions to LoST are defined for this purpose. The first is an element to indicate the
3485 type of match used, and is placed at the existing extension point of the
3486 <locationValidation> element. The second is a new warning element which can be used at
3487 the existing extension point within the standard <warnings> element of the response.

3488 **3.4.10.1 matchType Element**

3489 The <matchType> element is intended to contain an indication of the type of data used by
3490 the LVF's geocoding logic when attempting to match the location supplied in the request to
3491 the GIS data that has been provisioned. The value of the element is an xsd:token, and
3492 must be a registered value. It is RECOMMENDED that ECRFs and LVFs implement match
3493 type. If more than one token would apply, then "Hybrid" is used. A registry for
3494 <matchType> tokens is defined in Section 10.31.

3495 **3.4.10.1.1 XML Schema Definition**

3496 The <matchType> element is placed at the extension point defined with the
3497 <locationValidation> element of a LoST <findServiceResponse> and is defined by the
3498 following schema:

[MM/DD/YYYY]

Page 114 of 675



3499 <?xml version="1.0" encoding="UTF-8"?>
3500 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
3501 elementFormDefault="qualified"
3502 targetNamespace="urn:emergency:xml:ns:lostExt:validation1"
3503 xmlns:ns1="urn:emergency:xml:ns:lostExt:validation1">
3504 <xs:element name="matchType" type="xs:token"/>
3505 </xs:schema>

3506 This capability MAY be provided by an ECRF/LVF.

3507 **3.4.10.2 degradedMatch Element**

3508 The <degradedMatch> warning reuses the BasicException pattern from LoST and is placed
3509 at the extension point defined in the exceptionContainer of a findServiceResponse. The
3510 warning may include an optional message containing human-readable text. The warning is
3511 intended to convey the notion that the location queried was not able to be matched using
3512 the best available data. An example of this is when a location does not match any
3513 provisioned address points, but still falls within a range of addresses associated with a road
3514 centerline. The determination of "best available data" is left to the discretion of the LVF,
3515 and may vary from one geographic region to another. It is RECOMMENDED that ECRFs and
3516 LVFs implement degradedMatch. An LVF SHOULD NOT return a degradedMatch warning if
3517 there is no potential for improvement (e.g., a road centerline match in a region where
3518 address points are not able to be provisioned).

3519 **3.4.10.2.1 XML Schema Definition**

3520 The degraded match warning is defined by the following RelaxNG schema:

3521 <?xml version="1.0" encoding="UTF-8"?>
3522 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
3523 elementFormDefault="qualified"
3524 targetNamespace="urn:emergency:xml:ns:lostExt:validation1"
3525 xmlns:ns1="urn:emergency:xml:ns:lostExt:validation1">
3526 <xs:element name="matchType" type="xs:token"/>
3527 </xs:schema>

3528 This capability MAY be provided by an ECRF/LVF.

3529 **3.4.10.3 Example**

3530 The following example shows both the <matchType> element and the <degradedMatch>
3531 warning.

3532 <findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
3533 <mapping expires="2016-10-28T12:44:30Z" lastUpdated="2015-06-
3534 22T18:05:17Z" source="lost.example.com" sourceId="7608">
3535 <displayName xml:lang="en">Police Dispatch</displayName>
3536 <service>urn:service:sos</service>

```
3537      <uri>sip:sos@psap.example.com</uri>
3538      <serviceNumber>911</serviceNumber>
3539    </mapping>
3540    <locationValidation
3541      xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
3542      xmlns:lv1="urn:emergency:xml:ns:lostExt:validation1">
3543      <valid>ca:country ca:A1 ca:A3 ca:RD ca:STS</valid>
3544      <invalid />
3545      <unchecked>ca:HNO</unchecked>
3546      <lv1:matchType>RoadCenterline</lv1:matchType>
3547    </locationValidation>
3548    <warnings source="lost.example.com">
3549      <degradedMatch xmlns="urn:emergency:xml:ns:lostExt:degraded"
3550        message="The location was matched using road centerlines." xml:lang="en"
3551      />
3552    </warnings>
3553    <path>
3554      <via source="lost.example.com" />
3555    </path>
3556    <locationUsed id="nsTrQMfffoEa74" />
3557  </findServiceResponse>
```

3558 **3.4.10.4 Call and Incident ID Extension to LoST**

3559 This document defines an extension to LoST, which adds Call Identifiers and Incident
3560 Tracking Identifiers to any LoST request. All elements that implement LoST MUST
3561 implement the Call and Incident ID extension.

3562 **3.4.10.4.1 XML Schema Definition**

```
3563  <?xml version="1.0" encoding="UTF-8"?>
3564  <xsschema xmlns:xss="http://www.w3.org/2001/XMLSchema"
3565    elementFormDefault="qualified"
3566    targetNamespace="urn:emergency:xml:ns:lostExt:Ids"
3567    xmlns:ns1="urn:emergency:xml:ns:lostExt:Ids">
3568    <xss:element name="nenaCallIncidentId">
3569      <xss:complexType>
3570        <xss:attribute name="callId" use="required" type="xs:token"/>
3571        <xss:attribute name="incidentTrackingId" use="required"
3572          type="xs:token"/>
3573      </xss:complexType>
3574    </xss:element>
3575  </xss:schema>
```

3576 **3.4.10.5 Too Many Mappings Warning Extension to LoST**

3577 This document defines an extension to LoST, which adds a Too Many Mappings warning to
3578 a <findServiceResponse>. It is RECOMMENDED that ECRFs and LVFs implement
3579 TooManyMappings.

3580 **3.4.10.5.1 XML Schema Definition**

```
3581 <?xml version="1.0" encoding="UTF-8"?>
3582 <xss:schema xmlns:xss="http://www.w3.org/2001/XMLSchema"
3583   targetNamespace="urn:emergency:xml:ns:lostExt"
3584   xmlns:lost="urn:ietf:params:xml:ns:lost1"
3585   elementFormDefault="qualified">
3586   <xss:import namespace="urn:ietf:params:xml:ns:lost1"
3587     schemaLocation="lost1.xsd"/>
3588   <xss:element name="tooManyMappings" type="lost:basicException"/>
3589 </xss:schema>
```

3590 **3.4.11 LoST Query Examples**

3591 **3.4.11.1 Civic Address-based Call Routing LoST Interface Example Scenario**

3592 A <findService> well-formed civic address query:

```
3593 <?xml version="1.0" encoding="UTF-8"?>
3594 <findService xmlns="urn:ietf:params:xml:ns:lost1"
3595   recursive="true" serviceBoundary="value">
3596   <location id="627b8bf819d0bcd4d" profile="civic">
3597     <civicAddress
3598       xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
3599       <country>US</country>
3600       <A1>OH</A1>
3601       <A3>Columbus</A3>
3602       <RD>Airport</RD>
3603       <STS>Drive</STS>
3604       <HNO>2901</HNO>
3605       <NAM>Courtyard Marriott</NAM>
3606       <PC>43219</PC>
3607       <Room>Board Room B</Room>
3608     </civicAddress>
3609   </location>
3610   <service>urn:service:sos</service>
3611 </findService>
```

3612 A <findServiceResponse> response to a well-formed query:

```
3613 <?xml version="1.0" encoding="UTF-8"?>
3614   <findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
3615     <mapping
3616       expires="2010-01-01T01:44:33Z"
3617       lastUpdated="2009-09-01T01:00:00Z"
3618       source="esrp.state.oh.us.example"
3619       sourceId="e8b05a41d8d1415b80f2cddb96ccf109">
3620       <displayName xml:lang="en">
3621         Columbus PSAP
3622       </displayName>
3623       <service>urn:service:sos</service>
3624       <serviceBoundary
3625         profile="civic">
3626         <civicAddress
3627           xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
3628             <country>US</country>
3629             <A1>OH</A1>
3630             <A3>Columbus</A3>
3631           </civicAddress>
3632         </serviceBoundary>
3633         <uri>sip:columbus.psap@state.oh.us</uri>
3634         <serviceNumber>911</serviceNumber>
3635       </mapping>
3636       <path>
3637         <via source="ecrf.state.oh.us"/>
3638       </path>
3639       <locationUsed id="627b8bf819d0bcd4d"/>
3640     </findServiceResponse>
```

3641 A <findService> civic address query with partial information:

```
3642 <?xml version="1.0" encoding="UTF-8"?>
3643   <findService xmlns="urn:ietf:params:xml:ns:lost1"
3644     recursive="true" serviceBoundary="value">
3645     <location id="627b8bf819d0bcd4d" profile="civic">
3646       <civicAddress
3647         xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
3648           <country>US</country>
3649           <A3>Columbus</A3>
3650           <RD>Airport</RD>
3651           <STS>DR</STS>
3652           <HNO>2901</HNO>
3653         </civicAddress>
3654       </location>
3655       <service>urn:service:sos</service>
3656     </findService>
```

3657 An <error> response to a partially-formed query:

```
3658 <?xml version="1.0" encoding="UTF-8"?>
```

[MM/DD/YYYY]

Page 118 of 675



3659 <errors xmlns="urn:ietf:params:xml:ns:lost1"
3660 source="ecrf.state.oh.us">
3661 <badRequest message="invalid XML fragment" xml:lang="en"/>
3662 </errors>

3663 This response scenario indicates an error that the server cannot find an answer to the
3664 query.

3665 **Note:** Further examples of call routing will be provided in a future version of this
3666 document.

3667 **3.5 Event Notification**

3668 Events are communicated within and between ESInets using the SIP SUBSCRIBE/NOTIFY
3669 mechanism described in RFC 6665 [14]. ESInet functional elements MAY need to accept or
3670 generate events to outside elements using different asynchronous event notification
3671 mechanisms, which MUST be interworked to SIP SUBSCRIBE/NOTIFY at the ESInet
3672 boundary.

3673 NG9-1-1 events are defined by an event package which includes the name of the event,
3674 the subscription parameters, the conditions under which NOTIFYs are issued and the
3675 content of the NOTIFY, as described in RFC 6665.

3676 **3.6 Spatial Interface for Layer Replication**

3677 Geospatial data is stored in a Geographic Information System (GIS). This document does
3678 not standardize the GIS. However, the data in the GIS is used to provision the ECRF, the
3679 LVF, the Mapping Data Service, and other functions. In order to provide a standardized
3680 interface from the GIS to the rest of the functional elements that need GIS data, this
3681 document describes a "Spatial Interface" (SI), which is a standardized interface towards
3682 data consumers such as the ECRF/LVF.

3683 The SI could be built into a GIS system, or could be a stand-alone element with proprietary
3684 interfaces to GIS systems and the standardized interface towards the data consumers. The
3685 data model provided by the SI is based on the conventional GIS layer that consists of a set
3686 of geospatial features, each of which could be a point, line, or polygon, or a set of points,
3687 lines, or polygons. Each feature has a set of named attributes. For example, a part of a
3688 road might be represented as a set of connected straight lines of the road centerline, with
3689 attributes that name the road and provide the range of address numbers in that segment
3690 of the road.

3691 An SI provides an interface between an authoritative copy of GIS data and functional
3692 elements within an ESInet such as an ECRF and LVF. An SI layer replication interface is
3693 used within the ESInet to maintain copies of the data in the layers of the authoritative GIS
3694 system that drives routing and display of maps throughout the system. Furthermore, any

3695 element that obtains GIS data via the SI could provide copies of the data to another
3696 element with the same interface, thus permitting wide distribution of authoritative data.
3697 The SI interface is near-real-time: an authorized change to the authoritative GIS will be
3698 reflected in the copies nearly immediately via the SI.

3699 The SI MUST implement the server side of the ElementState event notification package and
3700 permit any ECRF or LVF that receives a feed from it to subscribe to it.

3701 The data structure for the SI is defined in Appendix B. The GIS Data Model [184] need not
3702 be the same as that defined for the SI: the SI could transform internal GIS data to the SI
3703 structure.

3704 OGC Document OGC 10-069r2 [94] describes a layer replication interface service for
3705 geospatial databases using the Web Feature Service (WFS) [93] and the ATOM protocol
3706 (RFC 4287 [95] and RFC 5023 [96]). Essentially, the changes in the database are
3707 expressed in WFS Insert/Update/Delete actions and ATOM is used to move the edits from
3708 the master to the copy. GeoRSS (<http://www.georss.org>) is a very simple mechanism used
3709 to encode the GML in RSS feeds for use with ATOM. There are three ATOM feeds proposed
3710 by OGC 10-069r2; a change feed, a resolution feed, and a replication feed. The SI layer
3711 replication interface is patterned after the replication feed described within OGC 10-069r2.

3712 **3.7 Discrepancy Reporting**

3713 Errors and discrepancies may occur in any set of data, including databases, configurations,
3714 etc. The functional elements described in this document MUST support the discrepancy
3715 report (DR) function. The DR function allows any entity to notify agencies and services
3716 (including the BCF, ESRP, ECRF, Policy Store, and LVF) when any discrepancy is found. The
3717 discrepancy report function is intended to be generated by any entity that is using the data
3718 and finds a problem. DRs are not intended to be an alarm function requiring immediate
3719 response. Examples include:

- 3720 • The LIS might need to file a Discrepancy Report on the LVF.
- 3721 • The ECRF/LVF may be receiving data from another ECRF/LVF and thus might need
3722 to file a DR on its upstream provider.
- 3723 • The ECRF/LVF might need to file a DR on the GIS.
- 3724 • The ESRP might need to file a DR on the owner of a routing policy (PSAP, ESRP)
3725 that has a problem.
- 3726 • The PSAP might need to file a DR on an ESRP if a call is misrouted.
- 3727 • The PSAP might need to file a DR on the GIS when issues are found in a map
3728 display.
- 3729 • Any client of an ECRF might need to file a DR on the routing data (which could be a
3730 GIS layer problem or something else).

- 3731 • A PSAP or ESRP might need to file a DR on a LIS.
3732 • A PSAP or ESRP might need to file a DR on an ADR/IS-ADR.
3733 • A BCF, ESRP, or PSAP needs to file a DR on an originating network sending it a
3734 malformed call.
3735 • Any client might need to file a DR on the ESInet operator (e.g., for general
3736 networking issues such as high latency, packet loss, incorrect DNS, or DHCP
3737 behavior).
3738 • One PSAP might need to file a DR on another PSAP that transferred a call to it
3739 • A data user might need to file a DR on a data owner due to rights management
3740 issues.
3741 • A log client (logging entry or query) might need to file a DR on the Logging Service
3742 • Any entity might need to file a DR on another entity due to authentication issues
3743 (bad certificate, unknown entity, etc.).
3744 • An ESRP or PSAP might need to file a DR on a Border Control Function
3745 • Any Policy Enforcement Point might need to file a DR on a Policy owner due to
3746 formatting, syntax or other errors in the policy.
3747 • A Test Call Generator might need to file a DR on a PSAP for problems encountered
3748 when generating a test call.
3749 • An entity verifying signed LogEvents might need to file a DR against an entity that
3750 logged an event if it is unable to obtain the certificate or verify the signature.

3751 This document provides a standardized Discrepancy Reporting mechanism in the form of a
3752 web service. Each database, service, and agency MUST provide a Discrepancy Reporting
3753 web service. When a discrepancy is reported on an element (such as an ECRF), the DR is
3754 reported using a DR web service operated by the entity that operates the element, not
3755 necessarily by the element itself. While an automated mechanism is specified to handle
3756 sending and receiving of DRs and the responses to those DRs, humans will usually be
3757 responsible for generating and acting on them. Since a human will be involved, there might
3758 be noticeable time elapsed from the sending of the report to receiving the resolution; a
3759 call-back mechanism is provided for the responding agency to send the resolution to the
3760 reporting agency.

3761 A Discrepancy Report (DR) is submitted by the entity reporting the discrepancy to a
3762 responding entity and passes through several phases:

- 3763 • The reporting entity creates the DR and submits it to the responding entity.
3764 • The responding entity acknowledges the DR and provides an estimate of when it will
3765 be resolved.
3766 • The reporting entity may request a status update and receive a response.
3767 • The responding entity resolves the DR and reports its resolution to the reporting
3768 entity using the call-back mechanism.

3769 All DRs MUST contain common data elements (a prolog) that include:

- 3770 • Time Stamp of Discrepancy Submittal
- 3771 • Discrepancy Report ID (a unique value generated by the reporting entity)
- 3772 • Discrepancy reporting entity FQDN
- 3773 • Discrepancy reporting agent user ID
- 3774 • Discrepancy reporting contact info
- 3775 • Service or Instance in which the discrepancy exists
- 3776 • Discrepancy Report type (from the list of DRs in this section)
- 3777 • Additional notes/comments
- 3778 • Reporting entity's assessment of severity
- 3779 • Discrepancy Service or Database specifics (as specified in the specific DR in this section)

3780 For each type of Discrepancy Report there is a specific database or service where the discrepancy originated or occurred, and a defined block of data specific to the Discrepancy Report type. This DR-specific block includes:

- 3781 • Query that generated the discrepancy
- 3782 • Full response to the query that generated the discrepancy (Message ID, Result Code, etc.)
- 3783 • What the reporting entity thinks is wrong
- 3784 • What the reporting entity thinks is the correct response, if available

3785 FEs creating Discrepancy Reports SHOULD limit the rate of similar reports to avoid having the DR service become a denial of service attack.

3786 The Service/Agency Locator (Section 4.15) provides the URI to an agency or service's DR interface.

3787 **3.7.1 Discrepancy Report**

3788 The Discrepancy Reporting web service is used by a reporting entity to initiate a Discrepancy Report. The OpenAPI description of this web service can be found in Appendix E.2. It supports the following functions:

3789 HTTP method: POST

3790 Resource name .../Reports

3791 Submits a Discrepancy Report. The DR is in the body of the POST, consisting of:

Name	Condition	Description
resolutionUri	MANDATORY	URI for responding entity to use for responses
reportType	MANDATORY	Type of DR (enumeration)

Name	Condition	Description
discrepancyReportSubmitTimestamp	MANDATORY	Timestamp of Discrepancy Report Submittal
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of report
reportingAgencyName	MANDATORY	FQDN of the entity creating the report
reportingAgentId	OPTIONAL	UserId of agent creating the report
reportingContactJcard	MANDATORY	jCard of contact about this report
problemService	Conditional, MUST be provided for specified DRs	Name of service or instance where discrepancy exists
problemSeverity	MANDATORY	<p>One of the following tokens representing the reporting entity's opinion of the discrepancy's severity:</p> <ul style="list-style-type: none"> • Minor (e.g., format/spelling) • Moderate (still functions) • Degraded • Impaired • Severe (service down but calls can proceed) • Critical (calls impaired)
problemComments	Conditional, MUST be provided for specified DRs, OPTIONAL otherwise	Text comment

- 3800 The object has additional "reportType"-dependent parameters, listed in subsections below.
 3801 Each database/service-specific discrepancy report description indicates whether the
 3802 "problemService" and/or "problemComments" parameter is required for that
 3803 database/service or not, and specifies additional parameters contained in the submitted
 3804 object.
 3805 The resolution to the Discrepancy Report is sent to the URI in the resolutionUri parameter
 3806 of the request.

3807 A successful report submission returns a DiscrepancyReportResponse that consists of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of agency responding to report
respondingContactJcard	MANDATORY	jCard of contact about this response
respondingAgentId	OPTIONAL	UserId of agent creating the response report
responseEstimatedReturnTime	OPTIONAL	Estimated response time stamp
responseComments	OPTIONAL	Text comment

3808 Status Codes

- 3809 201 Report successfully created
- 3810 454 Unspecified Error
- 3811 470 Unknown Service/Database ("not ours")
- 3812 471 Unauthorized Reporter

3.7.2 Discrepancy Resolution

3814 When the responding agency determines what the resolution to the DR is, it sends the resolution to the ResolutionUri parameter in the report request.

3816 HTTP method: POST

3817 Resource name .../Resolutions

3818 The POST contains a DiscrepancyResolution in the body, consisting of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of entity responding to the report
respondingContactJcard	MANDATORY	jCard of contact about this report
respondingAgentId	OPTIONAL	UserId of agent responding to the report
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of report
reportingAgencyName	MANDATORY	FQDN of agency creating the report
problemService	MANDATORY	Name of service or instance where discrepancy exists
responseTime	MANDATORY	Time stamp of response

Name	Condition	Description
responseComments	OPTIONAL	Text comment
resolution	MANDATORY	Details how the DR was resolved, as described in the DR-specific resolutions in the following subsections

3819 Status Codes

3820 201 Discrepancy Resolution successfully created

3821 454 Unspecified Error

3822 472 Unauthorized Responder

3823 473 Unknown ReportId

3824

3825 The report can be retrieved based on the Agency Name and discrepancyReportId

3826 HTTP method: GET

3827 Resource name .../Resolutions

Name	Condition	Description
agencyName	MANDATORY	FQDN of entity reporting the discrepancy
discrepancyReportId	MANDATORY	Id of the report

3828 A successful response returns the DiscrepancyResolution object described above

3829 Status Codes

3830 200 Resolution found

3831 404 Not Found

3832 471 Unauthorized Reporter

3833 473 Unknown ReportId

3834 475 Response not available yet

3.7.3 Status Update

3835 A reporting entity MAY request a status update. The mechanism defined assumes the responding entity continuously tracks the status of Discrepancy Reports that it has received (including those it has recently resolved), and can respond to the Status Update immediately. The update request includes:

3840 HTTP method: GET

3841 Resource name .../StatusUpdates

[MM/DD/YYYY]

Page 125 of 675



Name	Condition	Description
reportingAgencyName	MANDATORY	FQDN of entity that created the original report
discrepancyReportId	MANDATORY	Unique (to reporting agency) ID of original report

3842 A successful response to this request includes a StatusUpdate object consisting of:

Name	Condition	Description
respondingAgencyName	MANDATORY	FQDN of the entity responding to the report
RespondingContactJcard	MANDATORY	jCard of contact about this report
respondingAgentId	OPTIONAL	UserId of agent responding to the report
responseEstimatedReturn Time	MANDATORY	Estimated date/time when response will be returned to reporting agency or the actual time, in the past, when the response was provided.
statusComments	OPTIONAL	Text Comment

3843 Status Codes

3844	200	OK
3845	404	Not Found
3846	454	Unspecified Error
3847	471	Unauthorized Reporter
3848	454	Unspecified Error
3849	471	Unauthorized Reporter
3850	473	Unknown ReportId
3851	474	Resolution already provided

3.7.4 Policy Store Discrepancy Report

3853 A client of a Policy Store MAY report a discrepancy. The most commonly expected report is that a Policy Query returned an invalid Policy from the Policy Store. A Policy Owner MAY retrieve a policy it previously stored to verify that the returned policy is valid and an exact match of that stored, and if not, file a discrepancy report against the Policy Store. A Policy Store MAY report a discrepancy against itself to raise an issue to be addressed.

3858 When a **PolicyStoreDiscrepancyReport** is submitted, the “problemService” parameter is
3859 set to “PolicyStore” and the object contains the following elements:

Name	Condition	Description
policyType	CONDITIONAL, at least one of policyType, policyOwner, policyId or policyQueueName MUST be provided	Type of the policy. Values are limited to names in the Policy Types registry
policyId	CONDITIONAL, MUST NOT be specified unless policyType is “OtherRoutePolicy”	For “OtherRoutePolicy”, this is an arbitrary identifier for the policy
policyQueueName	CONDITIONAL, MUST NOT be specified unless policyType is “OriginationRoutePolicy” or “NormalNextHopRoutePolicy”	For “OriginationRoutePolicy” or “NormalNextHopRoutePolicy”, this is the policyQueueName
policyAgencyName	MANDATORY	The agency whose policy is requested. Must be a FQDN or URI that contains a FQDN
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none"> • PolicyInvalid • PolicyAltered • SignatureVerificationFailure • PolicyMissing • OtherPolicyStore
retrievePolicyResponse	MANDATORY	The Response received from the Policy Retrieve Request as shown in Section 3.3.1

3860 The Resolution parameter in a Policy Store Discrepancy Resolution report contains one of
3861 the following tokens:
 3862 • PolicyAdded
 3863 • PolicyUpdated
 3864 • NoSuchPolicy
 3865 • InsufficientCredentials
 3866 • NoDiscrepancy

[MM/DD/YYYY]

Page 127 of 675



- 3867 • OtherResponse

3868 **3.7.5 LoST Discrepancy Report**

3869 A client of an LVF/ECRF/LoST server (see Section 3.4) MAY report a discrepancy. An
3870 ECRF/LVF MAY report a discrepancy against another ECRF/LVF from which it receives data.
3871 An ECRF/LVF MAY report a discrepancy against itself to raise an issue to be addressed. The
3872 expected reports are:

- 3873 • the LoST server reports a location as invalid, when the client believes it is valid;
- 3874 • a LIS MAY report a discrepancy against an LVF (as well as against an Originating
3875 Service Provider) if a civic address provisioned by an Originating Service Provider for
3876 a fixed device is reported invalid by an LVF;
- 3877 • the LoST server returned an incorrect route in a findServiceResponse;
- 3878 • the LoST server returned an incorrect error or warning regarding the location;
- 3879 • the getServiceBoundaryResponse is incorrect;
- 3880 • the listServicesResponse is incorrect;
- 3881 • the listServicesByLocationResponse is incorrect.

3882 Other discrepancies may be reported but are expected to be less common. These include:

- 3883 • a client received an address reported as valid that it considers invalid;
- 3884 • multiple mappings were returned when only one was expected;
- 3885 • incorrect service number(s) returned;
- 3886 • expired data returned;
- 3887 • an incorrect <uri> element was returned.

3888 A DR against a LoST server MAY result in the LoST server reporting a discrepancy against
3889 the GIS data.

3890 When a **LoSTDiscrepancyReport** is submitted, the “problemService” parameter is set to
3891 “LoST” and the object contains the following elements:

Name	Condition	Description
query	MANDATORY	One of the following tokens: <ul style="list-style-type: none">• findService• getServiceBoundary• listServices• listServicesByLocation
request	MANDATORY	The request sent by the client (e.g., the findService request)

Name	Condition	Description
response	MANDATORY	The response received by the client (e.g., the findServiceResponse)
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none"> • BelievedValid • BelievedInvalid • NoSuchLocation • RouteIncorrect • MultipleMappings • ServiceBoundaryIncorrect • ServiceNumberIncorrect • DataExpired • IncorrectURI • LocationErrorInError • OtherLoST

3892 The Resolution parameter in a LoST DiscrepancyResolution report request) contains one of
 3893 the following tokens:
 3894

- DiscrepancyCorrected
- DiscrepancyNotFound
- EntryAdded

 3895

3.7.6 BCF Discrepancy Report

3896 An entity routing traffic through (to or from) a BCF (see Section 4.1) MAY report a
 3897 discrepancy. The expected reports are:

- 3898
 - Traffic was incorrectly blocked before a dialog has been established (e.g., an INVITE,
 3899 MESSAGE, or OPTIONS request, or response blocked);
 - traffic was incorrectly blocked during a dialog;
 - SIP signaling was inappropriately modified or dropped;
 - SDP was incorrectly regenerated during B2BUA/media anchoring;
 - Media was relayed with loss;
 - traffic was permitted that should have been blocked because it was generated by a
 3900 designated bad actor;
 - traffic was permitted that should have been blocked for some other reason;
 3901
 - QoS inconsistency;
 - Invalid or improper Call Detail Recording;
 - TTY to RTT transcoding errors;
 - Firewall (non SIP) errors.

3913 When a **BCFDiscrepancyReport** is submitted, the “problemService” parameter is set to
3914 “BCF” and the object contains the following elements:

Name	Condition	Description
request	Conditional: REQUIRED when the discrepancy concerns a dialog	If the discrepancy concerns a dialog, the initial INVITE that initiated the dialog
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none">• InitialTrafficBlocked• MidTrafficBlocked• BadSDP• BadSIP• MediaLoss• TrafficNotBlockedBadActor• TrafficNotBlocked• QoS• BadCDR• TTY• Firewall• OtherBCF
sosSource	MANDATORY	The emergency-source parameter of the dialog request (i.e., the initial INVITE)
eventTimestamp	MANDATORY	Timestamp of event being reported
packetHeader	Conditional, REQUIRED for InitialTrafficBlocked, MidTrafficBlocked, TrafficNotBlockedBadActor, TrafficNotBlocked, or Firewall, OPTIONAL otherwise	For InitialTrafficBlocked, MidTrafficBlocked, TrafficNotBlockedBadActor, TrafficNotBlocked, or Firewall, contains the packet’s header, encoded using base64

3915 The Resolution parameter in a BCF DiscrepancyResolution report contains one of the
3916 following tokens:

- 3917
 - DiscrepancyCorrected
 - PerPolicy (behavior was per policy, hence not a discrepancy)
 - NoDiscrepancy
 - OtherResponse

[MM/DD/YYYY]

Page 130 of 675



3921 **3.7.7 Logging Service Discrepancy Report**

3922 A Session Recording Client (SRC) or any entity generating logging events to, or retrieving
3923 logging records from, a Logging Service (see Section 4.12) MAY report a discrepancy. The
3924 expected reports are:

- 3925 • An SRC encountered an error inviting the SRS;
3926 • LogEvent returned an error when it shouldn't have;
3927 • RetrieveLogEvent returned an error when it shouldn't have.

3928 When a **LoggingDiscrepancyReport** is submitted, the "problemService" parameter is set
3929 to "Logging Service" and the object contains the following elements:

Name	Condition	Description
request	MANDATORY	The SIP INVITE or other request, or the LogEvent request, or the RetrieveLogEvent request
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none">• InviteSRSError• LogEventError• RetrieveLogEventError• OtherLogging
result	MANDATORY	The status code returned from the SIP request, the LogEvent request, or the RetrieveLogEvent request
callId	Conditional: REQUIRED if problem relates to a specific call	The Call Identifier
incidentId	Conditional: REQUIRED if problem relates to a specific incident	The Incident Tracking Identifier

3930 The resolution parameter in a DiscrepancyResolution report request) contains one of the
3931 following tokens:

- 3932 • DiscrepancyCorrected
3933 • NoDiscrepancy
3934 • OtherResponse

3935

[MM/DD/YYYY]

Page 131 of 675



3936 **3.7.8 PSAP Call Taker Discrepancy Report**

3937 A PSAP, downstream agency, or other entity MAY report a discrepancy against a PSAP Call
3938 Taker when a call is received that should not have been transferred to the reporting entity.

3939 When a **CallTakerDiscrepancyReport** is submitted, the "problemService" parameter is
3940 set to "CallTaker", the "Comment" parameter contains further explanation as to why the
3941 call transfer was in error, and the "object" contains the following elements:

Name	Condition	Description
CallId	MANDATORY	The Call ID assigned to the call
IncidentId	MANDATORY	The Incident ID associated with the call
pidfLO	MANDATORY	The PIDF-LO received with or via the call
callHeader	MANDATORY	The header field of the INVITE or MESSAGE

3942 The resolution parameter in a DiscrepancyResolution report contains one of the following
3943 tokens:

- CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)
- TransferCorrect (the transfer was correct)
- NoDiscrepancy
- OtherResponse

3949 **3.7.9 SIP Discrepancy Report**

3950 Any entity encountering an error communicating with another entity via SIP (such as a
3951 PSAP) MAY report a discrepancy. The source of the discrepancy might be an element
3952 within or in front of the problem entity (e.g., a BCF or ESRP) that might not be visible to
3953 the entity reporting the discrepancy; in such cases the entity accepts the DR and reports its
3954 own against the responsible entity.

3955 The expected reports are:

- An initial INVITE request failed;
- A MESSAGE request failed;
- An OPTIONS request failed;
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed;
- Required media stream (audio, text, video) failed to be accepted;
- Media problems during a dialog;
- Signaling failure.

[MM/DD/YYYY]

Page 132 of 675



3963 When a **SIPDiscrepancyReport** is submitted, the “problemService” parameter is set to
3964 “SIP” and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: <ul style="list-style-type: none"> • InitialINVITE • MESSAGE • OPTIONS • MidDialog • RequiredMedia • MediaProblem • EngorgedQ (a queue is fuller than it should be) • Signaling • OtherSIP
callId	Conditional: REQUIRED if problem is related to a specific call	The Call Identifier
incidentId	Conditional: REQUIRED if an IncidentID is available	The Incident Tracking Identifier
testCallGenerator	Conditional: REQUIRED if DR is related to a test call	The block of parameters specified in Section 4.6.17
request	Conditional: REQUIRED if the problem occurred on a SIP request or response	The SIP request
result	Conditional: REQUIRED if the problem occurred on a SIP request or response	The status code returned from the SIP request
queueName	Conditional: REQUIRED if the call was sent to a queue	The queue in question

3965 The Resolution parameter in a DiscrepancyResolution report contains one of the following
3966 tokens:

- 3967 • DiscrepancyCorrected
3968 • NoDiscrepancy
3969 • OtherResponse

3970 **3.7.10 Permissions/Security/Authentication Discrepancy Report**

3971 Any entity encountering a security issue or a permissions or authentication error that is
3972 believed to be incorrect, MAY report a discrepancy using the DR interface of the entity or
3973 element believed to be responsible for the discrepancy.

3974 The expected reports are:

- 3975 • Unable to authenticate;
- 3976 • Unable to SUBSCRIBE to an event package;
- 3977 • Permitted to SUBSCRIBE to an event package when it should have been denied;
- 3978 • Unable to read a resource;
- 3979 • Unable to write/modify a resource;
- 3980 • Unable to delete a resource;
- 3981 • Able to read a resource when it should have been denied;
- 3982 • Able to write/modify a resource when it should have been denied;
- 3983 • Able to delete a resource when it should have been denied;
- 3984 • Unable to establish secure communication (e.g., TLS certificate invalid or TLS failure)
- 3985 • Unable to verify digital signature of a resource (e.g., a routing policy signature
- 3986 verification failed or the certificate chain is invalid or contains an untrusted
- 3987 authority).

3988 When a **PermissionsDiscrepancyReport** is submitted, the “problemService” parameter
3989 is set to “Permissions” and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: <ul style="list-style-type: none">• UnableAuthenticate• UnableSubscribe• AbleSubscribe• UnableRead• UnableWrite• UnableDelete• AbleRead• AbleWrite• AbleDelete• OtherPermissions (details MUST be provided in Comment field)
resource	MANDATORY	The resource being SUBSCRIBEd, read, written/modified, or deleted, or at which

[MM/DD/YYYY]

Page 134 of 675



Name	Condition	Description
		authentication failed (URL if available)
identity	MANDATORY	AgentID (Agent Identifier, Agent Id or AgencyID (Agency Identifier, AgencyId of entity that attempted the action
result	MANDATORY	The result returned from the requested operation
detail	OPTIONAL	Provides more detail (e.g., specifics of the security failure)

3990 The resolution parameter in a DiscrepancyResolution report contains one of the following
3991 tokens:

- 3992 • DiscrepancyCorrected
- 3993 • PerPolicy
- 3994 • BadCertificateChain
- 3995 • NoDiscrepancy
- 3996 • OtherResponse

3.7.11 GIS Discrepancy Report

3998 A LoST server or other entity MAY report a discrepancy report against GIS data. Expected
3999 reports include a gap or overlap discovered when data is coalesced, incorrect information
4000 (such as the LoST server to query for information about an area), or bad GIS data (such as
4001 bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an
4002 address range issue on centerline, a general provisioning failure, or a malformed URI).

4003 When a **GISDiscrepancyReport** is submitted, the “problemService” parameter is set to
4004 “GIS” and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none">• Gap²⁰• Overlap²⁰

²⁰ There is a gap/overlap event package used by the ECRF/LVF to notify its provisioning source of gaps or overlaps, because immediate response is required. The DR may be used to report the problems to others, such as from an SI entity to the GIS data source.

Name	Condition	Description
		<ul style="list-style-type: none"> • IncorrectLoST • BadGeometry • DuplicateAttribute • OmittedField • IncorrectDataType • AddressRange • GeneralProvisioning • MalformedURI • DisplayData (call taker noted inaccuracies in the GIS data used in the PSAP's map display) • OtherGIS
layerIds	Conditional: REQUIRED if the error is specific to a layer or set of layers	The IDs of the layers as a white-space separated list
location	Conditional: REQUIRED if the error is specific to a location or set of locations	One or more locations where the gap or overlap can be found or for which an incorrect LoST referral is made
lostUri	Conditional: REQUIRED if a URI was provisioned	The URI provisioned
detail	Conditional: REQUIRED if the problem is an item that is duplicated, omitted, or contains an incorrect data type; or if the problem concerns bad geometry, an incorrect address range, or a malformed URI.	A string containing the name of the item that is duplicated, omitted, or contains an incorrect data type; or the geometry or address range is bad; or the URI is malformed

4005 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4006 tokens:

- 4007 • DataCorrected
4008 • NoDiscrepancy
4009 • OtherResponse

4010 **3.7.12 LIS Discrepancy Report**

4011 Any client of a LIS MAY report a discrepancy. Examples include a service provider that finds
4012 a discrepancy in the LIS' provisioning records, a client (such as an originating device)
4013 unable to obtain its own location value or reference, a client (such as an ESRP or PSAP)
4014 unable to resolve a location reference or receiving a badly formed PIDF-LO, or a PSAP call
4015 taker receiving an incorrect civic address (as verified by the call taker with the caller).

4016 When a **LISDiscrepancyReport** is submitted, the "ProblemService" parameter is set to
4017 "LIS" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • IncorrectRecords • OwnLocationUnavailable • LocationReferenceNotReso lved • BadPIDFLO • IncorrectLocation (incorrect civic location supplied with wireline (fixed) call) • OtherLIS
ownLocationRequest	Conditional: REQUIRED when problem is OwnLocationUnavailable	The request sent by a device for its own location
locationUrn	Conditional: REQUIRED when a location was returned by reference	The location reference
pidfLo	Conditional: REQUIRED for BadPIDFLO, SHOULD be supplied when a location was returned by value	The (possibly badly formed) PIDF-LO

[MM/DD/YYYY]

Page 137 of 675



4018 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4019 tokens:
4020 • RecordsCorrected
4021 • PermissionsCorrected
4022 • DeviceConfigError
4023 • PerPolicy
4024 • NoDiscrepancy
4025 • OtherResponse

4026 **3.7.13 Policy Discrepancy Report**

4027 Any entity (such as an ESRP) using a policy (such as a routing policy) MAY report a
4028 discrepancy against the owner of the policy (e.g., a PSAP or an ESRP). For example, an
4029 ESRP or ECRF MAY report a routing policy that results in an invalid route URN, or routes to
4030 an unknown PSAP, or where the route conflicts with other policies. A PSAP receiving an
4031 incorrectly routed call MAY report that a policy is causing calls to be routed to it in error. A
4032 Policy Store MAY report a policy that is malformed or creates a loop or that fails signature
4033 verification. Any Policy Enforcement Point MAY report a policy that is malformed or
4034 conflicting or that fails signature verification.

4035 When a **PolicyDiscrepancyReport** is submitted, the "problemService" parameter is set to
4036 "Policy" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • InvalidURN • UnknownPSAP • ConflictingRoute • OtherConflict • IncorrectURN • Malformed • Loop • VerificationFailure • OtherPolicy (details REQUIRED in the Comment field)
policyId	MANDATORY	The policy ID
location	Conditional: REQUIRED if DR is against a PRR policy	The location

[MM/DD/YYYY]

Page 138 of 675



Name	Condition	Description
callId	Conditional: REQUIRED if DR is specific to a call	Call Tracking Identifier
routeUrn	Conditional: REQUIRED if DR is against a PRR policy	The route URN

4037 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4038 tokens:

- 4039 • PolicyCorrected
4040 • NoError
4041 • NoDiscrepancy
4042 • OtherResponse

4043 **3.7.14 Originating Service Provider Discrepancy Report**

4044 An entity MAY report a discrepancy against an Originating Service Provider when a location
4045 provided by the Originating Service Provider fails validation. An ECRF or ESRP or PRF or
4046 PSAP MAY report a discrepancy when a default location is used for routing because location
4047 is missing or not usable. An LNG or other entity MAY report a call received without ANI. An
4048 LNG or ESRP or other entity MAY report that a badly formed PIDF-LO was received or a
4049 location query timed out without receiving a PIDF-LO. An LSRG or other entity MAY report
4050 that a call was dropped or terminated without appropriate signaling. A PSAP MAY report a
4051 discrepancy when a civic location received with a fixed (wireline) call is incorrect. A BCF,
4052 ESRP, PSAP, or other entity MAY report an incorrectly formed call (e.g., a SIP INVITE that
4053 is badly formed, lacks certain header fields or body parts, etc.). A BCF, ESRP, PSAP, or
4054 other entity, MAY report that an unusually large call volume (which might suggest a DoS or
4055 other attack) or an unusually low call volume is being generated by the Originating Service
4056 Provider. An Originating Service Provider MAY report a discrepancy against itself to raise an
4057 issue to be addressed. An entity MAY report a discrepancy when an Additional Data
4058 reference included in the call is invalid. An entity MAY report a discrepancy when an
4059 Additional Data value is invalid. The Secure Telephone Identity-Verification Service (STI-
4060 VS) FE [ref Section 4.21] MAY report a Secure Telephone Identity verification failure to an
4061 Originating Network.

4062 **Note:** A Discrepancy Report by an OSP toward the OCIF reporting an identity verification
4063 failure for a call from the OCIF will be addressed in a future edition of this document.

4064 When an **OriginatingServiceDiscrepancyReport** is submitted, the "problemService"
4065 parameter is set to "OriginatingService" and the object contains the following elements:

[MM/DD/YYYY]

Page 139 of 675



Name	Condition	Description
problem	MANDATORY	<p>One of the following tokens:</p> <ul style="list-style-type: none"> • LocationNotLVFValid • LocationMissing • NoANI • BadPIDFLO • QueryTimeOut • CallDropped • IncorrectLocation • BadSIP (problem details REQUIRED in Comment field) • CallDrought • CallFlood (service provider is sending too many calls, there may be a DoS attack, or other problem to investigate) • InvalidADR • BadAdditionalData • OtherOSP • STIerror
status	Conditional: REQUIRED when using InvalidADR or STIerror	<p>For InvalidADR, the status code returned with the rejection of the ADR dereference attempt.</p> <p>For STIerror, the status code returned in the Reason header field when the STI Verification Service (STI-VS) encounters a validation failure (see Section 4.21.1)</p>
location	Conditional: REQUIRED when DR relates to location associated with the call	The location value or reference provided by the Originating Service Provider. If there is no location, leave empty.
locationId	Conditional: REQUIRED when DR relates to location associated with the call	The client or endpoint identifier provided with the location

Name	Condition	Description
locationCorrect	Conditional: REQUIRED when DR relates to location associated with the call	<p>One of the following tokens:</p> <ul style="list-style-type: none"> • True (location received with the call is correct as verified by call taker with caller) • False (location received with the call is incorrect as verified by call taker with caller) • Unknown
callHeader	Conditional: REQUIRED when DR relates to a SIP header field	The header field of the INVITE or MESSAGE
callVolume	Conditional: REQUIRED when using CallDrought or CallFlood	The number of calls received within a measured period of time
callVolumeTimePeriod	Conditional: REQUIRED when using CallDrought or CallFlood	The period of time in seconds during which CallVolume calls were received

4066 The Resolution parameter in a DiscrepancyResolution report contains one of the following tokens:
 4067

- ProblemCorrected
- InvalidRecord
- NoDiscrepancy
- OtherResponse

4072 **3.7.15 Call Transfer Failure Discrepancy Report**

4073 A PSAP, LSRG, or other entity MAY report a discrepancy against a transfer entity when a transfer fails. The notification SHOULD be made to both the entity originating the transfer and the entity receiving the transfer.
 4074
 4075

4076 When a **CallTransferDiscrepancyReport** is submitted, the "problemService" parameter
 4077 is set to "CallTransfer" and the object contains the following elements:

Name	Condition	Description
callId	MANDATORY	The Call ID assigned to the call
incidentId	MANDATORY	The Incident ID associated with the call

[MM/DD/YYYY]

Page 141 of 675



Name	Condition	Description
origin	MANDATORY	The AgencyID of the originator of the transfer
status	MANDATORY	The status code received during the transfer attempt
destination	MANDATORY	The AgencyID of the recipient of the transfer

4078 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4079 tokens:

- 4080 • ProblemCorrected
- 4081 • NoDiscrepancy
- 4082 • OtherResponse

4083 **3.7.16 MSAG Conversion Service (MCS) Discrepancy Report**

4084 An LSRG or other entity MAY report a discrepancy against the MSAG Conversion Service
4085 (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR
4086 MAY also be filed when the conversion succeeded but the returned location from the MCS
4087 is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to
4088 MSAG or MSAG to PIDF-LO).

4089 When an **MCSDiscrepancyReport** is submitted, the "problemService" parameter is set to
4090 "MCS" and the object contains the following elements:

Name	Condition	Description
ServiceCall	MANDATORY	One of the tokens: <ul style="list-style-type: none">• PIDFLOtoMSAG• MSAGtoPIDFLO
pidfLo	MANDATORY	The PIDF-LO supplied to PIDFLOtoMSAG, or received from MSAGtoPIDFLO
msag	MANDATORY	The MSAG supplied to MSAGtoPIDFLO, or received from PIDFLOtoMSAG
Referral	Conditional: REQUIRED when a Referral to another MCS was returned	Referral value received from MCS
statusCode	MANDATORY	The status code received from the conversion attempt

4091 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4092 tokens:
4093 • ProblemCorrected
4094 • NoDiscrepancy
4095 • OtherResponse

4096 **3.7.17 ESRP Discrepancy Report**

4097 A PSAP or other entity MAY report a discrepancy against an ESRP when a call is received
4098 that should not have been routed to the PSAP, or the ESRP has one or more queues whose
4099 fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally
4100 be expected. A routing problem may be the result of incorrect data in the ECRF (GIS data).
4101 Calls are sent to PSAPs by ESRPs, so a PSAP should report a problem to the ESRP. The
4102 ESRP, in turn, reports any suspected GIS problems to the ECRF.

4103 When an **ESRPDiscrepancyReport** is submitted, the "problemService" parameter is set
4104 to "ESRP" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • CallReceived • EngorgedQ • CallDrought
callId	Conditional: REQUIRED when DR relates to a specific call	The Call ID assigned to the call
incidentId	Conditional: REQUIRED when DR relates to a specific Incident	The Incident ID associated with the call
pidfLo	Conditional: REQUIRED when the DR relates to a specific call	The PIDF-LO received with or via the call
queueName	Conditional: REQUIRED when the DR is due to one or more queues whose fullness is a problem; OPTIONAL when the DR is due to the PSAP receiving fewer calls than would normally be expected	The queue in question

4105 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4106 tokens:
4107

- ProblemCorrected
- GIS (GIS data incorrect; GIS DR filed)
- PerPolicy
- NoDiscrepancy
- OtherResponse

4111

4112 **3.7.18 ADR/IS-ADR Discrepancy Report**

4113 A PSAP, ESRP, ECRF, or other entity or function MAY report a discrepancy against an ADR
4114 or IS-ADR.

4115 When an **AdrDiscrepancyReport** is submitted, the “problemService” parameter is set to
4116 “ADR” and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: <ul style="list-style-type: none">• ReferenceNotResolved• Malformed• UnknownBlock• ReceivedIncorrectData (as verified by call taker with caller)• TooManyURIs (reported when an ECRF is provisioned with more URIs for a location than can be returned)• OtherADR
block	Conditional: REQUIRED if the problem relates to a specific block	The name of the block
location	Conditional: REQUIRED when a location was used to search for Additional Data	The location used to search for the Additional Data
identity	Conditional: REQUIRED for IS-ADR (as opposed to ADR)	The identity used to search for the additional data

Name	Condition	Description
url	Conditional: REQUIRED for ADR (as opposed to IS-ADR)	The additional data URI
result	Conditional: REQUIRED if a result was received from the ADR/IS-ADR	The result received from the ADR/IS-ADR

4117 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4118 tokens:

- 4119 • ProblemCorrected
4120 • NoDiscrepancy
4121 • OtherResponse

4122 **3.7.19 Network Discrepancy Report**

4123 Any entity MAY report a general networking discrepancy. For example, any entity MAY
4124 report a discrepancy with general network facilities (such as DNS or DHCP failure, high
4125 latency, packet loss, or routing failure) within an ESInet or PSAP. ESInet and PSAP
4126 operators MUST support receiving such DRs; other operators MAY support receiving them.

4127 When a **NetworkDiscrepancyReport** is submitted, the "problemService" parameter is
4128 set to "Network" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • TimeoutDNS • IncorrectDNS (incorrect results) • TimeoutDHCP • IncorrectDHCP (incorrect results) • PacketLoss • PacketLatency • Routing • OtherNetwork (details MUST be provided in Comment field)
iPAddressLocal	Conditional: REQUIRED unless DHCP related and IP address not available	The IP address of the machine experiencing the error

Name	Condition	Description
ipAddressRemote	Conditional: REQUIRED unless problem is DNS or DHCP related	The IP address to/from which the problem is occurring
url	Conditional: REQUIRED if known	The URL of the resource (e.g., the DNS or DHCP server)
timestamp	MANDATORY	The time at which the problem occurred

4129 The Resolution parameter in a DiscrepancyResolution report contains none of the following
 4130 tokens:
 4131 • ProblemCorrected
 4132 • NoDescrepancy
 4133 • OtherResponse

4134 **3.7.20 Interactive Media Response (IMR) Discrepancy Report**

4135 Any entity aware of a discrepancy at an Interactive Media Response (IMR) MAY report a
 4136 discrepancy at it. For example, a PSAP or ESRP MAY report a discrepancy if the IMR has
 4137 one or more queues whose fullness is a problem, a call taker MAY report a discrepancy if
 4138 the caller reports that an incorrect or confusing message was played, a call was transferred
 4139 incorrectly, the caller experienced excessive silence, or another script error occurred.

4140 When an **IMRDiscrepancyReport** is submitted, the "problemService" parameter is set to
 4141 "IMR" and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the following tokens: • EngorgedQ • ResponseIncorrect • ResponseConfusing • CallTransferIncorrect • ExcessiveSilence • UnknownScript • InputFailed (e.g., DTMF failure) • ScriptLogicFailure • OtherIMR (details MUST be provided in Comment field)
callId	MANDATORY	The Call ID assigned to the call

Name	Condition	Description
incidentId	Conditional: REQUIRED if used for an emergency call	The Incident ID associated with the call
callHeader	MANDATORY	The header field of the INVITE or MESSAGE

4142 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4143 tokens:

- 4144 • ProblemCorrected
- 4145 • NoDescrepancy
- 4146 • OtherResponse

4147 **3.7.21 Test Call Generator Discrepancy Report**

4148 When a Test Call Generator encounters errors initiating or processing a test call, it reports
4149 the discrepancy to the PSAP that should have received the test call.

4150 Note that a Test Call Generator might create other DRs in addition to or instead of this DR,
4151 and a PSAP that receives a test call might create DRs in response to the test call. For
4152 example, a Test Call Generator might file a SIP or IMR DR against a receiving PSAP
4153 whether or not it is the expected PSAP, as problems in its handling of the test call could
4154 warrant generating a DR against it regardless. Similarly, a Test Call Generator or a PSAP
4155 that receives a test call might create a Policy or ESRP DR if the test call was routed
4156 unexpectedly.

4157 The expected cases for this Discrepancy Report are:

- 4158 • an initial INVITE request failed;
- 4159 • a MESSAGE request failed;
- 4160 • an OPTIONS request failed;
- 4161 • a SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed;
- 4162 • loopback media stream (audio, text, video) failed to be accepted;
- 4163 • loopback media problems during the test dialog;
- 4164 • signaling failure.

4165 When a **TestCallDiscrepancyReport** is submitted, the "problemService" parameter is set
4166 to "TestCall" and the object contains the following elements:

4167

Name	Condition	Description
problem	MANDATORY	One of the tokens: • TestINVITE

[MM/DD/YYYY]

Page 147 of 675



Name	Condition	Description
		<ul style="list-style-type: none"> • TestMESSAGE • TestOPTIONS • TestMidDialog • TestMedia • TestLoopbackMedia • TestSignaling • TestCallOther
callId	MANDATORY	The Call Identifier
request	MANDATORY	The SIP request
result	MANDATORY	The status code returned from the SIP request
nbrOfCalls	MANDATORY	Number of test calls placed since the last time SendCallRequests was received from this PSAP (as an integer)
successCount	MANDATORY	Number of calls counted in NbrOfCalls that were completed successfully (as an integer)
failCount	MANDATORY	Number of calls counted in NbrOfCalls that were attempted, but failed to complete (as an integer)

4168 The Resolution parameter in a DiscrepancyResolution report contains one of the following
4169 tokens:

- ProblemCorrected
- NoDescrepancy
- OtherResponse

4173 **3.7.22 Log Signature/Certificate Discrepancy Report**

4174 When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures
4175 is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the
4176 signature verification fails, it reports the discrepancy to the entity that generated the
4177 LogEvent.

4178 The expected cases for this Discrepancy Report are:

- the certificate cannot be obtained (no “x5c” nor “x5u” field provided);

[MM/DD/YYYY]

Page 148 of 675



- 4180 • the “x5u” field cannot be resolved or does not resolve to a valid certificate;
 4181 • the “x5u” field is present but the “x5t#256” field is missing, or the thumbprint
 4182 specified does not match the certificate obtained from the “x5u” field;
 4183 • the signature of a LogEvent does not verify.

4184 When a **LogSignDiscrepancyReport** is submitted, the “problemService” parameter is set
 4185 to “LogSign” and the object contains the following elements:

Name	Condition	Description
problem	MANDATORY	One of the tokens: <ul style="list-style-type: none"> • BadAlgorithm (“alg” header was not set to “ES256”) • NoCert (neither “x5u” nor “x5c” fields present) • BadURL (unable to resolve the “x5u”) • BadThumb (an “x5u” field was present, but the “x5t#S256” field is either missing or doesn’t match the certificate obtained by resolving the “x5u” field) • BadCertX5c (invalid certificate in the “x5c” field) • BadCertX5u (invalid certificate obtained via the “x5u” field) • BadSignature (unable to verify signature) • OtherLogSignature
logEventId	MANDATORY	The logEventId of the LogEvent.
result	Conditional: REQUIRED if Problem is BadURL	The response received when resolving the “x5u” field.
thumbCalc	Conditional: REQUIRED if Problem is BadThumb	The thumbprint calculated from the certificate

4186 The Resolution parameter in a DiscrepancyResolution report contains one of the following
 4187 tokens:
 4188 • ProblemCorrected

[MM/DD/YYYY]

Page 149 of 675



- 4189 • NoDescrepancy
4190 • OtherResponse

4191 **4 Functions**

4192 **4.1 Border Control Function (BCF)**

4193 A BCF MUST be deployed between external networks and the ESInet/NGCS. A BCF
4194 SHOULD be deployed between the ESInet/NGCS and agency networks. The latter may be
4195 provided by the NGCS operator or may be provided by the PSAP, or both.

4196 **4.1.1 Functional Description**

4197 The BCF comprises several distinct elements pertaining to network edge control and SIP
4198 message handling. These include:

- 4199 • Border Firewall
4200 • Session Border Control
4201 • Call Suspicion/Bad Actor functions

4202 The BCF MUST support the following security related techniques:

- 4203 • Prevention
4204 • Detection
4205 • Reaction

4206 Additionally, the entirety of the functional element MAY include aspects of the following:

- 4207 • SIP B2BUA
4208 • Media anchoring
4209 • Stateful Firewall

4210 Border Firewall — this functional component of the BCF inspects ingress and egress traffic
4211 running through it. It is a dedicated appliance or software running on a computer. There
4212 are a variety of different roles a firewall can take; however, the typical roles are application
4213 layer and network layer firewalls:

- 4214 1) Application layer – these scan and eliminate known malware attacks from extranet
4215 and intranet sources at OSI layer 7 before they ever reach a user's workstation or a
4216 production server or another end point located inside the ESInet. These act as the
4217 primary layer of defense for most malware attacks that are protocol specific.
- 4218 2) Network layer — these manage access on the network perimeter and between
4219 network segments. Typically, they do not provide active scanning at the application
4220 layer and provide access control through the use of access control lists and port-

4221 based permission/denial management (UDP, TCP etc.). They also mitigate attacks
4222 on lower layer protocol layers (e.g., TCP SYN Flooding).

4223 Firewalls deployed on the ESInet SHALL meet the following specifications:

- 4224 1) Provide both application and network layer protection and scanning;
- 4225 2) Denial of Service (DoS) detection and protection;
 - 4226 a. Detection of unusual incoming IP packets that may then be blocked to protect
4227 the intended receiving user or network;
 - 4228 b. To prevent distributed denial of service (DDoS) attacks, destination specific
4229 monitoring, regardless of the source address, may be necessary.
- 4230 3) Provide a mechanism such that malware definitions and patterns can be easily and
4231 quickly updated by a national 9-1-1 Computer Emergency Response Team (CERT) or
4232 other managing authority;
- 4233 4) Capability to receive and update 9-1-1 Malicious Content (NMC) filtering
4234 automatically for use by federated firewalls in protecting multiple disparate ESInets.

4235 Please refer to NENA 04-503 [71] for more information on firewall requirements.

4236 Session Border Control — The session border controller functional element of the BCF plays
4237 a role by controlling borders to resolve problems such as Network Address Translation
4238 (NAT) or firewall traversal. Session Border Controllers (SBCs) are already being extensively
4239 used in existing service provider networks.

4240 Commercial Off The Shelf SBCs and Firewalls may be extended to have NGCS-specific
4241 capability, or a separate functional component may provide that functionality.

4242 The following primary functions are related to the SBC (or the NGCS-specific functional
4243 component within a BCF):

- 4244 • Identification of emergency call/session and priority handling for the IP flows of
4245 emergency call/session traffic. Use of the SBC or any other ESInet element for non-
4246 emergency calls that enter an ESInet is not described herein except for calls to an
4247 administrative number in the PSAP. Such non-emergency calls are beyond the scope
4248 of this document.
- 4249 • Conformance checking and mapping (if applicable) of priority marking based on
4250 policy for emergency calls/sessions.
- 4251 • Facilitate forwarding of an emergency call/session to an ESRP (and only an ESRP).
- 4252 • Adding Call and Incident Tracking identifiers to the signaling.
- 4253 • Adding the Resource-Priority header field if not already included.
- 4254 • Protection against DDoS attacks: The SBC component of the BCF shall protect
4255 against SIP specific and general DDoS attacks.
- 4256 • Implementing the “Bad Actor” mechanism as described in Section 4.1.2.

- 4257 • SIP Protocol Normalization: The SBC component of the BCF SHALL support SIP/SDP
4258 protocol normalization and/or repair, including adjustments of encodings to a core
4259 network profile. This may be done in order to facilitate backward compatibility with
4260 older devices that may support a deprecated version of SIP/SDP. The “lr” parameter
4261 should be added to the routing URIs if not already present.
- 4262 • NAT and Network Address and Port Translation (NAPT) Traversal: The SBC
4263 component of the BCF SHALL perform NAT traversal for authorized calls/sessions
4264 using the SIP protocol. The SBC component MUST be able to recognize that a NAT
4265 or NAPT has been performed on Layer 3 but not above and correct the signaling
4266 messages for SIP.
- 4267 • IPv4/IPv6 Interworking: The SBC component of the BCF SHALL enable interworking
4268 between networks utilizing IPv4 and networks using IPv6 through the use of dual
4269 stacks, selectable for each SBC interface. All valid IPv4 addresses and parameters
4270 SHALL be translated to/from the equivalent IPv6 values.
- 4271 • Signaling Transport Protocol Support: The SBC component of the BCF SHALL
4272 support SIP over the following protocols: TCP, UDP, TLS-over-TCP, and SCTP.
4273 Protocols supported MUST be selectable for each SBC interface to external systems.
4274 These transport layer protocols are generated and terminated at each interface to
4275 external systems (i.e., there is no “pass-thru” of transport layer information). The
4276 signaling for all calls entering the ESInet should be protected over TLS using AES-
4277 256 or better. The SBC component of the BCF MUST use TLS with AES-256 or better
4278 towards the ESInet.
- 4279 • VPN Bridging or Mediation: The SBC component of the BCF SHALL support
4280 terminating the IP signaling received from a foreign carrier onto the ESInet address
4281 space. The SBC component of the BCF SHALL support B2BUA functions to enable
4282 VPN bridging if needed.
- 4283 • QoS/Priority Packet Markings: The SBC component of the BCF SHALL be capable of
4284 populating the layer 2 and layer 3 headers/fields, based on call/session type (e.g.,
4285 9-1-1 calls) in order to facilitate priority routing of the packets.
- 4286 • Call Detail Records: The SBC component of the BCF SHALL be capable of producing
4287 CDRs based on call/session control information (e.g., SIP/SDP). These CDRs can be
4288 used to manage the network and for Service Level Agreement (SLA) auditing.
- 4289 • Transcoding: The SBC component of the BCF MAY support transcoding. For
4290 example, the SBC component MAY transcode Baudot tones to RFC 4103 [85] real-
4291 time text. See Section 3.1.9.3.
- 4292 • Media Protection: The media of all calls entering the ESInet should be protected
4293 against eavesdropping, alteration, and replay using SRTP with AES-256 or better. All
4294 media connections exiting the SBC towards the ESInet MUST be protected against
4295 eavesdropping, alteration, and replay using AES-256 or better. An SBC component

4296 of the BCF which always anchors media achieves this by accepting any media, with
4297 SRTP or not, and MUST protect the media towards the ESInet. An SBC that does not
4298 routinely anchor media MUST anchor media for calls entering without sufficient
4299 protection (AES-256 or better) and MUST protect the media towards the ESInet.

4300 Additionally, the SBC component of the BCF SHALL perform the following functions:

- 4301 • Opening and closing of a pinhole (firewall)
 - 4302 o Triggered by signaling packets, a target IP flow is identified by "5-tuples"
4303 (i.e., source/destination IP addresses, source/destination port number, and
4304 protocol identifier) and the corresponding pinhole is opened to pass through
4305 the IP flow.
- 4306 • Resource and admission control
 - 4307 o For links directly connected to the element, and OPTIONALLY networks
4308 behind the element, resource availability is managed and admission control is
4309 performed for the target call/session.
- 4310 • IP payload processing
 - 4311 o Transcoding (e.g., between G.711 and G.729) and DTMF interworking.
- 4312 • Performance measurement
 - 4313 o Quality monitoring for the target IP flow in terms of determined performance
4314 parameters, such as delay, jitter, and packet loss. Performance results may
4315 need to be collected for aggregated IP flows.
- 4316 • B2BUA for UAs that do not support Replaces
 - 4317 o The SBC component MAY include a B2BUA function for 9-1-1 calls in which
4318 the caller does not indicate support for the Replaces operation. See Section
4319 4.7.1.2.

4320 Typically, the firewall passes traffic for inbound SIP protocol to the Session Border
4321 Controller, which acts as an Application Layer Gateway for SIP. Primary non-SIP protection
4322 is accomplished by the Firewall functions of the BCF. Primary SIP protection is
4323 accomplished by the SBC component of the BCF.

4324 BCFs between the NGCS and a PSAP only need some of the above functionality.

4325 **4.1.2 Interface Description**

4326 The BCF supports SIP interfaces upstream and downstream per Section 3.1. The BCF, as
4327 the first active SIP element in the path of an emergency call, MUST add to the call the
4328 NENA Call Identifier, NENA Incident Tracking Identifier and a SIP Resource-Priority header
4329 field with a value from the "esnet" namespace (if not already present). These identifiers
4330 MUST be added to the initial message of a dialog forming transaction (INVITE) or the
4331 MESSAGE method associated with a non-interactive call. The identifiers SHOULD be added
4332 to all other SIP messages presented to the NGCS. The BCF SHALL police SIP Resource-
4333 Priority to appropriate values in the "esnet" namespace (See Section 3.1.7).

4334 The BCF SHALL support an automated interface that allows a downstream element to mark
4335 a particular source of a call as a "bad actor" (usually due to receipt of a call that appears to
4336 be part of a deliberate attack on the system) and send a message to the BCF notifying it of
4337 this marking. To facilitate this notification, the BCF SHALL insert a Call-Info header field
4338 with a purpose parameter of "emergency-source" in the outgoing INVITE message
4339 associated with every call. Because the SBC component of the BCF MAY rewrite addresses,
4340 calls MUST be marked by the SBC component in a way that allows the recipient to identify
4341 the BCF that processed the call. The source-ID is formatted as follows: <unique source-
4342 id>@<domain name of BCF> (e.g., "a7123gc42@sbc22.example.net"). It is common to
4343 have more than one SBC for a particular call source. The notification MUST be propagated
4344 to all such SBCs. The mechanism for doing so is not specified.

4345 Note: this construction does not specify a scheme and the lack of a scheme is not
4346 conformant to RFC 3261. This will be fixed in a future version of this document.

4347 Note: This construction does not conform to RFC 3261 (which requires a proper URL with a
4348 scheme). This will be addressed in a future version of this document.

4349 When the downstream element identifies a source as a "bad actor", it signals the BCF as to
4350 which source is misbehaving by sending it a BadActorRequest that contains the sourceId
4351 from the Call-Info header field with a 'purpose' parameter of "emergency-source" of the
4352 incoming INVITE message or MESSAGE request. The BCF responds by returning a
4353 BadActorResponse message that indicates whether or not an error was detected in the
4354 BadActorRequest message.

4355 Upon receiving the BadActorRequest, the SBC component of the BCF SHOULD, subject to
4356 local regulation, filter out subsequent calls from that source until the attack subsides.
4357 Provisioning determines whether the BCF deploys BadActor filtering. As an alternative to
4358 blocking calls, the Call Suspicion score (see Section 4.1.2.1 may be raised by a provisioned
4359 value.

4360 Note that blocking of emergency calls is a complex issue that may involve local regulation,
4361 liability issues and other legal implications. Use of this function may be restricted by such
4362 issues. Also note that a rogue actor within an ESInet could hinder calls for one or more
4363 PSAPs inappropriately. The BCF SHOULD restrict access to the mechanism to entities with a
4364 PSAP agency type in their PCA-traceable certificates. Source-Ids MUST be unguessable. If
4365 the BCF does not recognize the source-id, it MUST ignore the request.

4366 HTTP method: POST

4367 Resource name .../BadActors

4368 The request body contains the Bad Actor source-id as a string

4369 Status Codes

4370 201 Bad Actor successfully added

4371 401 Unauthorized

4372 432 Already reported

4373 433 No such sourceId

4374 454 Unspecified Error

4375 BCFs that anchor media MUST implement the Session Recording Client interface defined by
4376 SIPREC (RFC 7866) [116]. Provisioning MAY control whether the BCF logs media.

4377 Disabling BadActor filtering for a specific source is based on time and is implementation
4378 dependent. Frequency of calls from the source, types of calls, and prior history may
4379 determine how long the filtering is maintained.

4380 **4.1.2.1 CallSuspicion**

4381 The BCF MAY identify calls that may be part of a deliberate attack on the system. However,
4382 under normal conditions, the BCF will allow suspicious calls in, preferring to have a
4383 suspicious call show up rather than blocking a potentially legitimate call. The behavior of
4384 downstream elements (ESRPs for example) may be affected by the determination of the
4385 BCF. For this purpose, if the BCF evaluates suspicion, it SHALL insert a Call-Info header
4386 field with a purpose parameter of "emergency-CallSuspicion", with an integer value of 0-
4387 100 indicating the call suspicion score where 0 is least suspicious (i.e. no suspicion) and
4388 100 is most suspicious. The absence of the emergency-CallSuspicion parameter in a call
4389 means no determination was made.

4390 Note: This text does not describe how an integer is formatted in a Call-Info URL in
4391 conformance with RFC 3261. This will be addressed in a future version of this document.

4392 **4.1.3 Roles and Responsibilities**

4393 The ESInet operator is responsible for the BCF at the edge of the ESInet. PSAP or other
4394 agency is responsible for a BCF between its network and the ESInet.

4395 **4.1.4 Operational Considerations**

4396 Creation of a Public Safety Computer Emergency Response Team (CERT) is anticipated,
4397 and all BCF operators MUST arrange to receive alerts from the CERT and respond. All BCF
4398 support organizations MUST have trained staff available 24 x 7 x 365 to immediately
4399 respond to attacks and have the capability and training to be able to adjust the BCF to
4400 mitigate such attacks.

[MM/DD/YYYY]

Page 155 of 675



4401 **4.2 Emergency Service Routing Proxy (ESRP)**

4402 **4.2.1 Functional Description**

4403 **4.2.1.1 Overview**

4404 The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency
4405 calls for i3. As described in NENA 08-002 [70], ESRPs are used in several positions within
4406 the ESInet:

- 4407 • The "Originating ESRP" is the first routing element inside the ESInet. It receives calls
4408 from the BCF at the edge of the ESInet;
- 4409 • One or more "Intermediate ESRPs" which exist at various hierarchical levels in the
4410 ESInet. For example, the Originating ESRP may be a state-level function, and an
4411 intermediate ESRP may be operated by a county agency;
- 4412 • The "Terminating ESRP" is typically at the edge of the NGCS, just before the PSAP
4413 BCF.

4414 The function of the ESRP is to route a call to the next hop (the routing URI should contain
4415 the "lr" parameter to avoid Request-URI rewriting). The Originating ESRP routes to the
4416 appropriate intermediate ESRPs (if they exist), intermediate ESRPs route to the next level
4417 intermediate ESRP or to the Terminating ESRP (i.e., the appropriate PSAP). The
4418 Terminating ESRP routes to a PSAP's Call Handling and/or IMR FE.

4419 ESRPs typically receive calls from upstream routing proxies. For the originating ESRP, this
4420 is typically a carrier routing proxy. For an intermediate or terminating ESRP, this is the
4421 upstream ESRP. The destination of the call on the output of the ESRP is conceptually a
4422 queue, represented by a Queue Identifier. In most cases, the queue is maintained on a
4423 downstream ESRP, and is most often empty. However, when the network gets busy for any
4424 reason, it is possible for more than one downstream element to "pull" calls from the queue.
4425 The queue is most often First In First Out, but in some cases there can be out-of-order
4426 selections from the queue.

4427 The primary input to an ESRP is a SIP message. The output is a SIP message with a Route
4428 header field (possibly) rewritten (this URI should contain the "lr" parameter to avoid
4429 Request-URI rewriting), a Via header field added, and in some cases, additional
4430 manipulation of the SIP messages. In order for the Policy Routing Function (PRF) to
4431 evaluate and execute its rules, the ESRP has interfaces to the ECRF (for location-based
4432 routing information), LISes and ADRs, as well as to various event notification sources to
4433 gather state information.

4434 For typical 9-1-1 calls with a Request-URI starting with "urn:service:sos" received, the
4435 ESRP will:

[MM/DD/YYYY]

Page 156 of 675



- 4436 1) Evaluate an origination policy “rule set” (`OriginationRoutePolicy`) for the queue the
4437 call arrives on;
- 4438 2) Query the location-based routing function (ECRF) with the location included with the
4439 call (including any steps to dereference location included by reference) to determine
4440 the “normal” next hop (smaller political or network subdivision, PSAP, or call taker
4441 group) URI²¹;
- 4442 3) Evaluate a policy rule set (`NormalNexthopRoutePolicy`) triggered by an
4443 `InvokePolicyAction` using other inputs available to it such as header fields in the SIP
4444 message, time of day, PSAP state, etc.
- 4445 `InvokePolicyAction` may also be used to cause the ESRP to execute another policy
4446 (`OtherRoutePolicy`).
- 4447 The result of the policy rule evaluation is a URI. The ESRP forwards the call to the URI
4448 (which is a queue as described above).
- 4449 If the call arrives at an ESRP with no queue name or a queue name that the ESRP does not
4450 implement, the ESRP SHALL use a provisioned default queue for the call.
- 4451 The ESRP also has a SIP interface to the STI-VS FE (see section 4.21.1) for the purpose of
4452 validating the telephone identity of emergency calls presented to it.
- 4453 The ESRP MAY also handle calls to what used to be called “administrative lines”, meaning
4454 calls directed to, for example, a 10 digit number listed for a particular PSAP, although in
4455 NG9-1-1, they may be multimedia calls, and may be to a more general SIP URI. It is
4456 recommended that such calls route through the Outbound Call Interface Function (OCIF) of
4457 the serving NGCS (potentially through an Originating ESRP) to a next-hop ESRP, and be
4458 subject to the same security and policy routing as regular 9-1-1 calls. Such calls do not
4459 have a service URN in the Request-URI line, do not have Geolocation header fields, would
4460 typically arrive on a different queue with a different origination policy, would not query an
4461 ECRF, and would use a fixed URL for “Normal-Next Hop”.
- 4462 It is desirable in many circumstances for calls to be policy-routed instead of being sent
4463 directly to a PSAP, that is, the INVITE or MESSAGE should be sent to the ESRP instead of
4464 directly to the PSAP. This allows for testing various conditions (e.g.,
4465 ServiceState/SecurityPosture, TimeOfDay, etc.) at the PSAP prior to sending the call there.
4466 To accomplish this, it is RECOMMENDED that the URI in the ECRF for that PSAP MUST
4467 treat such calls the same way it treats all other calls arriving on queues it manages, that is,
4468 it evaluates the `OriginationRoutePolicy` associated with that queue. That PRR ruleset

²¹ The ECRF query is invoked as part of rule evaluation. A given rule set need not invoke an ECRF query, but all ESRPs must implement the capability to query an ECRF

however, should not cause an ECRF query. If calls transferred to a PSAP are to be policy-routed, then the URI in the ECRF SHALL point to a queue. Note that the responders may have URIs in the ECRF that are different from a URI found in, for example, the Agency Locator, which may follow different paths. Responders SHOULD use route policy for handling unusual circumstances that may require calls to be forwarded to alternative agencies, but they are NOT REQUIRED to do so. ESRPs which do not have a policy for the Route header field in this circumstance forward the call to the domain specified in the Route header field with no further processing.

A serving ESRP is usually the default outbound proxy for calls originated by a PSAP. When the ESRP is not configured as the default outbound proxy for the PSAP, the OCIF MAY be contacted directly, if so configured by the NGCS provider. An ESRP routes calls within the ESInet, and routes calls to destinations outside an ESInet using the OCIF. Call-backs to the original caller are an example of such outbound calls to external destinations. The ESRP routes outbound calls based on an origination policy for a provisioned ESRP queue used for calls which would route to an OCIF. While an ESRP could be an incoming proxy server for non-emergency calls, such use is beyond the scope of this standard.

Note: This section will be expanded in a subsequent version to include non-transferred calls.

4.2.1.2 Call Queuing

The destination of every routing decision is conceptually a queue of calls. The queue can be large or small, it can have one or many sources entering calls on a queue, and it can have one or many sources taking calls off the queue. All queues defined in this document are normally First In First Out, have defined maximum length and a current call-in-queue length. A unique Queue Identifier identifies a queue. A queue is normally managed by an ESRP or PSAP. A call sent to the queue URI MUST route to the entity that manages it. Calls are enqueued by forwarding them to the URI (which is usually obtained by policy rule evaluation of an upstream ESRP). Calls typically are dequeued by the ESRP, making a routing decision and sending the call to a downstream queue managed by an ESRP or PSAP. As such, all call queues are “ingress” queues, conceptually on the input side of an ESRP. In cases in which more than one dequeuer exists for a queue, one entity (normally an ESRP) manages the queue, and other ESRPs register to dequeue calls from the queue. The queue mechanism discussed here is not an “egress” queue, which would conceptually be on the output side of an ESRP. A given ESRP takes calls off its queues (or queues managed by some other entity if there are multiple dequeuers) and processes them. That ESRP will then enqueue the call on a downstream entity that manages another queue.

ESRPs may, and often will, manage multiple queues. For example, an ESRP may manage a queue that is used for normal 9-1-1 calls routed to the local ESInet, and one or more

4506 queues for calls that are diverted to it by ESRPs from other areas that are overloaded. Each
4507 queue MUST have a unique URI that routes to the ESRP. The queue length an ESRP
4508 reflects the number of calls to be routed.

4509 In practice, some proxy servers MAY be simple RFC 3261 [10] compliant servers. In such
4510 cases, the queue is considered to have a length of 1 and its existence can be ignored.

4511 The ESRP managing a queue may have policies controlling which entities may enqueue
4512 (Enquires) and dequeue (DequeueRegistration) calls to the queue. The dequeuing entity
4513 registers (DequeueRegistration) to receive calls from the queue. The ESRP would respond
4514 to a call from an entity not in its policy with a 404 error.

4515 Each ESRP element SHALL maintain a QueueState notifier and track the number of calls in
4516 queue for the queues that it manages. Changing the ServiceState MUST change the state
4517 of all Queues implemented by the Service to an appropriate QueueState (for example if
4518 ServiceState is set to Unstaffed, underlying QueueState values become Disabled). ESRPs
4519 normally are aware of downstream queue state, but do not report such status upstream.

4520 **4.2.1.3 QueueState Event Package**

4521 QueueState is an event that indicates to an upstream entity the state of a queue. The SIP
4522 Notify mechanism described in RFC 6665 [14] is used to report QueueState. The event
4523 includes the URI of the queue, the current queue length, allowed maximum length, and a
4524 state value from the queueState registry (Section 10.17).

4525 The registry includes the value "unreachable", which MUST NOT be returned in a NOTIFY.
4526 QueueState is NOT REQUIRED to be implemented on simple routing proxy or when queue
4527 length is 1 and only one dequeuer is permitted. QueueState MUST reflect the state of the
4528 (ESRP or PSAP) service state. If the ESRP is down, all of its queues MUST show a state
4529 matching the reason the service is not available.

4530 **Event Package Name:** emergency-QueueState

4531 **Event Package Parameters:** None

4532 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions filter specification may be
4533 present

4534 **Subscription Duration:** Default one (1) hour. One (1) minute to twenty-four (24) hours
4535 is reasonable.

4536 **NOTIFY Bodies:** MIME type Application/EmergencyCallData.queuestate+json

Name	Condition	Description
queueUri	MANDATORY	SIP URI of queue

Name	Condition	Description
queueLength	MANDATORY	Integer indicating current number of calls in the queue.
queueMaxLength	MANDATORY	Integer indicating maximum length of queue
state	MANDATORY	Enumeration of current queue state (e.g., Active/Inactive/Disabled)

- 4537 **Notifier Processing of SUBSCRIBE Requests:** The Notifier (i.e., the ESRP) consults the
4538 policy (queueState) to determine if the requester is permitted to subscribe. If not, the
4539 ESRP returns 603 Decline. The ESRP determines whether the queue is one of the queues
4540 managed by the Notifier. If not, the ESRP return 488 Not Acceptable Here. If the request is
4541 acceptable, the Notifier returns 200 OK.
- 4542 **Notifier Generation of NOTIFY Requests:** When state of the queue changes (call is
4543 placed on, removed from the queue, or management action/device failure changes the
4544 "state" enumeration), a new NOTIFY is generated, adhering to the filter requests.
- 4545 **Subscriber Processing of NOTIFY Requests:** Specific action NOT REQUIRED.
- 4546 **Handling of Forked Requests:** Forking between elements MUST NOT be used.
- 4547 **Rate of Notification:** This package is designed for relatively high frequency of
4548 notifications. The subscriber can control the rate of notifications using the filter rate control
4549 (RFC 6446) [80]. The default throttle rate is one notification per second. The default force
4550 rate is one notification per minute. The Notifier MUST be capable of generating NOTIFYs at
4551 the maximum busy second call rate to the maximum number of downstream dequeuing
4552 entities, plus at least 10 other subscribers.
- 4553 **State Agents:** Special handling is NOT REQUIRED.
- 4554 Race conditions exist in which a dequeued call may be sent to an entity that just became
4555 congested. A call/event sent to a queue which is Inactive or Disabled, or in which the
4556 current queue length is equal to or greater than the allowed maximum queue length, will
4557 have a Status (486 Busy Here) returned by the dequeuer. An ESRP that dequeues a call,
4558 sends it to a downstream entity, and receives a 486 Busy Here in return, MUST continue
4559 evaluating the existing rule set per Section 3.3.3.2.1. Note that the upstream ESRP MAY be
4560 configured with policy rules that will specify alternate treatment based on downstream
4561 queue state.
- 4562 ESRPs normally send calls to downstream entities that indicate they are available to take
4563 calls. "Available", however, is from the downstream entity's point of view. Network state

[MM/DD/YYYY]

Page 160 of 675



4564 may preclude an upstream entity from sending calls downstream. Normal SIP processing
4565 would eventually result in timeouts if calls were sent to an entity that never responds
4566 because the packets never arrive. Timeouts are long, however, and a more responsive
4567 mechanism is desirable to ensure that rapid response to changing network conditions route
4568 calls optimally.

4569 If active calls are being handled, the upstream entity knows the downstream entity is
4570 connected. However, some routes are seldom used, and a mechanism MUST be provided
4571 that ensures the connectedness of each entity remains known.

4572 For this purpose, relatively frequent NOTIFYs of the QueueState event are used. Successful
4573 completion of the NOTIFY is an indication to the upstream entity that calls sent to the
4574 downstream entity should succeed. The subscription may include a "force" and/or "throttle"
4575 filter (RFC 6446) [80] to control the rate of Notification.

4576 **4.2.1.4 DequeueRegistration Web Service**

4577 DequeueRegistration is a web service whereby the registering entity becomes one of the
4578 dequeuing entities, and the ESRP managing the queue will begin to send calls to it. Often,
4579 an ESRP or PSAP will manage a queue for which it is the only dequeuer; explicit
4580 DequeueRegistration for a single dequeuer is NOT REQUIRED. When there is more than
4581 one dequeuer, each dequeuer MUST register with this service. If the ESRP that manages
4582 the queue is also a dequeuer, it need not register (to itself). The registration includes a
4583 value for DequeuePreference that is an integer from 1-5. When dequeuing calls, the ESRP
4584 MUST send calls to the highest DequeuePreference entity available to take the call when it
4585 reaches the head of the queue. If more than one entity has the same DequeuePreference,
4586 the ESRP SHOULD fairly distribute calls to the set of entities with the same
4587 DequeuePreference measured over tens of minutes. The OpenAPI definition of this web
4588 service may be found in Appendix E.3. It contains one function:

4589 HTTP method: PUT

4590 Resource name .../Registration

4591 A Registration object in the body of the PUT contains:

Name	Condition	Description
queueUri	MANDATORY	SIP URI of queue on which to register
dequeuerUri	MANDATORY	SIP URI of dequeuer (where to send calls)
expirationTime	MANDATORY	Requested time in seconds this registration will expire

[MM/DD/YYYY]

Page 161 of 675



Name	Condition	Description
dequeuePreference	OPTIONAL	Integer from 1-5 indicating queuing preference.

4592 A successful response returns expirationTime

4593 Status Codes

4594 200 OK

4595 400 Bad Request

4596 554 Unspecified Error

4597 556 Bad queue

4598 557 Bad dequeuePreference

4599 558 Policy Violation

4600 The expirationTime in the response is the actual expiration, which may be equal to or
4601 greater than that in the request depending on the local policy (DequeueExpirationTime) of
4602 the ESRP. A request expirationTime of zero is a request to deregister. The entity managing
4603 the queue has a policy (DequeueRegistration) of identifying which elements are permitted
4604 to register to be a dequeuer. The policy may include specific entities, or classes of entities,
4605 appropriate for the queue.

4606 4.2.1.5 Policy Routing Function

4607 Policy Routing refers to the determination of the next hop a call or event is forwarded to by
4608 an ESRP. The PRF evaluates one or more policy rule sets, whose syntax is described in
4609 Section 3.3.3: one set determined by the queue the call arrives on; a second may be
4610 determined by the result of an ECRF query with the location of the caller. One policy may
4611 invoke another policy.

4612 The PRF in an ESRP accepts calls directed to a specific queue URI. (Any SIP URI that leads
4613 to an ESRP is considered a queue URI.) It extracts its own "RoutePolicy" from its Policy
4614 Store for that URI and executes the rule set. Usually at least one of the rules in the ruleset
4615 includes a condition LostServiceURN(<urn>) where <urn> is a service URN (either
4616 urn:service:... or urn:emergency:service:...). Upon encountering the
4617 LostServiceUrnCondition, the PRF queries its (configured) ECRF with the location received
4618 with the call using the <urn> parameter in the condition. If multiple location objects are
4619 presented with the call, the ESRP selects one, following the advice in Section 3.2 to be
4620 used for the ECRF query. If the query is successful, the resulting URI becomes the value of
4621 the variable "Normal-NextHop". The rule that has the LostServiceUrnCondition MUST
4622 contain an action "InvokePolicyAction" which uses the NormalNexthopRoutePolicy for

[MM/DD/YYYY]

Page 162 of 675



4623 <policyType>, and results in executing the rule set associated with the policy identified by
4624 the Normal-NextHop URI.

4625 The destination of a Route action is the URI of a queue. The PRF has access to queue state
4626 of downstream entities and can use that state in evaluating rules. Rules normally have a
4627 Route action that sends the call to a queue that is available and not full. A Route may also
4628 be a URI that points to an Interactive Media Response system conforming to RFC 4240
4629 [34], which plays an announcement (in the media negotiated by the caller) and potentially
4630 accepts responses via DTMF, KeyPress Markup Language (RFC 4730) [156], or other
4631 interaction styles.

4632 Other Actions that may occur in a NormalNexthopRoutePolicy include Busy and Notify. By
4633 using these mechanisms, the full range of call treatments can be applied to any class of call
4634 for any circumstance based on the PRF rule set.

4635 Rules have a priority. If more than one rule evaluates to true, the rule with the highest
4636 priority prevails.

4637 Usually, there is a generic rule for use when everything is in normal status. Most calls will
4638 route via this rule, for example, "IF True THEN
4639 InvokePolicyAction(NormalNexthopRoutePolicy)". Other rules exist for unusual
4640 circumstances.

4641 In congestion for typical transient overload, a specific PSAP would be delegated to take
4642 diverted calls (via a rule other than the generic rule). A call is said to be diverted when it is
4643 sent to a PSAP other than the one serving the location of the caller, usually due to some
4644 failure or overload condition. A queue may be established for that route, with one target
4645 PSAP. Such a diversion PSAP would be accepting calls on its normal queue as well as the
4646 diversion queue. Its rules can differentiate such calls from the queue on which they arrive.

4647 For more extensive overload, a group of PSAPs would subscribe to take calls from a
4648 designated queue. For example, all PSAPs in neighboring counties might subscribe to a
4649 queue that has a low priority rule that enqueues calls to it for overload from a county
4650 PSAP. Similarly, all NG9-1-1 PSAPs in a state might dequeue for a "Denial of Service Attack"
4651 queue, or interstate queues may be established that have a "ripple" effect (using priority)
4652 to spread calls out when the state queue becomes busy. These queues are maintained by
4653 the ESRP. The ESRP dequeues a call from the queue on which it arrived, and enqueues it
4654 to the lower priority queue from which the multiple PSAPs will dequeue.

4655 ESRPs managing a queue may receive calls from one or more upstream entities.
4656 Origination rules at the ESRP can govern how such calls are handled, as the URI used to
4657 get the call to the ESRP (which could be the name of a queue maintained at the ESRP) is
4658 an input to the PRF. When handling diverted calls, no ECRF dip may be needed. In such a

4659 case, the origination policy rule set would determine the route. PSAPs may dequeue for
4660 multiple call queues managed by it or other entities, placing them on internal queues for
4661 call takers.

4662 **4.2.1.6 ESRPnotify Event Package**

4663 The ESRP sends a Notify for this event when the PRF encounters a Notify action. It is used,
4664 for example, to inform entities that unusual conditions have occurred, and calls are being
4665 rerouted. The ESRPnotify event is defined as follows:

4666 **Event Package Name:** emergency-ESRPnotify

4667 **Event Package Parameters:**

Name	Condition	Description
NotifyEventQueueUri	MANDATORY	URI of queue that will contain a rule with a notify action
NotifyEventEventCodes	MANDATORY	Enumeration of event codes (see below). May occur more than once

4668 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions. Filter specification may be
4669 present

4670 **Subscription Duration:** Default one (1) hour. One (1) minute to twenty-four (24) hours
4671 is reasonable.

4672 **NOTIFY Bodies:** MIME type Application/EmergencyCallData.ESRProute+json

4673 The content of the NOTIFY is contained in the table below.

4674 **ESRPnotify**

Name	Condition	Description
queueUri	MANDATORY	URI of queue that Notify action occurred on
eventCode	MANDATORY	EventCode specified in Notify Action
urgency	MANDATORY	Urgency specified in Notify Action
comment	Conditional, MUST be present if Comment is specified in Notify action	Comment specified in Notify action
callLocation	MANDATORY	Location included with the call (by value or by reference as provided in the call)

Name	Condition	Description
additionalData	Conditional, MUST be provided if AdditionalData is included with the call	Additional Data included with the call (by value or by reference as provided in the call), or retrieved using the Additional Data associated with a location mechanism, or from an IS-ADR.
esrpRule	MANDATORY	Rule that triggered the event

4675 **Note:** If the URI in the Notify action in a rule contains a service URN, then the notification
4676 is sent to the entity whose service boundary intersects the location of the caller where the
4677 service URN matches that in the Notify action.

4678 This document defines a registry, "EsrpNotifyEventCodes" which registers values that MAY
4679 be used in an <event code>. The initially defined values in the registry can be found in
4680 Section 10.19.

4681 The NotifyBodiesEsrpCondition is a string consisting of the actual rule, per standardized
4682 syntax in Section 3.3.3.

4683 **Note:** A future version of this document will describe how to include the condition values
4684 that triggered the notify in the body of the NOTIFY.

4685 **Notifier Processing of SUBSCRIBE Requests:** The Notifier (the ESRP) consults the
4686 policy (NotifyPermissions) for Normal-NextHop to determine if the requester is permitted to
4687 subscribe. If not permitted, the ESRP returns 603 Decline. The ESRP determines whether
4688 at least one policy it uses contains a Notify action with that event code. If not, the ESRP
4689 returns a 488 Not Acceptable Here. If the request is acceptable, the ESRP returns 200 OK.

4690 **Notifier Generation of NOTIFY Requests:** The <notify> action causes the ESRP to
4691 send NOTIFY to a set of entities, which have previously subscribed to the EventCode and
4692 queue. If the recipient value in the Notify action is present and contains one or more URIs,
4693 NOTIFYs are sent to all entities in the recipient list. If the recipient list contains a urn,
4694 NOTIFYs are sent to all subscribers whose service area contains at least a part of the call
4695 location and whose service URN matches the recipient value in the Notify action. If no
4696 recipients are included in the action, all subscribers for the EventCode are notified.

4697 **Subscriber Processing of NOTIFY Requests:** No specific action required.

4698 **Handling of Forked Requests:** Forking between elements MUST NOT be used.

4699 **Rate of Notification:** A notification for each call/event handled by the ESRP could be
4700 sent. Rate controls (RFC 6446) [80] MAY be used to limit Notifications.

4701 **State Agents:** No special handling is required.

[MM/DD/YYYY]

Page 165 of 675



4702 **4.2.1.7 Processing of an INVITE or MESSAGE transaction**

4703 When the ESRP receives an INVITE transaction its PRF first evaluates the Origination rule
4704 set for the queue on which the call arrived. If the queue handles emergency calls, a
4705 LoSTServiceURN condition is normally encountered, which looks for the presence of a
4706 Geolocation header field. If present, the ESRP evaluates the header field and extracts the
4707 location following the URL found in the Geolocation header field (RFC 6442) [8]. Each ESRP
4708 MUST be capable of receiving location as a value or a reference and MUST be provisioned
4709 with credentials suitable to present to any LIS in its service area to be able to dereference
4710 a location reference using either SIP or HELD. For HELD location URIs, specifying a
4711 "responseTime" attribute set to "emergencyRouting" requests an immediate response with
4712 a location suitable for routing. For SIP location URIs, a SUBSCRIBE with an "Expires"
4713 header field set to 0 requests an immediate location response without creating a
4714 subscription. See Section 3.2 for guidance if multiple location objects are presented in the
4715 emergency call.

4716 The ESRP MUST be able to handle emergency calls with problems in location. For example,
4717 this can occur if the emergency call has no Geolocation header field at all, or the
4718 Geolocation header field value is a "cid" URL pointing to an empty body part (i.e., the
4719 PIDF-LO is not present in the body). This can also occur if the location contents are
4720 malformed, the LIS cannot be contacted, the LIS refuses to dereference, the LIS returns a
4721 malformed location value, or the ESRP encounters another error that results in no usable
4722 location being available. In all such cases the ESRP MUST determine a suitable LVF-valid
4723 default location to use to route a call with location problems, as part of the
4724 LoSTServiceURN condition processing. In other words, the ESRP MUST ensure the pre-
4725 conditions as are always there for the LoSTServiceURN condition to be evaluated
4726 successfully. For example, the call source, the IP address of the caller, or other information
4727 from the INVITE MAY be used to determine the best possible default location. This
4728 procedure is based on the assumption that the earlier in call processing that bad or missing
4729 location is identified, the more likely it is that the ESRP will have the information needed to
4730 determine the best possible default location.

4731 A PIDF-LO containing a Default Location MUST have its <method> element set to the
4732 value "Default"²², and its <provided-by> element set to the identity of the NGCS provider

²² The "Default" value must be registered in the Method Token registry with IANA. The Value is "Default" and the definition is "No location can be determined, or the location provided is unusable. A default location is used."

4733 that inserted it. The location elements MUST be populated to a level that yields an
4734 appropriate route URI in the LoST response from the ECRF.

- 4735 • The ESRP SHALL perform the following procedures when handling a default
4736 location: The ESRP SHALL preserve the original Geolocation header field values and
4737 PIDF-LO documents in the original INVITE;
- 4738 • If there is no Geolocation header field, the ESRP SHALL add the default location
4739 PIDF-LO document in the body of the INVITE (to do so, the ESRP MUST behave as a
4740 B2BUA), and add a Geolocation header field populated with a "cid" URI pointing to
4741 it;
- 4742 • If there is a Geolocation header field value in the original INVITE (but no associated
4743 body part), a new one is created and placed as the top-most entry of the
4744 Geolocation field sequence;
- 4745 • If the original INVITE contained a garbled PIDF-LO, the ESRP SHALL add a new
4746 body part with the default location PIDF-LO (to do so, the ESRP MUST behave as a
4747 B2BUA) and add a new Geolocation header field with a "cid" URI pointing to it as
4748 top-most entry of the Geolocation field sequence, retaining the garbled one;
- 4749 • If the original INVITE contained a garbled location reference in the Geolocation
4750 header field, or the location dereferencing timed out or yielded a garbled PIDF-LO
4751 document, the ESRP SHALL add a new body part with the default location PIDF-LO
4752 document (to do so, the ESRP MUST behave as a B2BUA) and add a new
4753 Geolocation header field with a "cid" URI pointing to it as top-most entry of the
4754 Geolocation field sequence, retaining the garbled one;
- 4755 • Once the INVITE has been groomed with a usable location for routing, albeit a
4756 default one, the ESRP MUST reprocess the Origination-Policy rule, including the
4757 LoSTServiceURN condition. Normal call processing ensued thereafter as described
4758 below.

4759 The ESRP then queries its local (provisioned) ECRF with the location, using the service URN
4760 specified and in the LoSTServiceURN condition member. For example, an Originating ESRP
4761 receiving an emergency call from outside the ESInet, in an environment where there are no
4762 intermediary ESRPs in its service area (meaning the originating ESRP routes calls directly to
4763 the PSAP), may use the service "urn:emergency:service.sos.psap". The ECRF returns a URI
4764 for that service. If the ESRP receives an error indication from the ECRF, or the ESRP does
4765 not receive a response from the ECRF within a specified period of time, the LostServiceUrn
4766 condition evaluates as 'false', evaluation of the ruleset conditions continues. If all rules fail
4767 then the ESRP MUST invoke the Fatal Error ruleset (see section 4.2.1.6).

4768 Any rule set may include an "InvokePolicy" action. Originating rule sets will always have at
4769 least one InvokePolicy action for the Normal-NextHop URI. The PRF evaluates the rule set
4770 specified in the InvokePolicy action. The ruleset typically has rules that test information

4771 available at the ECRF (such as PSAP state, time of day, queue state, information extracted
4772 from the INVITE, etc.) The ruleset may transfer control to another ruleset. The final ruleset
4773 normally has a terminal action such as RouteAction, which causes the ESRP to attempt to
4774 forward the call to a queue URI, using the DNS to translate the URI into an IP address. If a
4775 default location is used to determine the route for the emergency call, the ESRP SHALL
4776 pass the location information received in incoming signaling forward in the outgoing SIP
4777 INVITE/MESSAGE.

4778 DNS MAY provide alternate IP addresses to resolve the URI determined by the ESRP.
4779 Normal SIP and DNS processing is used to try these alternate IP addresses. Should no
4780 entity respond, the ESRP MUST reevaluate the ruleset with the rule which failed,
4781 interpreted as not satisfying its conditions.

4782 Calls to an administrative number are recognized by the value in the To header.
4783 Administrative calls do not have location, so they MUST be routed using a provisioned table
4784 in the ESRP that associates the called number or sip URI to a URI of a queue in the ESRP.

4785 Calls that are received by an ESRP which originate inside the ESInet (acting as a default
4786 outbound proxy) are routed per normal SIP routing mechanisms. Calls destined outside the
4787 ESInet are routed to the OCIF.

4788 **4.2.1.8 Processing a BYE Transaction**

4789 An ESRP MUST process BYEs per RFC 3261 [10].

4790 **4.2.1.9 Processing a CANCEL transaction**

4791 An ESRP MUST process CANCELS per RFC 3261.

4792 If a call arrives at the ESRP but a CANCEL is received prior to any round trip from a PSAP,
4793 such that the ESRP is unsure whether the PSAP ever got an INVITE, it SHOULD notify the
4794 PSAP using the AbandonedCall event.

4795 **4.2.1.10 Processing an OPTIONS transaction**

4796 An ESRP MUST process OPTIONS transactions per RFC 3261 [10]. OPTIONS is often used
4797 as a "keep alive" mechanism. During periods of inactivity, the ESRP SHOULD periodically
4798 send OPTIONS towards its downstream entities and expect to see OPTIONS transactions
4799 from its upstream entities. If the downstream entity is not reachable, the ESRP MUST treat
4800 its queues as Inactive.

4801 **4.2.2 Interface Description**

4802 **4.2.2.1 Upstream Call Interface**

4803 The ESRP has an upstream SIP interface that typically faces a BCF for the originating ESRP
4804 or an upstream ESRP for an intermediate or terminating ESRP. This interface also is used
4805 by a PSAP for calls it originates over the ESInet. The upstream SIP call interface for the
4806 originating ESRP must only assume the minimal methods and header fields as defined in
4807 Section 3.1.1, but MUST handle any valid SIP transaction. All other ESRPs MUST handle all
4808 methods and SIP header fields. The ESRP MUST respond to the URI returned by the ECRF
4809 and/or specified in a Route action for a rule for the upstream service the ESRP receives
4810 calls from.

4811 The upstream SIP interface is also used for calls originated inside the ESInet, where the
4812 ESRP is the outgoing proxy for a PSAP it serves. Non-emergency calls originated within the
4813 ESInet are routed to the OCIF.

4814 The upstream interface on the originating ESRP MUST support UDP, TCP, and TCP/TLS and
4815 MAY support SCTP transports. The upstream interface on other ESRPs MUST implement
4816 TCP/TLS but MUST be capable of fallback to UDP. SCTP support is OPTIONAL. The ESRP
4817 SHOULD maintain persistent TCP and TLS connections to downstream ESRPs or UAs that it
4818 serves.

4819 **4.2.2.2 Downstream Call Interface**

4820 The ESRP downstream call interface typically faces a downstream ESRP for all but the
4821 terminating ESRP, which typically faces a PSAP's Call Handling FE. The downstream SIP call
4822 interface MUST implement all SIP methods to be able to propagate any method invoked on
4823 the upstream call interface. The downstream interface MAY add any header fields noted in
4824 Section 3.1.5 permitted by the relevant RFCs to be added by proxy servers. The INVITE
4825 transaction exiting the ESRP MUST include a Via header field specifying the ESRP. It MUST
4826 include a Route header field containing a URI (which should contain the "lr" parameter to
4827 avoid Request-URI rewriting) of the downstream queue that receives the call. The Request-
4828 URI remains "urn:service:sos"²³ (although the ESRP may not depend on that; a call
4829 presented to an ESRP that is not recognized as an emergency call, for example, a call to an
4830 admin line, MUST be treated as an emergency call and its occurrence logged) and it
4831 replaces the top Route header field with the next hop URI (this is described in RFC 6881

23 The request URI does not change in the outgoing SIP message, even though the service URN used to query the ECRF may not be urn:service.sos. This is done through loose routing as defined in RFC 3261 [10] where the "lr" parameter is present in URIs used for routing.

4832 [46]). The ESRP adds History-Info header field and Reason parameter header fields per
4833 Section 3.1.8 using the cause code specified in the Route action if cause is specified (which
4834 would always be the case for a diverted call).

4835 A call entering the ESInet is initially assumed to be a new Incident. Thus, the first ESRP in
4836 the path MUST add a Call-Info header field, if one is not already present, with a purpose
4837 parameter of "emergency-IncidentId" and a new Incident Tracking Identifier per Section
4838 2.1.7. The ESRP MUST also create a new Call identifier (Section 2.1.6) and add a Call-Info
4839 header field with a purpose parameter of "emergency-CallId" if one is not already present.
4840 For example:

4841 Call-Info: <urn:emergency:uid:incidentid:a56e556d871:bcf.state.pa.us>;
4842 purpose=emergency-IncidentId
4843 Call-Info: <urn:emergency:uid:callid:a56e556d871:bcf.state.pa.us>;
4844 purpose=emergency-CallId

4845 The downstream interface MUST implement TCP/TLS towards downstream elements but
4846 MUST be capable of fallback to UDP. SCTP support is OPTIONAL. An ESRP MAY NOT
4847 remove header fields received in the upstream call interface; all header fields in the
4848 upstream message MUST be copied to the downstream interface except as required in the
4849 relevant RFCs. The ESRP SHOULD maintain persistent TCP and TLS connections to
4850 downstream ESRPs.

4851 The downstream SIP interface MAY also accept calls originating within the ESInet,
4852 specifically for callback. A callback would be accepted on its downstream interface and sent
4853 towards the originating network on its upstream interface.

4854 4.2.2.3 ECRF interface

4855 The ESRP MUST implement a LoST interface towards a (provisioned) ECRF. The ESRP
4856 MUST use a TCP/TLS transport and MUST be provisioned with the credentials for the ECRF.
4857 The ESRP SHOULD maintain persistent TCP and TLS connections to the ECRF.

4858 This document defines service URNs that can be used by an ESRP to query an ECRF. These
4859 service URNs include:

URN	Use
urn:emergency:service:sos.psap	Route calls to primary PSAP
urn:emergency:service:sos.level_2_esrp	Route calls to a second level ESRP (for example, a state ESRP routing towards a county ESRP)
urn:emergency:service:sos.level_3_esrp	Route calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).

URN	Use
urn:emergency:service:sos.call_taker	Route calls to a call taker within a PSAP. Note that the call handling FE in the PSAP may handle this instead.

4860 ESRPs use these service URNs to perform finer resolution routing (e.g., state to regional,
4861 regional to psap, or other next hop). Each ESRP in the path MAY use a different service
4862 URN that relates to the hierarchy of routing within a given ESInet. The URIs returned by
4863 the ECRF using these service URNs (along with location) would be associated with queues
4864 used by downstream elements. Typically, those queues would not allow any entity other
4865 than the upstream ESRP to enqueue calls on that queue, which is specified by that queue's
4866 policy (See Section 4.2.1.4). The specific service URN used by an ESRP is specified in its
4867 origination routing policy (see Section 3.3.3.1.9). Any URN in the "urn.service.sos" (and its
4868 urn:service:test.sos equivalents) or "urn:emergency.service.sos" tree MUST be supported
4869 by all ESRPs. Loops can result if the service urns specified in the policy are not
4870 appropriately chosen.

4871 There are no other entities inside or outside the ESInet other than ESRPs (as described
4872 above) that use these specific emergency:service URNs; they normally would use
4873 "urn:service:sos". For example, a PSAP that manually corrects an erroneous location in a
4874 call that resulted in a misroute would use "urn:service:sos" to find the route to the correct
4875 PSAP, regardless of location.

4876 The ESRP MUST use the ECRF interface with the "urn:emergency:service:additionaldata"
4877 service URN when accessing Additional Data associated with a location in the evaluation
4878 of a rule set that contains an Additional Data condition, as described in Section 4.2.2.5
4879 Additional Data Interfaces. The same location used for the location-based route is used for
4880 the Additional Data query.

4.2.2.4 LIS Dereference Interface

4882 The ESRP MUST implement both SIP Presence Event Package and HELD dereferencing
4883 interfaces. When the ESRP receives a location URI (in a Geolocation header field on the
4884 upstream SIP interface) it uses the LIS dereferencing interface to obtain a location value to
4885 use in its ECRF query. The ESRP uses its PCA-issued credentials to authenticate to the
4886 LIS²⁴. The ESRP MUST use TCP/TLS for the LIS Dereferencing interface, with fallback to
4887 TCP (without TLS) on failure to establish a TLS connection. The ESRP SHOULD maintain

²⁴ The LIS must accept credentials issued to the ESRP traceable to the PCA. If a call is diverted to an alternate PSAP, it could be any willing PSAP, anywhere. The alternate PSAP must be able to retrieve location.

4888 persistent TCP and TLS connections to LISes with which it has frequent transactions. A
4889 suggested value for “frequent” is more than one transaction per day.

4890 **4.2.2.5 Additional Data Interfaces**

4891 The ESRP MUST implement mechanisms for retrieving Additional Data (RFC 7852) [107].
4892 These services are invoked when the ESRP receives a call with a Call-Info (RFC 3261) [10]
4893 header field having a “purpose” starting with “EmergencyCallData” a dot, and a block
4894 name²⁵, or from a PIDF-LO with an appropriate <provided-by> element and when directed
4895 to do so by the invoked rule set. The resulting data structure is an input to the Policy
4896 Routing Function (PRF). The ESRP MUST be able to accommodate multiple additional data
4897 services and structures for the same call.

4898 Additional Data, when passed by reference, is retrieved by dereferencing each provided
4899 URI against its associated Additional Data Repository (ADR).

4900 Multiple Call-Info header fields (or one or more Call-Info header fields containing multiple
4901 values) with a “purpose” parameter prefix of “EmergencyCallData”, a dot, and an Additional
4902 Data block name, passed by value using the Content Identifier or by reference with an
4903 HTTPS URI, may occur (e.g., when more than one originating network handles the call
4904 and/or the device itself reports data). For example, a call may have Additional Data
4905 provided by a wireless carrier as well as a telematics service provider or the device (see
4906 3.1.19 for more information about telematics calls and datasets).

4907 Additional Data is primarily accessed via the following mechanisms:

- 4908 • Through dereferencing URI(s), added to a Call-Info header field by the device,
4909 originating network, or service provider handling the call. Additional Data can be
4910 passed by reference via an HTTPS URI (referencing an external ADR) and by value
4911 via a Content Identifier (CID) URI (referencing a body part). Each by-reference
4912 Additional Data URI is dereferenced against its respective target ADR to return an
4913 Additional Data block.
- 4914 • By querying an “Identity Searchable Additional Data Repository” (IS-ADR) with the
4915 identity obtained from Caller’s From or P-Asserted-Identity header fields to retrieve
4916 any available Additional Data²⁶ blocks.

4917 Additional Data may also be retrieved by the ESRP through a location-based query
4918 executed against the ECRF. This query returns a URI for Additional Data associated with

25 e.g., purpose=EmergencyCallData.ProviderInfo

26 Refer to Section 4.11.1 Identity Searchable Additional Data Repository (IS-ADR) for further detail on the interfaces exposed by this functional element.

4919 that location. This URI is dereferenced by the ESRP against an ADR as needed by PRF
4920 rules. Any such returned Additional Data URI MAY be added in a Call-Info header field so
4921 that it can be more easily accessed by downstream systems. The location used for this
4922 query may specify an area that encompasses more than one location that has Additional
4923 Data. In that event, the ECRF returns more than one mapping, each with a URI. The ECRF
4924 is not expected to handle more than 100 mappings, and MAY truncate its response if more
4925 than 100 mappings would be returned from a query. A new warning is defined in Section
4926 3.4.10.5 for this condition.

4927 The call MAY have more than one of each block type of Additional Data. This can occur
4928 when, for example, the call is from a residence wireline telephony service in which there is
4929 more than one resident and each supplies its own Additional Data blocks or multiple service
4930 providers participate in the call. When used in a routing rule, the PRF merges multiple
4931 "like" Additional Data objects. If the merge results in conflicting information, the
4932 information identified as most recently updated by the data source shall take precedence
4933 over information determined to be older.

4934 **Note:** Using the latest data may be problematic in some situations. Making the rules for
4935 merging objects more explicit would limit cases of conflicting information. This will be
4936 covered in a future version of this document.

4937 When evaluating a rule set that contains an Additional Data condition, at minimum
4938 the ESRP accesses and evaluates against the condition criteria all Additional Data blocks
4939 that are conveyed by value or by reference via Call-Info header fields. It is
4940 implementation dependent if the ESRP also performs an ECRF query for URIs for Additional
4941 Data associated with a location and then dereferences those URIs, or queries IS-ADRs,
4942 to access and evaluate further Additional Data blocks against the Additional Data condition.

4943 Note that when retrieving Additional Data from an ADR, an HTTP Redirect may occur,
4944 which may itself lead to a redirect, etc. ESRPs should protect against excessive delay when
4945 accessing Additional Data (e.g., using timers and/or maximum redirect counters). ESRPs
4946 log resulting error situations (using the AdditionalDataResponseEvent) and may
4947 generate Discrepancy Reports against the policy owner, and if feasible, the ADR operator.

4948 **4.2.2.6 ESRP, PSAP, and Call Taker State Notification and Subscriptions**

4949 The ESRP MUST implement the client side of the ElementState and ServiceState event
4950 notification packages. The ESRP MUST maintain Subscriptions for these packages on every
4951 downstream element/service it serves. These state interfaces supply inputs to the Policy
4952 Routing Function.

4953 The ESRP MUST implement the server-side of the ElementState event notification package
4954 and accept Subscriptions for all upstream ESRPs from which it expects to receive calls. The

4955 ESRP MUST promptly report changes in its state to its subscribed elements. Any change in
4956 state that affects its ability to receive calls MUST be reported.

4957 The set of ESRPs within an NGCS MUST implement the server-side of the ServiceState
4958 event notification package. It is RECOMMENDED that if there are multiple levels of ESInet
4959 within a state, that the state level NGCS implement ServiceState as a single service, rather
4960 than having a ServiceState for each level of NGCS within the state. In such a service, if any
4961 regional or local NGCS' ESRPs are not operating properly, the state ESRP service would
4962 show some form of non-normal state for the ESRP ServiceState.

4963 **4.2.2.7 Time Interface**

4964 The ESRP MUST maintain reliable time synchronization. The time-of-day information is an
4965 input to the Policy Routing Function as well as the logging interface.

4966 **4.2.2.8 Logging Interface**

4967 The ESRP MUST implement a logging interface per Section 4.12. The ESRP MUST be
4968 capable of logging every transaction and every message received and sent on its call
4969 interfaces, every query to the ECRF, and every state change it receives or sends. It MUST
4970 be capable of logging the rule set it consulted, the rules found to be relevant to the route,
4971 and the route decision it made. Specific LogEvent records for these are provided in Section
4972 4.12.3.

4973 **4.2.2.9 AbandonedCall Event**

4974 The ESRP uses the AbandonedCallEvent to notify a PSAP that a call was started, but then
4975 cancelled prior to the PSAP responding to the INVITE. The AbandonedCall Notify is sent to
4976 the PSAP that would have received the call, had it been completed. If rule set evaluation
4977 was not complete when the call was abandoned, rule evaluation with best-effort values for
4978 conditions in the rules is completed in order to determine where to send the Notify.

4979 **Event Package Name:** emergency-AbandonedCall

4980 **Event Package Parameters:** None

4981 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions filter specification may be
4982 present

4983 **Subscription Duration:** Default one (1) hour. One (1) minute to twenty-four (24) hours
4984 is reasonable.

4985 **NOTIFY Bodies:** MIME type application/emergencyCallData.AbandonedCall+json

[MM/DD/YYYY]

Page 174 of 675



Name	Condition	Description
invite	MANDATORY	Content of INVITE message
inviteTimestamp	MANDATORY	Timestamp call was received at ESRP
cancelTimestamp	MANDATORY	Timestamp CANCEL was received at ESRP

4986 **Notifier Processing of SUBSCRIBE Requests:** The notifier consults the policy
4987 (AbandonedCall) to determine if the requester is permitted to subscribe. It returns 603
4988 (Decline) if not acceptable. If the request is acceptable, it returns 200 OK.

4989 **Notifier Generation of NOTIFY Requests:** When the ESRP receives a CANCEL for a call
4990 prior to any non-100 response received from a PSAP, such that the ESRP is unsure whether
4991 the downstream entity ever got an INVITE, a new NOTIFY is generated to the PSAP that
4992 would have received the call as determined by interpreting the ruleset, adhering to the
4993 filter requests. If there are multiple ESRPs in the path, the ESRPs before the terminating
4994 ESRP may not get the INVITE or the CANCEL, but will receive a NOTIFY from the upstream
4995 ESRP. They MUST send a NOTIFY downstream following the above process.

4996 **Subscriber Processing of NOTIFY Requests:** No specific action required.

4997 **Handling of Forked Requests:** Forking between elements MUST NOT be used.

4998 **Rate of Notification:** A series of fast INVITE/CANCEL is a possible DDoS attack. The rate
4999 of notification SHOULD be limited to a provisioned value. Three (3) per second is a
5000 reasonable limit.

5001 **State Agents:** No special handling is required.

5002 **4.2.2.10 Secure Telephone Identity Verification Service Interface**

5003 The ESRP has a SIP interface to the STI-VS FE (see section 4.21.1). The ESRP only invokes
5004 the STI-VS if an Identity header field value conforming to RFC 8224 [60] is received in
5005 incoming signaling. The ESRP MUST invoke the STI-VS before applying the RoutePolicy
5006 ruleset for the queue the emergency calls arrives on.

5007 **4.2.3 Policy Elements**

5008 The ESRP uses an RoutePolicy rule set for each queue it manages. The ESRP MUST have
5009 access to the appropriate RoutePolicy ruleset for every URI that the ECRF can return in
5010 response to a service query made by the ESRP (Normal-NextHop).

5011 The enqueuer policy (Enquers) specifies which entities can enqueue calls on the queue.

[MM/DD/YYYY]

Page 175 of 675



5012 The ESRProuteEvent Policy determines which entities may subscribe to the ESRProute
5013 Event (see Section 4.2.1.6).
5014 The QueueState policy determines which entities may subscribe to the QueueState event.
5015 The ElementState policy determines which entities may subscribe to its ElementState
5016 event.
5017 The ServiceState policy determines which entities may subscribe to its ServiceState event.
5018 The DequeueRegistration policy determines which entities may subscribe to the
5019 DequeueRegistration event.
5020 The ESRP MUST be provisioned with the policy store it uses. Use of an external Policy Store
5021 MUST be possible even if an implementation includes a Policy Store.

5022 **4.2.4 Provisioning**

5023 The ESRP is provisioned with:

- 5024 • The queues it manages;
- 5025 • The queues from which it dequeues;
- 5026 • The default locations it uses, including (potentially) one for each origination domain,
5027 and an overall default location;
- 5028 • The ECRF it uses;
- 5029 • The Logging service it uses;
- 5030 • Mappings from 10 digit PSAP telephone numbers to URIs (if the ESRP handles 10-
5031 digit calls on behalf of PSAPs);
- 5032 • The Policy Store it uses;
- 5033 • A maximum InvokePolicyAction counter value;
- 5034 • A Fatal Error ruleset.

5035 **4.2.5 Roles and Responsibilities**

5036 An ESRP may be operated by a State, Regional, or local 9-1-1 Authority. Downstream
5037 entities maintaining queues that upstream ESRPs queue calls on MUST supply a rule set for
5038 the upstream ESRP.

5039 **4.2.6 Operational Considerations**

5040 A routing rule that dereferences Additional Data from a server that is not under the control
5041 of a 9 1 1 Authority could add significant delay when processing the rule, and could
5042 increase fragility (decrease reliability).

5043 **4.2.6.1 Tactical NG9-1-1 Emergency Call Routing Changes**

5044 Tactical routing is defined as the alternate routing of calls on short notice due to an
5045 unforeseen situation. An example of such is when the footprint of a disaster is greater than
5046 previously envisioned; thus, the policies in the PRF were not designed for such a condition.
5047 Both the ECRF and the ESRP/PRF are involved in the routing of NG9-1-1 calls, leaving in
5048 question the best method of making spur-of-the-moment changes. Unfortunately, there is
5049 no clear-cut answer to this situation. The answer is highly dependent on a number of
5050 parameters, all of which are deployment-specific.

5051 **4.2.6.2 Making Changes In Policy Routing Rules**

5052 The PRF is the natural place to make changes to routing based on conditions at the time of
5053 the call. Changes made in PRR take effect on the very next call. Making the decision to
5054 make routing changes in PRR depends on a number of factors:

- 5055 • Whether it is possible to construct a rule to detect the current condition;
5056 • Ability and confidence in making routing rule changes on the fly;
5057 • In the case routing rules are under service provider control, contractual agreements
5058 or other considerations might constrain making such changes;
5059 • Ability to conduct test calls simulating the condition to validate the rule change.

5060 **4.2.6.3 Making Changes In the ECRF**

5061 When the nominal PSAP for a certain area is no longer available to take calls, the expected
5062 duration may warrant changing the nominal PSAP for the affected area(s). For example,
5063 calls to an urban PSAP may need to be distributed to a number of neighboring smaller
5064 PSAPs. An important consideration is that changes made in the ECRF may not take effect
5065 immediately, because responses to ECRF queries can be cached and reused as specified in
5066 the 'expires' field of the response. It is important to consider the following: the operational
5067 parameters of the ECRF that affect the 'expires' value; the operational processes involved
5068 in making changes to the ECRF; what value was configured in the ECRF; and the treatment
5069 calls will receive until such time that the changes fully take effect. It may be necessary to
5070 modify the policy rules to cover the interim period.

5071 **4.3 Emergency Call Routing Function (ECRF) and Location Validation Function**
5072 **(LVF)**

5073 In i3, emergency calls are routed to the appropriate PSAP based on the location of the
5074 caller²⁷. In addition, PSAPs may utilize the same routing functionality to determine how to
5075 direct emergency calls to the correct responder. The NG9-1-1 functional element
5076 responsible for providing routing information to the various querying entities is the
5077 Emergency Call Routing Function (ECRF).

5078 The NENA NG9-1-1 solution MUST properly route incoming IP packet-based emergency
5079 calls to the appropriate or designated PSAP, as well as support the dispatch of responders
5080 to the right location. The location information used, when provided in civic form, MUST be
5081 proved sufficient for routing and dispatch prior to the call being placed. We refer to this as
5082 having a "valid" location for the call²⁸. The i3 architecture defines a function called the LVF
5083 (Location Validation Function) for this purpose. The LVF is only used for civic location
5084 validation. There is no concept of validation of a geodetic location in LoST (5222) [48]. The
5085 primary validation is accomplished as locations are placed in a LIS during provisioning.
5086 Validation MAY also be done by an endpoint if it is manually configured with location, or if
5087 it retrieves location from the LIS (via a location configuration protocol (RFC 6443) [4]).
5088 LVFs MUST support draft-ecrit-lost-planned-changes [178] allowing a LIS to be notified of
5089 planned changes in GIS data and for it to pre-validate a location against this new GIS data
5090 before it becomes live. Periodic re-validation of stored location is also RECOMMENDED
5091 (RFC 6881) [46]²⁹ ³⁰.

27 When coarse location is provided in a wireless call, the location is one agreed to between the wireless operator and the 9-1-1 Authority, and not the location of the caller, and thus the route will be to the designated PSAP.

28 We note that RFC5222, which describes the LoST protocol used by the LVF, validates against the service urn provided in the query, which for an outside (the ESInet) entity would be urn:service:sos. Strictly speaking, this is a call routing validation. NG9-1-1 requires validation for dispatch purposes. The LVF will validate to a level suitable for both routing and dispatch when the urn:service:sos is specified in the query.

29 Short periods (days or a few weeks) allow errors that arise due to changes in underlying data the LVF uses to validate to show up sooner. However, the more often a LIS validates, the more load this places on the LIS and the LVF. A maximum period of 30 days is recommended. LIS operators may wish to consult with the LVF operator to determine an optimal revalidation period.

30 In areas that have little change in data, such as fully built out, stable communities that are already part of a municipality, it may be reasonable to set revalidation periods of 6 months or longer, especially if the lost-planned-changes [178] mechanism is widely used by LISes. In areas that are quickly growing, 20- to 30-day revalidation may be more appropriate even though such revalidation would be the majority of the traffic on the LVF.

5092 As specified in Section 3.4.2, the LVF MUST support the validation of location around
5093 planned changes as defined by draft-ecrit-lost-planned-changes [178].
5094 ECRFs and LVFs are queried using the LoST protocol (see Section 3.4). 9-1-1 Authorities
5095 provide authoritative ECRFs and LVFs both inside and outside ESInets. Other entities, such
5096 as originating networks, can provide their own ECRF/LVFs, or equivalent functions that can
5097 be provisioned from authoritative data provided by the 9-1-1 Authority.
5098 An ECRF or LVF provided by a 9-1-1 Authority and accessible from outside the ESInet
5099 MUST permit querying by an IP client/endpoint, an IP routing proxy, a Legacy Network
5100 Gateway, and any other entity outside the ESInet. An ECRF or LVF accessible inside an
5101 ESInet MUST permit querying from any entity inside the ESInet. ECRF/LVFs provided by
5102 other entities may have their own policies on who may query them. An originating network
5103 MAY deploy an ECRF, or a similar function within its own network, to determine an
5104 appropriate route, equivalent to what would be determined by the authoritative ECRF
5105 provided by the 9-1-1 Authority, to the correct ESInet for the emergency call. The ECRF
5106 MUST be used within the ESInet to route calls to the correct PSAP, and by the PSAP to
5107 route calls to the correct responders.

5108 **4.3.1 Functional Description**

5109 The ECRF/LVF supports a mechanism by which location information (either civic address or
5110 geo-coordinates) and a Service URN serve as input to a mapping function that returns a
5111 URI used to route an emergency call toward the appropriate PSAP for the caller's location
5112 (for an ECRF) and validation information (for an LVF). In an ECRF, depending on the
5113 identity and credentials of the entity requesting the routing information, the response MAY
5114 identify the PSAP or an Emergency Service Routing Proxy (ESRP) that acts on behalf of the
5115 PSAP to provide final routing towards the PSAP. The same database used to route a call to
5116 the correct PSAP MAY also be used to subsequently route the call to the correct responder
5117 (e.g., to support selective transfer capabilities). Depending on the type of routing function
5118 requested, the response may identify a secondary agency. In addition, the ECRF provides
5119 the capability to retrieve other location related URIs, such as Additional Data URIs.

5120 ECRF/LVFs are arranged in trees. The ECRF and LVF trees are separate. The Forest Guide
5121 contains entries for (nominally) state level ECRF/LVFs. State ECRF/LVFs MAY be
5122 authoritative for the entire state, or it MAY refer or recurse to regional or local ECRF/LVFs.
5123 In some areas, regional ECRF/LVFs MAY have copies of all of the region's information or
5124 MAY refer to local ECRF/LVFs. Entities MAY perform LoST server discovery (as described in
5125 RFC 5223 [131]) to find their local ECRF or MAY be provisioned with a LoST server
5126 address. They send queries to that ECRF. A LIS has a provisioned LVF. The local ECRF/LVF
5127 can either answer the query or will refer or recurse in the tree to an ECRF/LVF that will
5128 eventually lead to the correct response. When stressed, or under attack, the Forest Guide

5129 MAY selectively refuse queries from any entity, for example, ECRF/LVFs whose coverage
5130 regions are not stored in the National Forest Guide. For this reason, it is RECOMMENDED
5131 that entities querying using LoST use recursion. Entities MUST NOT bypass their local
5132 ECRF/LVF and query a National Forest Guide directly. A National Forest Guide MAY reject
5133 queries from other entities, for example, if it is overloaded. Not all areas will have state
5134 level ECRF/LVFs and some local or regional ECRFs MAY be listed as stand-alone trees in a
5135 National Forest Guide. By arranging ECRFs and LVFs in this manner, and since the National
5136 Forest Guide will contain listings for all trees globally, a query to a local ECRF/LVF will
5137 result in a correct response for any location.

5138 ECRFs SHOULD return an 'expires' element with at least a minute of cacheable mappings.
5139 Implementors should note the text in Section 3.3.3.1.9 when 'NO-CACHE' is returned.

5140 **4.3.2 Interface Description**

5141 **4.3.2.1 Routing Query Interface**

5142 The ECRF and LVF query interface implements the LoST (RFC 5222) [48] protocol as
5143 described in Section 3.4. When an ECRF receives a LoST query, it determines whether the
5144 query was received from an authenticated entity (e.g., an ESRP) and the type of service
5145 requested (i.e., emergency services). Authentication MUST apply to all entities that initiate
5146 queries to the ECRF within the ESInet. TLS is used by all ECRFs and LVFs within the
5147 ESInet, and credentials issued to the querying entity that are traceable to the PCA MUST
5148 be accepted. Devices and carriers outside the ESInet may not have credentials, TLS is not
5149 required, and the ECRF/LVF should assume a common public identity for such queries.
5150 Based on the service requested, the ECRF determines which URI is returned in the LoST
5151 response, which could be a URI of a PSAP or a downstream ESRP. The same database
5152 used to route a call to the correct PSAP may also be used to subsequently route the call to
5153 the correct responder (e.g., to support selective transfer capabilities).

5154 The ECRF is provisioned with a service boundary layer containing one or more service
5155 boundary polygons (See Appendix C). Each of the polygons contains attributes that specify
5156 the service URN that the polygon applies to and the URL the ECRF should return if the
5157 proffered location is within the polygon. Conceptually, the ECRF geocodes the location if it
5158 is specified in civic form and intersects the location of the service with polygons that have
5159 the same URN as the proffered service URN. The ECRF returns the URL attribute of the
5160 service boundary matching the URN that contains the location.

5161 If the proffered location is not specified as a point (i.e., the location in the query is a
5162 shape) and the shape intersects more than one service boundary with a given service URN,
5163 the ECRF response SHALL be the URI of the service boundary with the greatest area of
5164 overlap (with a tie-breaking policy for the case of equal area of overlap).

5165 If more than one service boundary for the same service URN at a given location exists in
5166 the ECRF, multiple <mapping> elements will be returned. The querier (e.g., a PSAP),
5167 MUST have local policy to determine how to handle the call. In some cases, the ECRF can
5168 use the identity of the querier, or a distinguished Service URN to return the URI of the
5169 correct agency. This condition only occurs for queries to an ECRF from within an ESInet.
5170 External queries will only return one (PSAP) URI. The ECRF is not expected to handle more
5171 than 100 mappings, and MAY truncate its response if more than 100 mappings would be
5172 returned from a query. A new warning for this purpose is described in Section 3.4.10.5.

5173 LoST MAY return a service boundary in the response, see Section 4.3.3.3.

5174 In the deployment strategy envisioned in this document, a query from outside an ESInet
5175 for "urn:service:sos" is mapped to state level ESInets, and thus state ESRPs. The boundary
5176 returned in such cases is a state boundary, or subset of it as described above. Neither
5177 ECRFs nor LVFs are required to return service boundaries.

5178 When a query is performed using a service URN that contains a subservice (e.g.,
5179 "urn:service:sos.police" or "urn:service:sos.ecall.automatic"), if the ECRF does not have a
5180 service boundary with an attribute for that exact service URN, it uses the closest matching
5181 service URN. Thus, a multi-level subservice may match a more general subservice (such
5182 as "urn:service:sos.ecall" for "urn:service:sos.ecall.automatic") or no subservice
5183 ("urn:service:sos" for any subservice). When a query is performed using a service URN
5184 that is "urn:service:test.sos" or a subservice, it matches "urn:service:sos" with the same
5185 subservices. This is how test calls are routed the same as non-test calls. (Because the
5186 Request-URI is preserved, the receiving PSAP knows a test call from a non-test call.)

5187

5188 **4.3.2.2 Validation Interface**

5189 RFC 5222 [48] Section 8.4.2 states that the inclusion of location validation is optional, and
5190 subject to local policy. All LoST server implementations, deployed as an LVF, MUST support
5191 the inclusion of location validation information in the "findServiceResponse" message.
5192 ECRFs may receive a request to validate a location. The ECRF MAY:

- 5193
 - 5194 • Not return any validation response
 - 5194 • Perform the validation and return the validation response
 - 5195 • Recur (or refer) to an LVF that can perform the validation³¹

31 Recursion to an LVF may not be desirable since the LVF is not a real-time element.

5196 Local policy at the ECRF determines what the ECRF does, which MAY take into account
5197 load at the ECRF.

5198 Local LVF policy is also responsible for determining which elements are given priority in
5199 determining which URI and which associated location data element tokens are deemed
5200 valid. Sometimes different data elements are in conflict with each other. As in the example
5201 message, the findServiceResponse message returns the Postal Code (value of 45054) as
5202 <invalid>, showing that the A1 & A3 (State & City) data elements in combination – in this
5203 case – are given preference over a Postal Code that doesn't exist. Whereas the decision to
5204 prefer real data to non-existent data makes good sense, it is possible to have cases in
5205 which all data elements are real, but not consistent with each other. In this case, local
5206 policy will determine which elements are used, and are shown as valid.

5207 As specified in Section 3.4.2, the LVF MUST support the validation of location around
5208 planned changes as defined by draft-ecrit-lost-planned-changes [178].

5209 **4.3.2.3 Mapping Data Provisioning Interface**

5210 The ECRF/LVF's data source is geospatial information, specifically, a set of layers from one
5211 or more source Spatial Interfaces (SIs). An SI layer replication interface, as described in
5212 Section 3.6, is used to maintain copies of the required layers. Appendix B describes the
5213 layers needed by the ECRF/LVF. The ECRF/LVF is provisioned with the URI of the SI and
5214 the information necessary to identify the required layers. It has layers that define the
5215 locations (state/county/municipality/street/address), as well as service boundary polygons.
5216 ECRF/LVFs may be built to coalesce data from more than one SI.

5217 It is essential to the proper operation of the Next Generation 9-1-1 system that
5218 provisioning of the routing data in an ECRF is online, near real-time. An authorized change
5219 in the authoritative GIS to flow through the SI to the ECRF in near real-time is desirable,
5220 and SHOULD result in changes in routing immediately, although caching of mappings may
5221 prevent route changes from being honored as quickly. LVF provisioning is less critical.

5222 **4.3.2.4 Time Interface**

5223 The ECRF/LVF MUST implement an NTP client interface for time of day information. The
5224 ECRF/LVF MAY also provide an interface to a hardware clock. The time-of-day information
5225 is an input to the mapping expiration time as well as the logging interface.

5226 **4.3.2.5 Logging Interface**

5227 The ECRF/LVF MUST be capable of generating LogEvents per Section 4.12. The ECRF/LVF
5228 MUST be capable of logging every incoming routing/validation request along with every
5229 recursive request and all response messages. In addition, the ECRF/LVF MUST log all

5230 provisioning and synchronization messages and actions. Specific LogEvent records for
5231 these are provided in Section 4.12.3.

5232 **4.3.2.6 Element State**

5233 Each ECRF and each LVF MUST implement the server-side of the ElementState event
5234 notification package. The ECRF/LVF MUST promptly report changes in its state to its
5235 subscribed elements. Any change in state that affects its ability to route (ECRF) or validate
5236 (LVF) MUST be reported.

5237 **4.3.2.7 Service State**

5238 The set of ECRF and LVF FEs within an ESInet MUST implement the server side of the
5239 ServiceState event notification package for the ECRF and the LVF service. It is
5240 RECOMMENDED that if there are multiple levels of ESInet within a state, that the state
5241 level NGCS implement ServiceState as a single service, rather than having a ServiceState
5242 for each level of NGCS within the state. In such a service, if any regional or local NGCS'
5243 ECRF or LVF is not operating properly, the state ECRF and/or LVF service would show some
5244 form of non-normal state for the ECRF/LVF ServiceState.

5245 **4.3.3 Data Structures**

5246 **4.3.3.1 Data to Support Routing Based on Civic Location Information**

5247 The ECRF MUST be able to provide routing information based on location information
5248 represented by a civic address. To do so, it is expected that the ECRF will represent the
5249 geographic service boundary in a manner that allows the association of a given address
5250 with the service boundary within which it is located. Theoretically, the ECRF maintains the
5251 civic address data as the SI layers used to provision it, using a geocode followed by point-
5252 in-polygon algorithms to determine the service boundary the civic address is located within.
5253 The ECRF MAY internally compute a tabular civic address form of data representation with
5254 the associated URI resulting from the point-in-polygon operation. This would reduce the
5255 LoST query resolution for a civic address to a table lookup. However, if the provisioning
5256 data changes, the ECRF MUST respond immediately to the change, which may invalidate
5257 (for at least some time) the precalculated tabular data.

5258 ECRFs MUST accept location information conforming to U.S. addressing standards defined/
5259 in CLDXF [77] and its eventual Canadian equivalents.

5260 **4.3.3.2 URNs**

5261 An ECRF/LVF MAY be authoritative for a given (set of) URN(s) in a given service area if
5262 they are provisioned from the authoritative SI for that area. There MAY be replicas of the

5263 ECRF/LVF, but they all supply the same resultant URI. ECRF/LVFs can recur or iteratively
5264 refer to other ECRF/LVFs or the National Forest Guide to obtain answers based on queries
5265 for service URNs or locations outside their area. Two queries from the same entity that
5266 uses the same service URN and location that are sent to different ECRFs SHOULD return
5267 the same response. Unless the ECRF/LVF is provisioned to return different responses to
5268 different credentials of the querier, all queries with the same URN and location SHALL
5269 return the same response.

5270 **4.3.3.3 Service Boundaries**

5271 The service boundary in a <mapping> MAY be returned by value or by reference, or not at
5272 all, at the discretion of the server. If the server returns a service boundary reference, the
5273 client may then obtain the actual service boundary with a <getServiceBoundary> request.
5274 A service boundary represented by a given reference can never change, so a client only
5275 needs to retrieve the boundary value a single time. Future mappings returned by the server
5276 and having the same service boundary MAY reuse the reference, eliminating the need to
5277 transmit the boundary value again.

5278 Devices handling service boundaries may be limited in processing power and battery
5279 capacity, and thus sending complex polygons SHOULD be avoided. Devices may have to
5280 handle a polygon with several points when the device is very close to an edge where the
5281 mapping will be different. When a device is not close to an edge, a simplified
5282 representation of a geodetic service boundary (such as a simple shape that does not
5283 extend past the actual service area) SHOULD be returned.

5284 Because a service boundary is not needed to initiate an emergency call an ECRF MAY be
5285 configured to return geodetic service boundaries by reference. Devices querying an ECRF in
5286 order to immediately initiate an emergency call SHOULD NOT attempt to obtain the service
5287 boundary by value.

5288 As long as a device stays within the boundary returned, and is within the expiration time of
5289 the mapping, it need not re-query the ECRF.

5290 Location represented by geodetic coordinates provides data that corresponds to a specific
5291 geographic location shape. A service boundary is represented by a polygon set. More than
5292 one polygon MAY occur in the set, for example, when the service area has holes or non-
5293 contiguous regions.

5294 For each service URN supported by an ECRF/LVF, one or more layers will provide polygon
5295 sets associated with URIs³². Two types of attribute are associated with these polygons:
5296 • URN: The service URN this boundary is associated with
5297 • URI: A URI returned if the location is within the boundary
5298 The ECRF/LVF computes a response to a LoST query by finding the polygon whose service
5299 URN attribute matches that provided in the LoST query and whose service boundary
5300 contains the location provided in the LoST query, and returns the URI attribute of that
5301 polygon set. If the proffered location is a shape, that shape MAY overlap more than one
5302 service boundary. The ECRF response SHALL be the service boundary with the greatest
5303 area of overlap. The ECRF will return multiple <mapping> elements in a response if the
5304 query has multiple matches (e.g., a query within an ESInet for
5305 "emergency:service:responder:police" with a location within the jurisdiction of campus,
5306 city, county, and state police agencies) A querier could use the service boundaries (e.g., to
5307 determine which has the smallest service area and thus might be the most specific to the
5308 location).
5309 Note that the provisioning interface to the ECRF/LVF is the SI layer replication protocol,
5310 and thus always delivers a geodetic service boundary definition to it. The ECRF/LVF MAY
5311 compute a civic representation of the boundaries internally. A trivial example is a service
5312 boundary polygon exactly matching a state, county, or municipal boundary.

5313 **4.3.3.4 Service to access Additional Data for a location**

5314 In the case of the Additional Data service, the ECRF does not use the service boundary
5315 polygons. Additional Data is associated with a site/structure. This will be addressed in a
5316 future version of this document. When the ECRF receives a findService request for the
5317 Additional Data service URN, and the proffered location information is a civic address, the
5318 ECRF returns the content of the Additional Data URI element associated with the
5319 site/structure, if available. If the location information proffered is a point, the ECRF finds
5320 the enclosing site/structure polygon, if there is one, or the nearest site/structure feature,
5321 and returns the associated Additional Data URI, if available³³. In the case in which a
5322 location is a shape, rather than a point, and there are more than one site/structures

32 Multiple URIs, each with a different scheme, may be returned from an ECRF query

33 The Additional Data block is intended to reference the civic address to which it refers, so a geodetic querier can determine to which address the response refers. This will be addressed in a future version of this document.

5323 partially or completely within that shape, the ECRF returns all of the Additional Data URIs
5324 associated with those sites/structures³⁴.

5325 When dereferenced by a client using PCA-traceable credentials, URIs returned for the
5326 Additional Data service MUST resolve to Additional Data blocks registered in the IANA
5327 Emergency Call Additional Data registry [179].

5328 **4.3.3.5 Routing Data – URI Format**

5329 For an end-to-end IP network in which the caller is an IP endpoint and the PSAP is
5330 accessed over an IP network, routing information will be in the form of a URI. The source
5331 of the query and/or the service URN determines which URI is returned. URI format is
5332 described in RFC 3986 [126]. URIs can be of variable length. It is suggested that the
5333 length allowed for a URI be as compact as possible, not exceeding 1.3 KB, which is the
5334 maximum size of a packet on the ESInet, less any header field information.

5335 **4.3.3.6 Validation Data**

5336 The LVF uses the same data provided to the ECRF as described in Section 4.3.3.1 above.

5337 **4.3.4 Coalescing Data and Gap/Overlap Processing**

5338 ECRFs and LVFs MAY coalesce data from several 9-1-1 Authorities. The resulting database
5339 appears to be a seamless route database for the union of the service areas of each 9-1-1
5340 authority. Such ECRF/LVFs are provisioned to accept data from multiple GIS' via separate
5341 SIs.

5342 In some local GIS', for convenience, the 9-1-1 Authority may provide data that extends
5343 beyond the service boundary of the PSAPs within their jurisdiction. When provisioning data
5344 for an ECRF and LVF through the SI, a 9-1-1 Authority (or 9-1-1 Authority designee) MUST
5345 only include GIS data for their geographic area of responsibility and MUST ensure the data
5346 includes coverage for the entire extent of that area. When the data are coalesced,
5347 boundaries may have gaps and overlaps. The relevant 9-1-1 Authorities SHOULD endeavor
5348 to address such issues early, but despite best efforts, the ECRF/LVF may encounter a gap
5349 or overlap. The ECRF/LVF MUST have a provisionable threshold parameter that indicates
5350 the maximum gap/overlap that is ignored by it. This threshold is expressed in square

³⁴ The definition of “nearest”, when the ECRF is determining the Additional Data URIs from a point, is implementation-dependent. The querier can control this by sending a circle shape rather than a point, in which case the ECRF will intersect the circle with the site/structure entries, and return all of them that are completely or partially in the circle. If the number of URIs to be returned is large, the number of mappings in the response may be limited in an implementation-dependent way

5351 meters. Gaps or overlaps that are smaller than this parameter MUST be handled by the
5352 ECRF/LVF using an algorithm of its choice. For example, it may split the gap/overlap
5353 roughly in half and consider the halves as belonging to one of the constituent sources.

5354 The ECRF/LVF MUST report gaps and overlaps larger than the provisioned threshold. To do
5355 so, it makes use of the GapOverlap event. All 9-1-1 Authorities which provide source GIS
5356 data to an ECRF/LVF MUST subscribe to its GapOverlap event. The event notifies all
5357 impacted agencies when it receives data that show a gap or overlap larger than the
5358 threshold. The notification includes the layer(s) in which the gap/overlap occurs, whether it
5359 is a gap or an overlap, and a polygon that represents the gap or overlap area. The optional
5360 effective and expires times in the data may indicate a future gap/overlap as opposed to
5361 one that exists when the event is generated. The report includes a Timestamp of when the
5362 gap/overlap will occur.

5363 The response of the agencies MUST be to provide updates to the data that address the
5364 gap/overlap. The ECRF/LVF will repeat the notification at least daily until it is resolved (by
5365 changing the SI data so the gap/overlap is eliminated or at least smaller than the threshold
5366 parameter). During the period when the gap/overlap exists, notifications have been issued,
5367 and queries arrive (which could be at call time) with a location in the gap/overlap, the
5368 ECRF/LVF MUST resolve the query using an algorithm of its choice. For example, it may
5369 split the gap/overlap roughly in half and consider the halves as belonging to one of the
5370 constituent sources.

5371 A service may have areas within the service area of the ECRF for which there is no
5372 responder. For example, the mountain rescue service is not available in flat terrain. Also,
5373 there are still some areas where 9-1-1 service is not available. In such cases, a service
5374 boundary MUST exist in the ECRF with the Service URI field set to
5375 urn:emergency:servicenotimplemented. The ECRF MUST return the
5376 <serviceNotImplemented> error if asked to provide a route for a location within that areas.

5377 The GapOverlap event is defined as follows:

5378 **Event Package Name:** emergency-GapOverlap

5379 **Event Package Parameters:** none

5380 **SUBSCRIBE Bodies:** Standard RFC 4661 [92] + extensions filter specification may be
5381 present

5382 **Subscription Duration:** Default 24 hour. 1 hour to 96 hours is reasonable.

5383 **NOTIFY Bodies:** MIME type Application/EmergencyCallData.GapOverlap+json

Name	Condition	Description
agency	MANDATORY	URI of Agency with gap/overlap. Will be repeated at least twice
layer	MANDATORY	Enumeration of layer in which gap/overlap exists. May occur multiple times
gap	MANDATORY	Boolean: True if gap, False if overlap
dateTime	OPTIONAL	Timestamp when gap/overlap will occur. If not provided, gap/overlap is present now
area	MANDATORY	GML Polygon area of gap/overlap

5384 **Notifier Processing of SUBSCRIBE Requests:** The Notifier consults the policy
 5385 (NotifyPermissions) for GapOverlap to determine if the requester is permitted to subscribe;
 5386 agencies allowed to provide authoritative data to the ECRF are permitted by default. If the
 5387 requester is not permitted, the Notifier returns 603 Decline. Otherwise, the Notifier returns
 5388 200 OK.

5389 **Notifier Generation of NOTIFY Requests:** When the provisioning GIS data creates a
 5390 gap or overlap whose area is above the GapOverlapThreshold parameter, the Notifier
 5391 generates a Notify to all subscribers. The Notifier repeats the Notification at least once per
 5392 24 hours as long as the gap/overlap remains.

5393 **Subscriber Processing of NOTIFY Requests:** No specific action required.

5394 **Handling of Forked Requests:** Forking between elements MUST NOT be used.

5395 **Rate of Notification:** Notifies normally only occur when the provisioning data changes.
 5396 Throttle MAY be used to limit Notifications.

5397 **State Agents:** No special handling is required.

5398 4.3.5 Replicas

5399 An ECRF/LVF is essentially a replica of a subset of the layers of one or more source GIS'
 5400 The ECRF/LVF in turn, may provide a feed to other ECRF/LVFs who wish to maintain a copy
 5401 of its data. As the ECRF/LVF is not the data owner, the source GIS MUST have a policy
 5402 (GISReplicas) that permits the ECRF/LVF to do so, and the policy MAY restrict to which
 5403 entities it may provide replication data. The ECRF/LVF also has a policy (ECRF-LVFreplica)
 5404 that defines to whom it will provide data. If the ECRF/LVF provides a replica service, the
 5405 interface is the layer replication service as described in Section 3.6. In this case, the

5406 ECRF/LVF is the server-side, as opposed to the client interface it must provide towards the
5407 SI(s) from which it receives data.

5408 **4.3.6 Provisioning**

5409 The ECRF/LVF is provisioned with a set of layers from one or more SIs, the domains from
5410 which it may accept queries, if its use is restricted is specified with a policy
5411 (AcceptableLoSTQuerySources).

5412 To maximize the probability of getting help for any kind of emergency to foreign visitors
5413 who may have separate dial strings for different types of emergencies, the ECRF/LVF
5414 SHOULD be provisioned with every sos URN in the IANA registry³⁵. All sos service URNs
5415 that represent services provided by the PSAP return the dial string '911' and the PSAP URI.
5416 Other services available in the area would typically return a tel URI with the proper PSTN
5417 telephone number, other dial strings, or other provisioned values. In such cases, the
5418 telephone number for the service would also be returned in the service number parameter
5419 of the response. Any ECRF that is authoritative for a top level URN MUST also be
5420 authoritative for all lower level URNs for the same coverage regions.

5421 **4.3.7 Roles and Responsibilities**

5422 The ECRF/LVF plays a critical role in the location-based routing of emergency calls.
5423 Therefore, it is crucial that the data in the ECRF/LVF be accurate and authorized. 9-1-1
5424 Authorities are responsible for providing the authoritative data for their jurisdiction to the
5425 ECRF/LVF. The data may be aggregated at a regional or state level, and the ECRF/LVF
5426 system provided at that level may be the responsibility of the associated state or regional
5427 emergency communications agency. In addition, access or originating network operators
5428 may maintain replicas of the ECRF/LVF. Thus, the operation and maintenance of individual
5429 ECRF/LVFs may be the responsibility of the provider of the network in which they physically
5430 reside, but it is the 9-1-1 Authority that is responsible for maintaining the integrity of the
5431 source data housed within those systems. The 9-1-1 Authority will also provide input to the
5432 definition of the policy which dictates the granularity of the routing data returned by the
5433 ECRF (i.e., ESRP URIs vs. PSAP URIs), based on the identity of the query originator and/or
5434 service URN.

³⁵ While there is only one dial string, 911, for emergencies in North America, all services in the sos tree should return a valid route when queried. For services the PSAP is responsible for, such as sos.police, the same URI used for urn:service:sos should be returned.

5435 **4.3.8 Operational Considerations**

5436 The NG9-1-1 architecture allows for a hierarchy of ESInets, with replicas of ECRF/LVFs at
5437 different levels of the hierarchy as well as in access/originating networks. It is expected
5438 that ECRFs that are provided as local copies to network operators will only have the layers
5439 necessary to route to the correct originating ESRP, whereas ECRFs that are inside the
5440 ESInet(s) will have all available layers and use authorization to control who has access to
5441 what information. Since it is not possible that all entities that need to access an ECRF will
5442 have one in their local domain, an ECRF for each 9-1-1 Authority MUST be accessible from
5443 the Internet³⁶. Consideration needs to be given to the operational impacts of maintaining
5444 different levels of data in the various copies of the ECRF. In addition, tradeoffs between
5445 the aggregations of data in higher level ECRFs versus the use of Forest Guides to refer
5446 requests between ECRFs that possess different levels of ECRF data must be considered.
5447 LVFs always provide the same data to all queriers and thus are provisioned identically.
5448 Provisioning of data within appropriate ECRF/LVF systems for use in overload and backup
5449 routing scenarios MUST also be supported.

5450 For example, a local ECRF may have an SI to another local ECRF, a regional ECRF may
5451 have an SI to all the local ECRFs in its area, a state ECRF may have an SI to all of the
5452 regional ECRFs, and an access network provider may have an ECRF that has an SI from the
5453 state ECRF. A change in the GIS system by the local 9-1-1 Authority is propagated via its
5454 local SI to the local ECRF, and that local ECRF propagates it to the regional ECRF, which
5455 propagates it to the state ECRF that propagates it to the access network ECRF.

5456 The placement of ECRF/LVF elements in the IP-enabled network varies with
5457 implementation. Since both end devices as well as LIS elements need to validate location,
5458 it is recommended that LVF elements are within the local domain or adjacent to it. Given
5459 that NG9-1-1 elements will also need to validate civic locations that either come with an
5460 emergency call, or are conveyed over the voice path, it is also a requirement that LVF
5461 elements MUST be reachable from within any ESInet. Since it is not possible that all
5462 entities that need to access an LVF will have one in their local domain, an LVF MUST be
5463 accessible from the Internet³⁷. Similar considerations apply for an ECRF, but the entities
5464 that route are often different from the entities that validate, so differences in deployments
5465 may occur. All devices and services that route MUST have access to an ECRF. External
5466 ECRFs MUST be accessible to all devices and services, including those on the Internet.

36 The Internet-accessible ECRF may be a state or regional ECRF containing the local ECRF data of all 9-1-1 Authorities within the state or region.

37 The Internet-accessible ECRF/LVF may be a state or regional ECRF/LVF containing the local data of all PSAPs within the state or region.

5467 Ideally, originating networks will have replicas of the authoritative (usually state) ECRFs
5468 maintained inside their networks for use by their services and devices. Within the ESInet,
5469 ECRFs MUST be accessible from all ESRPs and all agencies that may receive or transfer
5470 calls or EIDOs related to calls.

5471 LVF elements are based on the LoST server architecture and use the LoST protocol (RFC
5472 5222) [48]. The LVF is a logical function that MAY share the physical platform of an ECRF,
5473 and MUST share the same data for a given jurisdiction as the ECRF. The justification for
5474 shared data is rooted in the idea of consistency – expecting a similar result from the same,
5475 or matching data. The LVF is used during a provisioning process (loading data into a LIS
5476 for example), while an ECRF is in the near real-time call flow. Separating the functions may
5477 make more sense. The Service Level Agreements for the two functions may dictate
5478 whether they can be combined or not.

5479 An ECRF/LVF, wherever deployed, whether within an Origination or Access network, MUST
5480 be able to reach out to other ECRF/LVFs in case of missing data, or in the case in which
5481 the requested location is outside its local jurisdiction. If the ECRF/LVF doesn't know the
5482 answer, based on configuration, it will either recurse (refer) a request for validation to one
5483 or more other ECRF/LVFs, or it will iterate the request to some other ECRF/LVF, providing
5484 the other ECRF/LVF's URL in the original ECRF/LVF response.

5485 Redundant ECRF/LVF elements are RECOMMENDED, similar to DNS server deployments
5486 (the ECRF/LVF shares some of the same replication characteristics with DNS), by example,
5487 in order to maintain a high level of availability and transaction performance.

5488 Given the close association between the LVF and ECRF elements, ECRF/LVFs SHOULD be
5489 deployed hierarchically and with "n" number of replicas at each level of the hierarchy. The
5490 same redundancy/replica considerations apply to access/calling/originating networks that
5491 use an ECRF/LVF. This level of redundancy aids in maintaining high levels of availability
5492 during unexpected system outages, scheduled maintenance windows, data backup
5493 intervals, etc.

5494 Localized ECRF/LVF elements MAY have limited data, sufficient to provide routing/location
5495 validation within its defined boundaries, but MUST rely on other ECRF/LVFs for
5496 routing/validation of a location outside its local area.

5497 ECRFs and LVFs within the ESInet will likely have considerably more data than those in
5498 access or originating networks, providing aggregation for many local access areas as well
5499 as PSAP jurisdictions. Even the level of data that an ECRF/LVF might contain will vary
5500 depending on the hierarchy of the ESInet that it supports. An ESInet serving a local PSAP
5501 MAY have within its ECRF/LVF only base civic location data for its described jurisdiction,
5502 whereas a State-level or County-level ECRF/LVF MAY aggregate all of the local PSAP data
5503 within that level of hierarchy.

5504 Tactical Routing considerations in NG9-1-1 may require an Emergency Call Routing Change
5505 made in the ECRF. See discussion of ECRF changes in Section 4.2.6.3.

5506 **4.3.9 Internal and External ECRF/LVFs**

5507 ECRF/LVFs exist inside and outside the ESInet. Originating networks that route calls to the
5508 correct ESInet and validate locations MAY use external ECRFs. Originating networks MAY
5509 also use equivalent mechanisms that would result in the same route that the external ECRF
5510 would provide for the location of the caller for a querier without credentials known by the
5511 ECRF. Internal ECRF/LVFs are used by elements inside the ESInet to route calls to the
5512 appropriate downstream entity and validate civic locations. While the interfaces and
5513 functional descriptions are nearly identical, the provisioning data may not be the same for
5514 internal and external ECRFs. An external ECRF need only have the external (which ESInet)
5515 route for "urn:service:sos.*" The internal ECRF also needs routes for ESRP use
5516 ("urn:emergency:service:sos.*") and other internal services such as
5517 "urn:emergency:service:serviceagencylocator". If the data in the internal and external
5518 ECRFs are different, this would only affect service boundary data. All LVFs are provisioned
5519 with the same data, whether inside or outside the ESInet.

5520 **4.3.10 Relationship Between ECRF and LVF**

5521 The ECRF and LVF functions have the same interfaces and contain the same data. They
5522 MAY be combined into a single implementation. However, it should be noted that the ECRF
5523 is a real-time element in the path of an emergency call. The LVF is used primarily while
5524 provisioning a LIS. If the ECRF and LVF are combined, the implementation MUST assure
5525 ECRF queries are processed promptly, and LVF traffic does not interfere with proper
5526 operation of the ECRF function.

5527 LVF interaction at emergency call time MAY be performed by a PSAP to validate locations
5528 not received through incoming call signaling.

5529 **4.4 MSAG Conversion Service (MCS)**

5530 The MSAG Conversion Service provides a convenient way to provide data to, or get data
5531 from, a non-upgraded system that still uses MSAG data. This web service provides
5532 conversion between PIDF-LO and MSAG data. Two functions are defined:

- 5533 • PIDFOtoMSAG: which takes a PIDF-LO, as described in RFC 4119 [6] and updated
5534 by RFC 5139 [53] and RFC 5491 [52], and returns an MSAG address as an XML
5535 object conforming to NENA 02-010 Version 4, XML Format for Data Exchange;
- 5536 • MSAGtoPIDFO: which takes an MSAG address as an XML object conforming to
5537 NENA 02-010 Version 4, XML Format for Data Exchange, and returns a PIDF-LO, as
5538 described in RFC 4119 and updated by RFC 5139 and RFC 5491.

5539 MSAG Conversion Service is provisioned using the same mechanism as is used to provision
5540 the ECRF and LVF: layer replication from the master SI. The layers include all of the layers
5541 to create a PIDF-LO as described above, plus a table containing the MSAG field content
5542 used prior to NG9-1-1 migration. Field use in MSAGs varies wildly. Nearly every MSAG has
5543 some variations from the original NENA data standards as to how fields are used. Because
5544 of this variation, the MCS needs a complete set of fields [as defined by
5545 NENA-STA-015.10-2018 (originally NENA 02-010v9)] for each MSAG record and a link
5546 between the MSAG record and street/address point records in the ECRF/LVF.

5547 Some MSAGs have content in address numbers, and address number suffixes that would
5548 not match that in the ECRF/LVF site/structure layer. Address numbers normally use the
5549 PIDF-LO fields for the equivalent MSAG fields. When the content differs, an exception
5550 record is provided in an MSAG Street Number Exception layer, and a link to that record is
5551 included in site/structure.

5552 The PIDFLOtoMSAG function locates the point in the database represented by the input
5553 PIDF-LO and retrieves the MSAG data associated with that point. It constructs an MSAG
5554 address using any MSAG data available, and the PIDF-LO layers in which MSAG and
5555 PIDF-LO are the same. The functions return NENA Version 4 XML data exchange, but the
5556 client can convert to any other MSAG version from the XML representation.

5557 The OpenAPI definition of this web service may be found in Appendix E.4.

5558 **4.4.1 PIDF-LO to MSAG Conversion**

5559 Converts PIDF-LO to MSAG data.

5560 HTTP method: POST

5561 Resource name .../PidfloToMsag

5562 The body of the request MUST contain a PIDF-LO as a string.

5563 A successful query returns an AQS MSAG address as an XML object in a string

5564 Status Codes

5565 200 OK

5566 307 Temporary Redirect

5567 454 Unspecified Error

5568 468 No Address Found

5569 469 Unknown MCS/GCS

5570 **4.4.2 MSAG to PIDF-LO Conversion**

5571 The MSAGtoPIDFLO function works in the same manner, locating the point in the database
5572 to which the MSAG address refers, and composing a PIDF-LO from the PIDF-LO layers.

5573 Converts PIDF-LO to MSAG data.

5574 HTTP method: POST

5575 Resource name .../MsagToPidfLo

5576 The body of the request MUST contain a MSAG address XML component as a string.

5577 A successful query returns a pidfloAddress as a string containing the PIDF-LO

5578 Status Codes

5579 200 OK

5580 307 Temporary Redirect

5581 454 Unspecified Error

5582 468 No Address Found

5583 469 Unknown MCS/GCS

5584 The service logs the invocation of the function, as well as the input and output objects.

5585 Each FE in the MCS MUST implement the server-side of the ElementState event notification
5586 package. The MCS MUST promptly report changes in its state to its subscribed elements.

5587 The set of MCS FEs within an ESInet MUST implement the server-side of the ServiceState
5588 event notification package for the MCS. It is RECOMMENDED that if there are multiple
5589 levels of ESInet within a state, that the state level MCS implement ServiceState as a single
5590 service, rather than having a ServiceState for each level of NGCS within the state. In such
5591 a service, if any regional or local NGCS' MCS is not operating properly, the state MCS would
5592 show some form of non-normal state for the MCS ServiceState.

5593 We observe that the Centerline layer, together with the StreetSegment table and the MCS,
5594 can be used to create or re-create an MSAG. For each entry in the centerline layer,
5595 construct an MCS PIDFLOToMSAG record with any of the address numbers in the
5596 corresponding StreetSegment record. With the remaining information in the centerline and
5597 corresponding StreetSegment records, an MSAG record can be created and the set of those
5598 records would be a complete MSAG for every address in the database. Some MSAGs
5599 contain unusual records for extenuating circumstances that don't have corresponding
5600 records in the centerline layer. These would need to be maintained manually.

5601 **4.5 Geocode Service (GCS)**

5602 The Geocode Service provides geocoding and reverse-geocoding. This web service provides
5603 two functions:

- 5604 • Geocode: which takes a PIDF-LO, as described in RFC 4119 [6], and updated by RFC
5605 5139 [53] and RFC 5491 [52], which contains a civic address, and returns a PIDF-LO
5606 containing a geodetic representation for the same location.
- 5607 • ReverseGeocode: which takes a PIDF-LO as described in RFC 4119 and updated by
5608 RFC 5139 and RFC 5491, which contains a geodetic representation, and returns a
5609 PIDF-LO that contains a civic address for the same location.

5610 The Geocode Service is provisioned using the same mechanism as is used to provision the
5611 ECRF and LVF: layer replication from the master SI. The layers include all of the layers to
5612 create a PIDF-LO as described above.

5613 Any conversion, and specifically geocoding and reverse geocoding, can introduce errors.
5614 Unless the underlying SI provides very accurate polygons to represent all civic locations
5615 precisely, the conversion is complicated by the inherent uncertainty of the measurements
5616 and the “nearest” point algorithm employed. Users of these transformation services should
5617 be aware of the limitations of the geocoding and reverse geocoding mechanisms. Reverse
5618 geocoding is typically less accurate than geocoding, although some error and unquantified
5619 uncertainty is inherent in both.

5620 The Geocode function locates a civic address, represented by the input PIDF-LO, by finding
5621 a match in its site/structure address points or road centerlines, and uses the matching
5622 feature to obtain a geodetic location that represents the civic address. It constructs a
5623 PIDF-LO with the geodetic location. If the PIDF-LO in the request contains more than one
5624 location, the return must contain only one result, which is the conversion of the first
5625 location in the PIDF-LO.

5626 The OpenAPI definition of this web service may be found in Appendix E.5.

5627 **4.5.1 GeocodeRequest**

5628 Converts civic address to geodetic representation of the location in PIDF-LO format.

5629 HTTP method: POST

5630 Resource name .../Geocode

5631 The body of the request MUST contain a PIDF-LO as a string.

5632 A successful query returns:

[MM/DD/YYYY]

Page 195 of 675



5633 GeodeticData

Name	Condition	Description
pidfLoGeo	Conditional, MUST be present if conversion succeeds	PIDF-LO resulting from conversion
gcsReferralUri	Conditional, MUST be present if conversion does not succeed	URI of another GCS

5634 Status Codes

- 5635 200 Data successfully converted
5636 307 Temporary Redirect
5637 454 Unspecified Error
5638 468 No Address Found
5639 469 Unknown MCS/GCS

4.5.2 ReverseGeocodeRequest

5641 The ReverseGeocode function works in the same manner. It converts geodetic representation of the location to civic address in PIDF-LO format.

5643 HTTP method: POST

5644 Resource name .../ReverseGeocode

5645 The body of the request MUST contain a PIDF-LO as a string.

5646 A successful query returns:

5647 CivicAddress

Name	Condition	Description
PIDFLOAddress	Conditional, MUST be present if conversion succeeds	PIDF-LO resulting from conversion
gcsReferralUri	Conditional, MUST be present if conversion does not succeed	URI of another GCS

5648 Status Codes

[MM/DD/YYYY]

Page 196 of 675



5649 200 Data successfully converted
5650 307 Temporary Redirect
5651 468 No Address Found
5652 469 Unknown MCS/GCS

5653 The service logs the invocation of the function, as well as the input and output objects.
5654 Each FE in the GCS must implement the server-side of the ElementState event notification
5655 package. The GCS must promptly report changes in its state to its subscribed elements.

5656 The set of GCS FEs within an ESInet MUST implement the server-side of the ServiceState
5657 event notification package for the GCS. It is RECOMMENDED that if there are multiple
5658 levels of ESInet within a state, that the state level GCS implement ServiceState as a single
5659 service, rather than having a ServiceState for each level of NGCS within the state. In such
5660 a service, if any regional or local NGCS' GCS is not operating properly, the state GCS would
5661 show some form of non-normal state for the GCS ServiceState.

5662 **4.6 PSAP**

5663 A PSAP is a service, typically composed of more than one functional element. The
5664 functional elements that make up a PSAP are defined in NENA STA-023.1-202Y, *NG9-1-1*
5665 *PSAP Specifications for the NENA i3 Solution* (forthcoming). A PSAP provides the following
5666 interfaces towards the ESInet.

5667 **4.6.1 SIP Call interface**

5668 The PSAP MUST deploy the SIP call interface as defined in Section 3.1 including the
5669 multimedia capability, and the non-interactive call (emergency event) capability. PSAPs
5670 MUST recognize calls to their administrative numbers received from the ESInet (and
5671 distinguishable from normal 9-1-1 calls by the presence of the number in a sip or tel URI in
5672 the To header field and the absence of the sos service URN in a Request-URI line, and
5673 identified in the target PSAP's SALR, if available). The SIP call interface MAY also be used
5674 to place non 9-1-1 calls (including callbacks) from the PSAP. Such outbound calls will be
5675 routed to the OCIF of the serving ESInet/NGCS for processing and routing. Callback and
5676 other non-emergency outbound call INVITE messages MUST comply with the SIP call
5677 interface as defined in Section 3.1, and constructed using the guidance provided in section
5678 4.20 (OCIF), with the following clarifications. The To header field value of the callback
5679 INVITE message MUST be set to a value that will allow reaching the home network of the
5680 target. If the To header field value is a tel URI, the OCIF will route the callback toward the
5681 PSTN, which means that only the voice portion will go through. If the To header field value
5682 is a sip URI, the domain SHALL be the one of the home network of the target. The
5683 Request-URI line SHOULD contain the same URI value as in the To header field.

5684 The PSAP can use a number of techniques to determine the best route for the call to the
5685 home network of the target. Specifically for emergency callbacks, the PSAP MAY rely on the
5686 domain available in the P-A-I (preferred) or From header field of the original emergency
5687 call from a fixed wireline-type network. For mobile networks supporting roaming and other
5688 IMS-based networks, the PSAP MAY rely on the domain found in the "orig-roi" parameter of
5689 a P-Charging-Vector (RFC 7315 [209]) header field or alternatively, in a P-Charge-Info
5690 header field (RFC 8496 [208]) of the original emergency call, if available. The domain of
5691 the home network is to be populated in the Request-URI line and the To header field of the
5692 callback INVITE message.

5693 Outbound calls MAY be placed via the ESInet using the ESRP as an outgoing proxy server
5694 (see Section 4.2.2.1). In most circumstances the ESRP will forward calls to the OCIF, which
5695 uses a Network-to-Network Interface to an interconnected network as described in section
5696 4.20.

5697 **Note:** Handling of media other than voice-only callbacks is incompletely specified and will
5698 be addressed in a future version of this document.

5699 **4.6.2 Media**

5700 All i3 PSAPs MUST support all media, voice, video, and text. If a PSAP receives an Offer
5701 containing both MSRP and RTT, it SHOULD send an Answer with only one of them. If the
5702 PSAP receives an Answer containing both RTT and MSRP, it MUST be prepared to deal with
5703 both simultaneously. When placing callbacks, PSAPs SHOULD offer all supported media
5704 choices, subject to operational considerations.

5705 Emergency calls marked with a humintlang tag (RFC 8373) [173] SHOULD be processed
5706 with appropriate language-specific resources available to the PSAP. SDP offers and answers
5707 generated by the PSAP MUST include appropriate language tags. Answers to offers that
5708 included language tags MUST include language tags. The PSAP is not obligated to offer
5709 languages it supports with outside entities such as a language translation service.

5710 Note that a future edition of this document will include a standard method to invoke a
5711 language translation service using the humintlang (RFC 8373) [173] mechanism.

5712 **4.6.3 LoST interface**

5713 The PSAP MUST implement a LoST client interface as defined in Section 3.4. The PSAP
5714 uses the ECRF and LVF to handle calls that must be dispatched and calls that must be
5715 transferred based on the actual location of the incident. The LoST interface is used with the
5716 "urn:emergency:service:responder" URNs to achieve "selective transfer" operations. The
5717 PSAP would query the ECRF using LoST with the appropriate responder URN and the
5718 location of the incident. It would receive the URI to which the call should be directed.

5719 The PSAP MAY also use the LoST interface to find an AgencyLocator URI by location by
5720 querying the ECRF with a service URN of a subservice of
5721 "urn:emergency:service:serviceagencylocator". The AgencyLocator record can be retrieved
5722 from the URI by dereferencing it with HTTPS GET. [4.15.1] The Agency Locator record
5723 document is returned. From the AgencyLocator record, other interface points, such as a
5724 URI to which to send an EIDO, may be found.

5725 **4.6.4 LIS Interfaces**

5726 The PSAP MUST implement both SIP Presence Event Package and HELD dereferencing
5727 interfaces to any LIS function as described in Section 4.10. When the PSAP receives a
5728 location reference (in a Geolocation header field on the upstream SIP interface³⁸) it uses
5729 the LIS dereferencing interface to obtain a location value. The PSAP MUST be able to be
5730 provisioned with credentials for every LIS in its service area³⁹. The PSAP MUST use TCP
5731 with TLS for the LIS dereferencing interface, with fallback to TCP (without TLS) on failure
5732 to establish a TLS connection when TLS is used. The PSAP SHOULD maintain persistent
5733 TCP (and TLS when used) connections to LISes with which it has frequent transactions. A
5734 suggested value for "frequent" is more than one transaction per day.

5735 For HELD location URIs, specifying responseTime = emergencyDispatch should result in a
5736 location meeting current regulatory accuracy requirements. If the PSAP wishes an
5737 immediate location, it can specify a short responseTime (perhaps 250 ms), and get the
5738 best location quality available in that amount of time. Location updates for location URIs
5739 using HELD may be obtained by repeating the dereference request.

5740 PSAPs receiving SIP location URIs SHOULD subscribe to the Presence event per RFC 3856
5741 [25] in order to receive the location value. In response to a subscribe request, the PSAP
5742 receives an immediate location report, which may reflect the best available location at the
5743 time of the subscription. A subsequent location update is sent when more accurate location
5744 information is available. By setting the expiration time of the subscription, the PSAP is able
5745 to control which updates it receives. PSAPs that wish to track the motion of a caller could
5746 use the location filter and event rate control mechanisms (RFC 6447) [72] and rate-control
5747 (RFC 6446) [80] to control updates.

38 If the PSAP receives a call via a transfer from another agency, the location of the caller will be found in the EIDO included in the transfer and not in a Geolocation header.

39 This document specifies that the LIS accept credentials issued to the PSAP traceable to the PCA. Notwithstanding that requirement, ESInet elements needing location, including PSAPs, must be able to be provisioned with credentials acceptable to LISes that do not accept the PCA credential.

5748 Note that because the PSAP will not have an identity of an arbitrary device with which it
5749 could query a LIS to get the device's location, the "manual ALI query" function, also known
5750 as "Reverse-ALI" in E9-1-1, has no equivalence in NG9-1-1.

5751 **4.6.5 Bridge Interface**

5752 A PSAP MAY deploy a bridge (as described in Section 4.7) inside the PSAP, in which case it
5753 MUST provide the bridge controller interfaces. PSAPs MUST be able to accept calls from,
5754 and utilize the features of, outside bridges.

5755 **4.6.6 ElementState**

5756 The PSAP MUST deploy an ElementState Notifier. Any element inside a PSAP that provides
5757 a call queue MUST deploy an ElementState notifier as described in Section 2.4.1.

5758 **4.6.7 ServiceState**

5759 The PSAP MUST deploy a ServiceState notifier as described in Section 2.4.2.

5760 **4.6.8 AbandonedCall Event**

5761 The PSAP MUST implement the subscriber side of the AbandonedCall Event as described in
5762 Section 4.2.2.9.

5763 **4.6.9 DequeueRegistration**

5764 The PSAP MUST implement a DequeueRegistration client, as described in Section 4.2.1.4,
5765 for every queue on which it expects to receive calls. When the PSAP registers, it specifies a
5766 URI to direct calls to it. That URI will appear in the top Route header field when the PSAP
5767 receives an emergency call or the Request-URI on an admin call. If that URI is constructed
5768 appropriately, the PSAP can identify which queue inside the PSAP to which the call is
5769 destined.

5770 **4.6.10 QueueState**

5771 The PSAP MUST implement a QueueState notifier as described in Section 4.2.1.3 for all
5772 queues it manages.

5773 **4.6.11 SI**

5774 The PSAP MAY provide⁴⁰ a GIS server interface, as described in Section 3.6, for the ECRF,
5775 GIS Replica, and other interfaces. The PSAP MAY provide the MSAG Conversion Service
5776 (server side) or MAY use an ESInet service (client side).

5777 **4.6.12 Logging Service**

5778 The PSAP MUST implement a Logging Service client, as defined in Section 4.12, including
5779 the client side of the media recording mechanism (Section 4.12.2). Provisioning controls
5780 whether the PSAP records media. The PSAP MAY deploy a Logging Service (as described in
5781 Section 4.12) inside the PSAP, in which case it MUST provide the Logging Service retrieval
5782 functions. A PSAP MUST be able to use a Logging Service hosted in the ESInet.

5783 **4.6.13 Security Posture**

5784 The PSAP MUST provide a Security Posture notifier as described in Section 2.4.2.

5785 **4.6.14 Policy**

5786 The PSAP MAY provide a Policy Store as described in Section 3.3.1, in which case it MUST
5787 implement the server-side of the policy retrieval functions, and MAY provide the server-side
5788 of the policy storage function. The PSAP MAY provide a Policy Editor, in which case it MUST
5789 deploy the client-side of the policy retrieval and storage functions. If the PSAP uses a Policy
5790 Store outside the PSAP to control functions inside the PSAP, it MUST deploy the client-side
5791 of the policy retrieval functions.

5792 PSAPs MUST provide a RoutePolicy in the upstream PRF for the queue(s) to which its calls
5793 are sent. PSAPs MUST also provide an Enqueuer policy to specify which entities are allowed
5794 to send it calls.

5795 **4.6.15 Additional Data Dereference**

5796 The PSAP MUST deploy a dereference (HTTPS GET) interface for additional data as
5797 described in Section 7, as well as the IS-ADR identity query mechanism. Local PSAP policy
5798 MAY dictate which Additional Data, if any, is retrieved and used. The PSAP MUST also be
5799 able to dereference an EIDO URI for a call transferred to it.

⁴⁰ The GIS system may be provided by a 9-1-1 Authority.

5800 **4.6.16 Time Interface**

5801 The PSAP MUST implement an NTP client interface for time of day information. The PSAP
5802 MAY also provide an interface to a hardware clock.

5803 **4.6.17 Test Call**

5804 PSAPs MUST support the test call interface as described in Section 9, although
5805 administrative provisioning processes SHOULD be available to disable it, especially under
5806 overload conditions. The test interface includes the ability of the test caller to offer media,
5807 receive a response, and loop back a small number of packets of each media accepted at
5808 the PSAP. PSAPs MUST support test of all media – voice, video, and text.

5809 PSAPs may wish to arrange to have test calls sent to it periodically from a known source so
5810 that it can be assured that calls from outside the ESInet can get to the PSAP. For that
5811 purpose, a “Test Call Generator” Functional Element may be used that the PSAP can
5812 control. The Test Call Generator interface includes a Web Service with a single function:
5813 SendCallRequests. The OpenAPI definition of this web service may be found in Appendix
5814 E.6.

5815 **4.6.17.1 SendCallRequests**

5816 Updates an existing send call request identified by the PSAP ID or creates a new one if the
5817 request does not exist.

5818 HTTP method: PUT

5819 Resource name .../ SendCallRequests/{psapId}:

5820 Parameters:

Name	Condition	Description
psapId	MANDATORY	AgencyId of the PSAP that wishes to have test calls sent to it
location	MANDATORY	PIDF-LO used for location of test calls
frequency	MANDATORY	Minutes between test call send
discrepancyRateLimit	MANDATORY	Max number of Discrepancy Reports per hour
startDate	MANDATORY	When to start sending test calls
endDate	MANDATORY	When to stop sending test calls

Name	Condition	Description
testConditions	OPTIONAL	PrrTest conditions (see below) for the test

5821 Status Codes

5822 200 OK
 5823 442 Unacceptable Parameters
 5824 454 Unspecified Error
 5825 458 Policy Violation

5826 **4.6.18 Testing of Policy Rules**

5827 To be able to test that the ruleset for a particular nominal next hop works as expected, the test call MAY include a Call-Info header field with a purpose parameter of "emergency-prr-test". The data retrieved from the URI in the Call-Info header field is a JSON data structure that contains a list of name/value pairs. The names are strings that would be legal as a single component in the condition portion of a PRR rule (not allowing AND/OR). The structure includes the hostname of an ESRP and the unique ID (FQDN) of a "nominal next hop". The ESRP processing such a test call, if it is named in the structure, and the nominal next hop is named in the structure, sets the elements in the list to the corresponding values, rather than the actual values, when it evaluates the ruleset.

5836 PrrTest

Name	Condition	Description
hostName	MANDATORY	ESRP Hostname that test conditions are specified for
nominalNextHop	MANDATORY	URI of for nominal next hop that rule set conditions are applied to
conditions	MANDATORY (may be repeated)	Array

5837 The conditions array contains:

[MM/DD/YYYY]

Page 203 of 675



Name	Condition	Description
name	MANDATORY	One of TimePeriodCondition, SipHeaderCondition, AdditionalDataCondition, MimeBodyCondition, LocationCondition, CallSuspicionCondition, QueueStateCondition, LostServiceUrnCondition, ServiceStateCondition, CallSourceCondition, BodyPartCondition, RequestUriCondition, NormalNextHopCondition, IncomingQueueCondition, SdpOfferCondition, CapCondition, CallingNumberVerificationStatusCondition]
value	MANDATORY	Value of the condition (as a string)

5838

5839 These test calls MUST originate from within the ESInet and MUST come from an entity with
 5840 credentials traceable to the PCA and trusted by the ESRP. The ESRP has a policy
 5841 (TestCalls) that specifies which originators (the identifier in the credential) from which it
 5842 will process PRR test calls. The URIs are dereferenced with an HTTPS GET protected by
 5843 TLS. The credentials used by the server MUST be traceable to the PCA and MUST occur in
 5844 the ESRP policy.

5845 More than one Call-Info URI with a purpose of “emergency-prr-test” may occur in a test
 5846 call, each with unique combinations of ESRP and nominal-next-hop targets.

5847 **4.6.19 Call Diversion**

5848 A PSAP may become overloaded and be unable to answer every call. Overload is
 5849 determined by exceeding the size of the primary queue to which its calls are sent. Routing
 5850 rules for the PSAP would then cause calls to receive an alternate call treatment:

- 5851 • Calls can be sent a “Busy” indication;
- 5852 • Calls can be diverted to an Interactive Media Response unit;
- 5853 • Calls can be diverted to one or more alternate PSAPs.

5854 The latter is mechanized by sending the call to queues that other PSAPs dequeue. Since
 5855 the diverted-to PSAP(s) must explicitly permit (via the Enqueue policy and possibly
 5856 DequeueRegistration) calls to be placed on its queues, no calls can be sent to a PSAP that
 5857 hasn’t explicitly asked for them.

[MM/DD/YYYY]

Page 204 of 675



5858 PSAPs that agree to take calls from other PSAPs may require explicit management approval
5859 at the time the calls are sent. Effectively, such PSAPs are agreeing to take calls on a
5860 standby basis only, and explicit management action is required before the calls will actually
5861 be accepted.

5862 To accomplish this, the diverted-to PSAP registers to the DequeueRegistration of the
5863 diverted-from PSAP. The diverted-from PSAP subscribes to the QueueState event for the
5864 diversion queue, but the diverted-to PSAP will have the "Standby" parameter set to "true".
5865 It may specify a filter that limits notifications to those setting QueueState to
5866 "DiversionRequested". When the QueueState event notification occurs with
5867 "DiversionRequested" state, the diverted-to PSAP management would be alerted. If it
5868 agrees to accept calls, it would change its QueueState Standby parameter to "false", and
5869 calls would subsequently be sent to it. When the diverted-to PSAP determines that its
5870 services are no longer needed, it can reinstate the Standby to "true".

5871 **4.6.20 Incidents**

5872 A new emergency call arrives with a new Incident Tracking Identifier already assigned.
5873 Initially, each emergency call is a new Incident. The call taker may determine that the call
5874 is actually part of another Incident, usually reported in a prior call. The PSAP MUST merge
5875 the IncidentTrackingID assigned by the ESRP with the actual IncidentTrackingID. It does
5876 so with the IncidentMergeEvent log record and sends an EIDO with a Merge Information
5877 component. Incidents can also be linked or split as described in the Logging Service
5878 (Section 4.12). The actual IncidentTrackingID would be part of the EIDO object passed to
5879 a secondary PSAP or responder and part of the INVITE if the call is transferred. When the
5880 PSAP completes processing of an Incident, it logs a IncidentClearEvent record.

5881 **4.7 Bridging and Transfers**

5882 Bridging is used in NG9-1-1 to transfer calls and conduct conferences. Bridges have a SIP
5883 signaling interface to create and maintain conferences and media mixing capability. Bridges
5884 MUST be multimedia capable (voice, video, text). A bridge is necessary to transfer a call
5885 because IP-based devices normally cannot mix media, and transferring always adds the
5886 new party (for example, a call taker at a transfer-to PSAP) to the call before the transferor
5887 (for example, the original call taker at the PSAP which initially answered the call) drops off
5888 the call.

5889 **4.7.1 Attended Transfers**

5890 This document describes two ways that bridging is employed. One way is termed "ad hoc"
5891 and is characterized by using a bridge only when it is needed during transferring or
5892 conferencing more than two parties.

5893 The rough transfer sequence for ad hoc, based on the procedures defined in RFC 4579⁴¹
5894 [39], is:

- 5895 1. PSAP creates a conference on the bridge
- 5896 2. PSAP REFERs the caller to the bridge
- 5897 3. PSAP tears down the original PSAP-Caller leg
- 5898 4. PSAP REFERs transfer target (transfer-to PSAP for example) to the conference
- 5899 5. PSAP tears down its leg to the conference, the transfer-to PSAP and the caller
5900 remain
- 5901 6. Transfer-to PSAP REFERs the caller to it
- 5902 7. Transfer-to PSAP terminates the conference.

5903 **Note:** When the caller drops voluntarily or involuntarily from the ad hoc Bridge, leaving
5904 only two participants, the ad hoc bridge must identify which participant will release the
5905 bridge resources. This can be achieved by moving the host in the <host-info> element on
5906 the conference subscription's NOTIFY. A future revision of this document will normatively
5907 specify this behavior.

5908 Some calling devices may not support the Replaces header field (which can be determined
5909 by examining the content of the Supported header field to see if a "replaces" option tag is
5910 present, or by completing an OPTIONS transaction and obtaining the Accept header field
5911 that way). If the calling device does not support the Replaces header field, then a B2BUA
5912 in the path MUST be present which does support the Replaces header field in an ESInet
5913 supporting ad hoc bridging. Often, this B2BUA will be part of the BCF. All calls are relayed
5914 through the B2BUA. The B2BUA is transparent to signaling with the following exceptions:

- 5915 1. The Contact URL is modified to be a URL of the B2BUA for both the caller (Contact
5916 in INVITE) and PSAP (Contact in 200 OK).
- 5917 2. The REFER method, when executed on the PSAP side to a conference bridge, causes
5918 the bridge to invite the B2BUA to the conference, and the B2BUA to respond as
5919 illustrated below. The leg between the caller and the B2BUA sees no transaction.
- 5920 3. If the B2BUA receives an INVITE from a caller that does not include a Supported
5921 header field containing the "replaces" option-tag, it MUST include a Supported

⁴¹ The ad hoc method described in this document functionally adheres to RFC 4579 however the terminology used herein may differ. For example, the "Bridge" relates to the "Focus" application in RFC 4579 and the "Conference Application" relates to the "Conference-Factory" application in RFC 4579. The terms used herein should be interpreted broadly to support functionalities defined in RFC 4579.

5922 header field containing the “replaces” option-tag in the INVITE forwarded to the
5923 ESInet and provide the functionality described in this section.

5924 4. Media endpoints towards both the caller and the PSAP MAY be rewritten to be
5925 contained within the B2BUA.

5926 The other mechanism is “Route All Calls Via a Conference Aware UA”. In this mechanism,
5927 at least the signaling portion of a bridge is always in the call path, and transfer is
5928 accomplished by adding and deleting parties to the bridge. An element in the call path
5929 effectively operates as a B2BUA, modifying the call signaling towards the PSAP and the
5930 response to the caller so that it appears as a bridge in the path, and, when transfer is
5931 actually needed, what was a B2BUA operates as a true bridge, allowing the transfer-to
5932 PSAP to be added to the bridge and the transfer-from PSAP to drop from the bridge. Often,
5933 a media mixer is not in the path unless needed.

5934 The high-level transfer sequence for this method is:

- 5935 1. The original call arrives at a conference-aware UA.
- 5936 2. The conference-aware UA acts as a B2BUA and modifies the signaling towards the
5937 PSAP by adding the conference marker (“isfocus”) and modifying the Contact to be
5938 itself rather than the caller.
- 5939 3. The PSAP gets the call, and responds in the normal way. The response to the initial
5940 call will be sent to the conference-aware UA.
- 5941 4. The conference-aware UA modifies the response from the PSAP towards the caller
5942 by adding the conference indicator, and modifies the Contact to identify itself. It
5943 MAY NOT modify the SDP, so the media is set up directly between the caller and the
5944 PSAP.
- 5945 5. At some point, the PSAP desires to transfer the call to a transfer-to PSAP. Since it
5946 has the ‘isfocus’ from the conference UA already, it sends the conference-aware UA
5947 a REFER to ask it to add the transfer-to PSAP to the conference.
- 5948 6. The conference-aware UA sends an INVITE to the transfer-to PSAP. It also MAY re-
5949 INVITE both the caller and the transfer-from PSAP, including SDP that moves the
5950 media to a media mixer if it was not already connected to one. The conference-
5951 aware UA is now acting as a normal bridge.
- 5952 7. All parties accept their INVITEs and a 3-way conference with media mixing ensues.
- 5953 8. The transfer-from PSAP then leaves the conference by sending a BYE.
- 5954 9. The conference-aware UA then MAY re-INVITE the caller and the transfer-to PSAP,
5955 including signaling that will move the media to be direct between the transfer-to
5956 PSAP and the caller.

5957 All Bridges in the ESInet/NGCS MUST implement the Session Recording Client interface
5958 defined by SIPREC (RFC 7866) [116]. Provisioning MAY control whether the bridge does log
5959 media.

5960 When the bridge is used to transfer the call, the location of the caller and any Additional
5961 Data included (or retrieved in conjunction) with the call MUST be transferred to the
5962 transfer target. The NENA Call Identifier and the NENA Incident Tracking Identifier MUST
5963 be copied from the REFER to the outgoing INVITE. The REFER MUST contain a suitable
5964 URN, usually the urn used to query the ECRF to determine the correct responder, or an
5965 appropriate urn from the urn:emergency:service:responder tree if a specific responder was
5966 selected, a 'serviceurn' parameter of the Refer-To . A misrouted call being transferred to
5967 the proper PSAP would typically be urn:service:sos, but could be
5968 urn:emergency:service:psap if the ECRF was not used to reroute the call. The Refer-To
5969 header field contains the URI of the target (which may be returned from a LoST query) and
5970 MUST contain the URN (in the urn:service:sos or urn:emergency:service:sos trees) as a
5971 URI parameter of 'serviceurn'. The REFER to the bridge has the bridge's URI in the To: and
5972 in the Request-URI. It also contains a Referred-By header field (RFC 3892) [28] with the
5973 URI of the primary PSAP. When the INVITE is created by the bridge to the secondary
5974 PSAP, the INVITE MUST contain the service URN in the Request-URI, with a Route header
5975 field containing the URI (which should include the "lr" parameter to avoid Request-URI
5976 rewriting) found in the Refer-To header field, and MUST contain a Referred-By header field
5977 with the URI of the primary PSAP per RFC 3892. S/MIME protection of the referrer is
5978 OPTIONAL. If there was no 'serviceurn' parameter and there is an EIDO, the bridge sets
5979 the Request-URI to urn:emergency:service:sos. Additionally, any information the PSAP has
5980 determined beyond what it was sent SHOULD be given to the transfer target. The
5981 mechanism for accomplishing this is to create an EIDO and include it "by reference" in the
5982 transfer operation. The transferor creates the EIDO and includes a reference to the EIDO in
5983 a Call-Info header field with a purpose parameter of "emergency-eido" as an escaped
5984 header field in the Refer-To header field. Note that the Refer-To header field MUST be a
5985 sip URI. Tel URIs do not support purpose parameters. The bridge will then include this
5986 header field in the INVITE it sends to the transfer target. The EIDO includes the location
5987 reported for the caller (in the form it received it, i.e., by-value or by-reference), the
5988 callback number, and any Additional Data included (or retrieved in conjunction with) the
5989 call. (See Section 4.7.2 for further discussion.) An example of the associated header fields
5990 is shown below.

5991 REFER sip:+12125551234@OSP-Provider.com SIP/2.0
5992 ...
5993 Refer-To:<sip:Poison-Control@cnty.st.us?Call-Info=https%3A%2F%2FNG911PSAP-%
5994 A.911Authority-A.net%2Feido09245673%3Bpurpose%3Demergency-eido>
5995 ...

5996 The bridge is a service: each element of the bridge MUST implement the server-side of
5997 ElementState and the set of bridge elements MUST implement the server-side of
5998 ServiceState. As bridges are typically a local service, it is RECOMMENDED that ServiceState

[MM/DD/YYYY]

Page 208 of 675



5999 for the bridge service be implemented by each NGCS that provides a bridge service. For
6000 the Ad Hoc case, the transfer-to PSAP MUST release the bridge when the transfer-from
6001 PSAP terminates its leg of the call in order to release bridge resources.

6002 As discussed in Section 5.7 of NENA 08-002 [70], there is a problem in that some devices
6003 which could originate 9-1-1 calls do not support the Replaces header field. If a PSAP needs
6004 to transfer a call originated by such a device, it cannot use the standardized SIP signaling
6005 to the caller as described above. With Route All Calls Via a Conference-Aware UA, the
6006 conference-aware UA never changes the leg towards the caller (unless it must re-INVITE to
6007 change SDP if the initial media was negotiated directly between the caller and the PSAP).
6008 Thus, the calling device need not support the Replaces header field. For the ad hoc
6009 method, to support devices that do not implement the Replaces header field, a Back-to-
6010 Back User Agent is needed between the caller and the bridge/PSAP. Often the B2BUA will
6011 be located in the BCF, because most commercial Session Border Controllers which are
6012 deployed within a BCF have that functionality built in. Some SBCs may “anchor” media,
6013 meaning that they terminate the caller’s media at the B2BUA and relay it towards the PSAP
6014 or bridge. Others may only affect the signaling. The B2BUA element will always be in the
6015 path for all callers if deployed, especially if it is part of the BCF but may not affect the
6016 signaling for callers that indicate support for Replaces.

6017 Conferencing procedures are documented in RFC 4579 [39]. This document includes
6018 definition of an Event package that allows conference participants to manage the
6019 conference. In the message sequences below, all participants are conference-aware (that
6020 is, they implement the event package). It is not necessary for the caller to be conference-
6021 aware. If the caller is not conference aware, the SUBSCRIBE to the conference package
6022 does not occur. The caller, or some element in the path, MUST implement the Replaces
6023 header field (see Section 3.1.1.2). Three scenarios are illustrated below: Ad Hoc without
6024 B2BUA, Ad Hoc with B2BUA- and Route All Calls Via a Conference-Aware UA.

6025 **4.7.1.1 SIP Ad Hoc Flow with No B2BUA on Ingress Call Path**

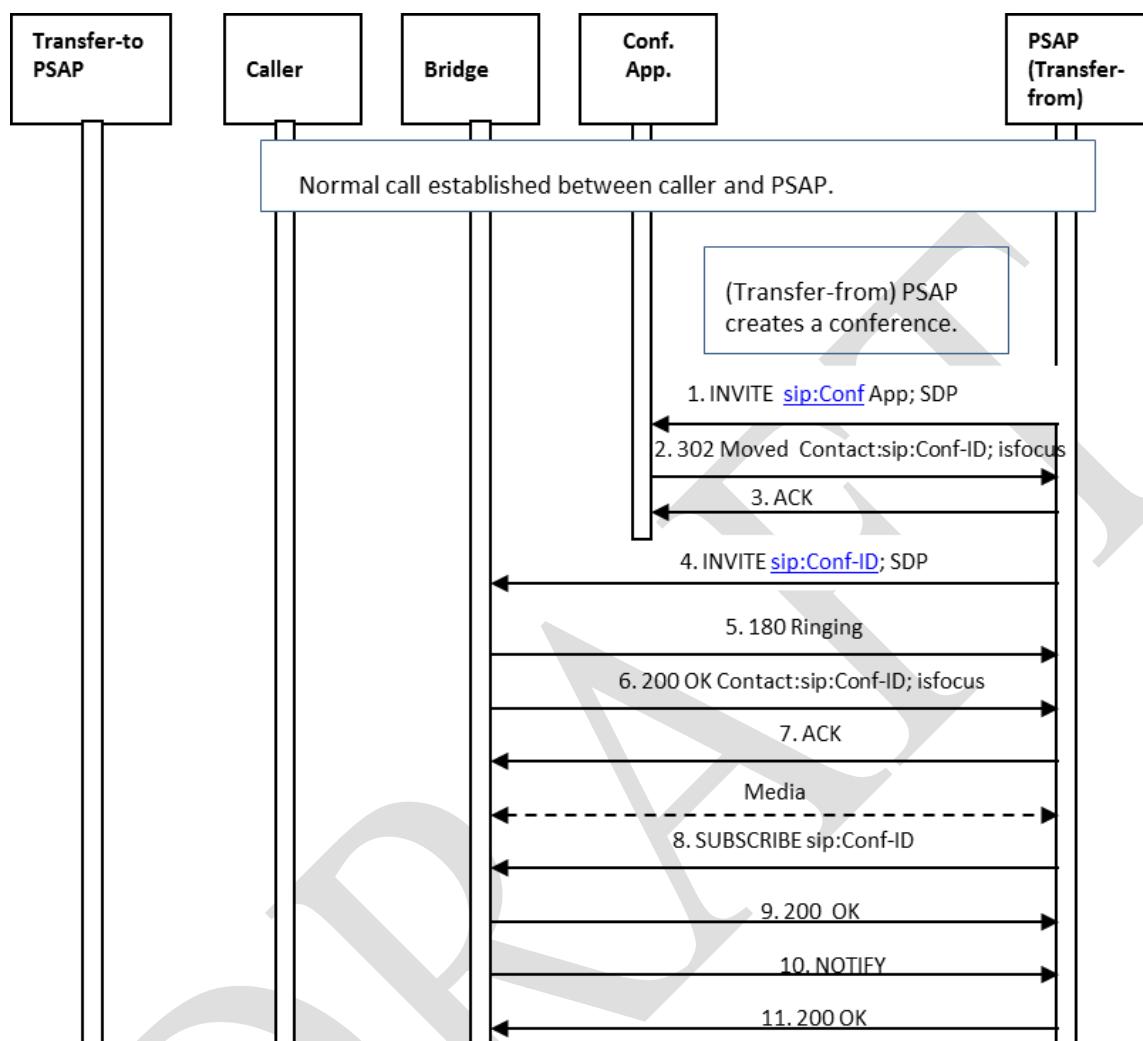
6026 **4.7.1.1.1 Creation of a Conference**

6027 This scenario described in the call flow depicted below follows Section 5.4 of RFC 4579
6028 [39].

[MM/DD/YYYY]

Page 209 of 675





6029

6030

Figure 4-1. Ad Hoc Conference Call Flow Using SIP

- 6031 1. The transfer-from PSAP creates a conference by first sending an INVITE with
6032 specified Media in the SDP to a conference application, using a URI that is known
6033 by/provisioned at the transfer-from PSAP.
6034 2. The Conference Application responds by sending a 302 Moved message, which
6035 redirects the transfer-from PSAP to the conference bridge and provides the
6036 Conference URI that SHOULD be used for the conference.
6037 3. The transfer-from PSAP acknowledges the receipt of the 302 Moved message.

[MM/DD/YYYY]

Page 210 of 675

- 6038 4. The transfer-from PSAP generates an INVITE with specified Media in the SDP to
6039 establish a session with the conference bridge⁴².
6040 5. The conference bridge responds to the INVITE by returning a 180 Ringing message.
6041 6. The conference bridge then returns a 200 OK message, and a media session is
6042 established between the transfer-from PSAP and the conference bridge.
6043 7. The transfer-from PSAP returns an ACK message in response to the 200 OK.
6044 *Media: If SDP includes media-type specification for audio and/or video and/or RTT, then*
6045 *RTP media is exchanged. If SDP includes media-type specification for MSRP, then*
6046 *MSRP messages are exchanged.*
6047 8. through 11. Once the media session is established, the transfer-from PSAP
6048 subscribes to the conference associated with the URI obtained from the Contact
6049 header field provided in the 200 OK message from the conference bridge.

6050 **4.7.1.1.2 Transfer-from PSAP Asks Bridge to Invite the Caller to the**
6051 **Conference**

6052 This flow is based on Section 5.10 of RFC 4579 [39].

⁴² Note that, based on RFC 4579, the messages sent in Steps 2, 3, and 4 are optional and may not be exchanged if the conference application and the media server are the same.

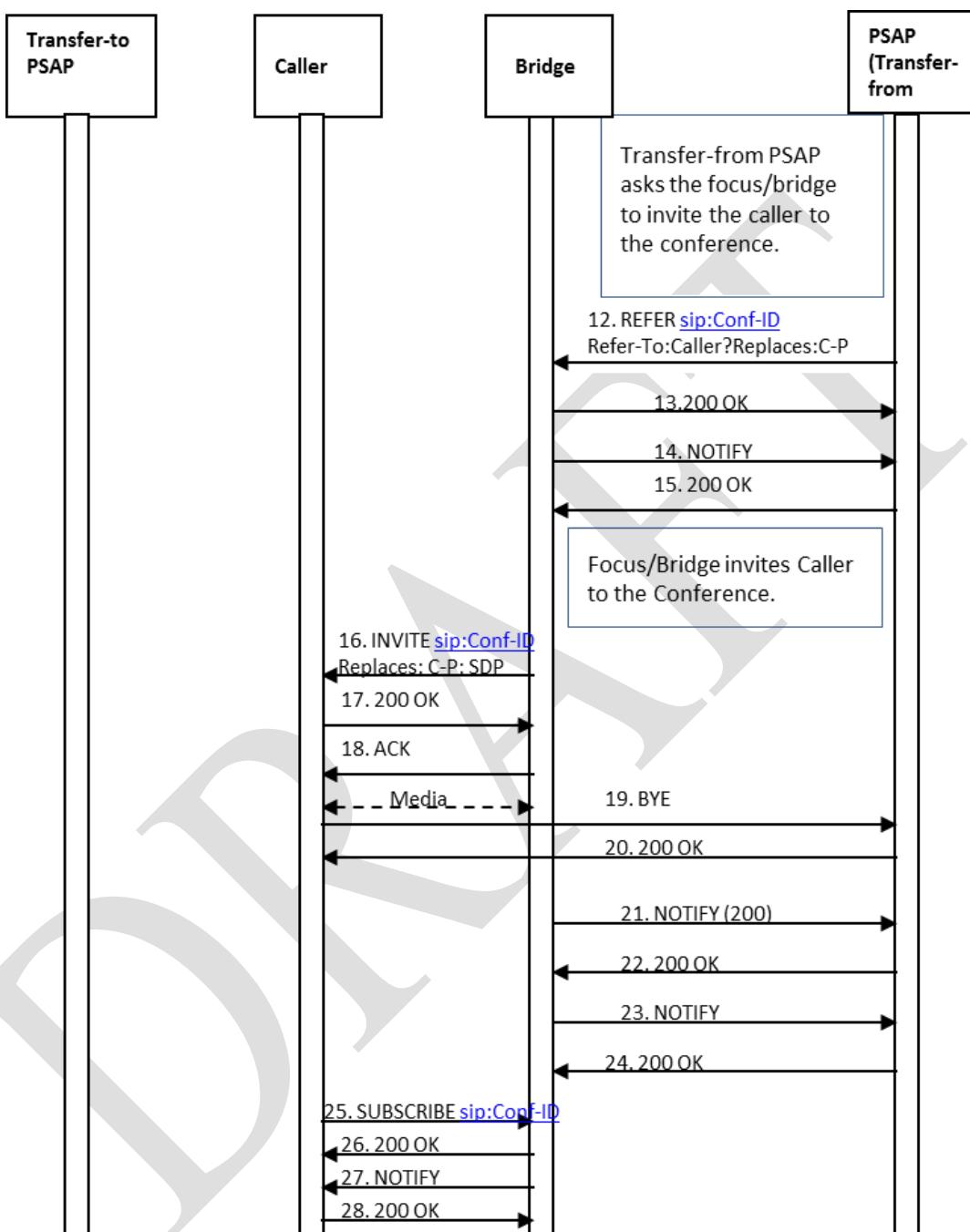


Figure 4-2 Transfer-from PSAP Asks Bridge to Invite the Caller to the Conference

6053

6054

6055

6056

6057

12. After the transfer-from PSAP establishes the conference, it sends a REFER method to the conference bridge asking it to invite the caller to the conference. The REFER

- 6058 method contains an escaped Replaces header field value in the URI included in the
6059 Refer-To header field.
- 6060 13. The bridge returns a 200 OK message to the transfer-from PSAP.
- 6061 14. The bridge then returns a NOTIFY message, indicating the subscription state of the
6062 REFER request (i.e., active).
- 6063 15. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
- 6064 16. The bridge invites the caller to the conference by sending an INVITE method
6065 containing the Conference URI and a Replaces header field that references the leg
6066 between the caller and the transfer-from PSAP and specified Media in the SDP.
- 6067 17. The caller accepts the invitation by returning a 200 OK message.
- 6068 18. The bridge acknowledges receipt of the 200 OK message by returning an ACK.
A media session is established between the caller and the bridge.
- 6069 *If SDP includes media-type specification for audio and/or video and/or RTT, then RTP
6070 media is exchanged. If SDP includes media-type specification for MSRP, then MSRP
6071 messages are exchanged.*
- 6072 19. The caller releases the connection to the transfer-from PSAP by sending a BYE
6073 message.
- 6074 20. The transfer-from PSAP responds by returning a 200 OK message.
- 6075 21. The bridge sends a NOTIFY message to the transfer-from PSAP to provide REFER
6076 processing status.
- 6077 22. The transfer-from PSAP responds by returning a 200 OK message.
- 6078 23. The bridge sends a NOTIFY message to the transfer-from PSAP to provide updated
6079 status associated with the conference state.
- 6080 24. The transfer-from PSAP responds by returning a 200 OK message.
- 6081 25. The caller subscribes to the conference associated with the Conference URI provided
6082 in the INVITE message from the bridge by sending a SUBSCRIBE message to the
6083 bridge. (Optional)
- 6084 26. The bridge acknowledges the subscription request by sending a 200 OK message
6085 back to the caller. (Optional)
- 6086 27. The bridge then returns a NOTIFY message to the caller to provide subscription
6087 status information. (Optional)
- 6088 28. The caller responds by returning a 200 OK message. (Optional)
- 6089
- 6090

6091 **4.7.1.1.3 Transfer-to PSAP is Invited to the Conference**

6092 This flow is based on Section 5.5 of RFC 4579 [39].

[MM/DD/YYYY]

Page 213 of 675



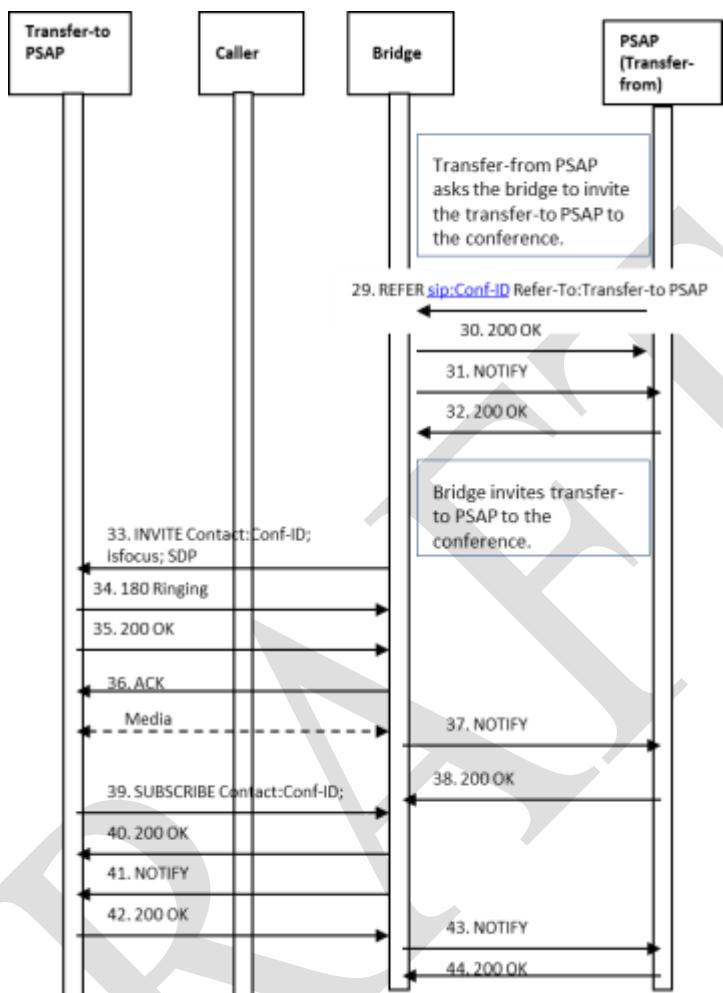


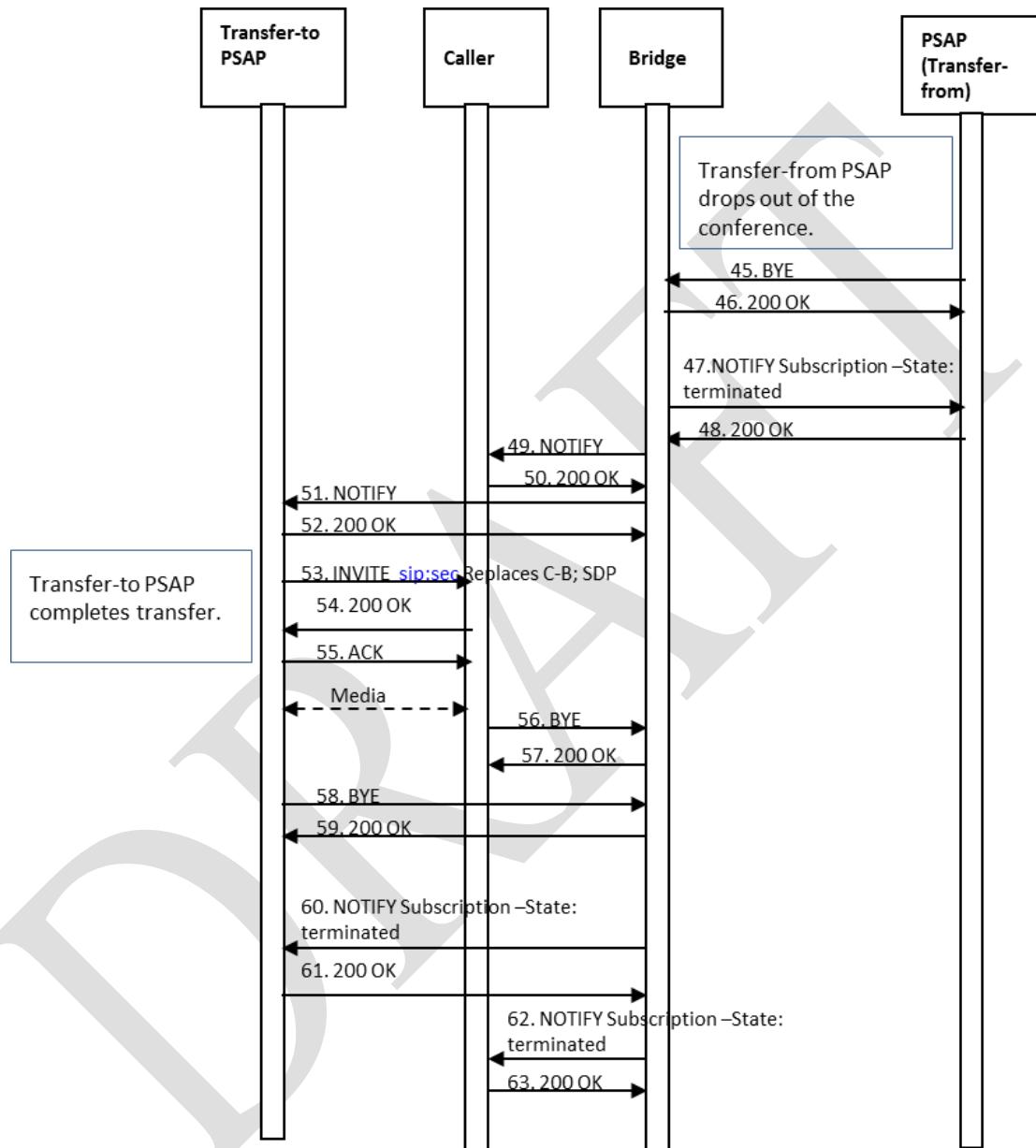
Figure 4-3 Secondary PSAP Invited to Conference

- 6093
6094
6095 29. The transfer-from PSAP sends a REFER method to the conference bridge asking it to
6096 invite the transfer-to PSAP to the conference. The REFER method contains the
6097 Conference URI and a Refer-To header field that contains the URI of the transfer-to
6098 PSAP. The REFER method also contains an escaped Call-Info header field value
6099 containing a reference URI that points to the EIDO data structure and a purpose
6100 parameter of "emergency-eido".
6101 30. The bridge returns a 200 OK message to the transfer-from PSAP.
6102 31. The bridge then returns a NOTIFY message, indicating that subscription state of the
6103 REFER request (i.e., active).
6104 32. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
6105 33. The bridge invites the transfer-to PSAP to the conference by sending an INVITE
6106 method with SDP containing the Conference URI and Contact header field that

6107 contains the Conference URI and the 'isfocus' feature parameter. The INVITE
6108 contains the Call-Info header field containing a reference URI that points to the
6109 EIDO data structure and a purpose parameter of "emergency-eido".
6110 34. The transfer-to PSAP UA responds by returning a 180 Ringing message to the
6111 bridge.
6112 35. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
6113 36. The bridge acknowledges receipt of the 200 OK message by returning an ACK.
6114 *A media session is established between the transfer-to PSAP and the bridge.*
6115 *If SDP includes media-type specification for audio and/or video and/or RTT, then RTP*
6116 *media is exchanged. If SDP includes media-type specification for MSRP, then MSRP*
6117 *messages are exchanged.*
6118 37. The bridge returns a NOTIFY message to the transfer-from PSAP to provide updated
6119 status of the subscription associated with the REFER request.
6120 38. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6121 message.
6122 39. The transfer-to PSAP subscribes to the conference associated with the Conference
6123 URI provided in the INVITE message from the bridge by sending a SUBSCRIBE
6124 message to the bridge.
6125 40. The bridge acknowledges the subscription request by sending a 200 OK message
6126 back to the transfer-to PSAP.
6127 41. The bridge then returns a NOTIFY message to the transfer-to PSAP to provide
6128 subscription status information.
6129 42. The transfer-to PSAP responds by returning a 200 OK message.
6130 43. The bridge sends a NOTIFY message to the transfer-from PSAP providing updated
6131 status for the subscription associated with the REFER request.
6132 44. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6133 message.
6134 *At this point the caller, transfer-from PSAP, and transfer-to PSAP are all participants in*
6135 *the conference.*

6137
6138

4.7.1.1.3.1 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP Completes Transfer



6139
6140
6141
6142
6143

Figure 4-4 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

45.Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the bridge.

- 6144 46. The conference bridge responds by returning a 200 OK message.
6145 47. The bridge then returns a NOTIFY message indicating that the subscription to the
6146 conference has been terminated.
6147 48. The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
6148 49. The bridge then returns a NOTIFY message to the caller indicating that there has
6149 been a change to the subscription state. (Optional)
6150 50. The caller returns a 200 OK in response to the NOTIFY. (Optional)
6151 51. The bridge returns a NOTIFY message to the transfer-to PSAP indicating that there
6152 has been a change to the subscription state.
6153 52. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.
6154 53. Upon recognizing that the caller and the transfer-to PSAP are the only remaining
6155 participants in the conference, the transfer-to PSAP completes the transfer by
6156 sending an INVITE to the caller requesting that they replace their connection to the
6157 bridge with a direct connection to the transfer-to PSAP. The transfer-to PSAP learns
6158 the URI of the caller through the entity attribute in the endpoint section of the user's
6159 container in the conference NOTIFY from the bridge.
6160 54. The caller responds by returning a 200 OK message to the transfer-to PSAP.
6161 55. The transfer-to PSAP returns an ACK in response to the 200 OK.

6162 *A media session is established between the transfer-to PSAP and the caller.*
6163 *If SDP includes media-type specification for audio and/or video and/or RTT, then RTP*
6164 *media is exchanged. If SDP includes media-type specification for MSRP, then MSRP*
6165 *messages are exchanged.*

6166 56. The caller then sends a BYE to the bridge to terminate the session.
6167 57. The bridge responds by sending the caller a 200 OK message.
6168 58. The transfer-to PSAP also terminates its session with the bridge by sending a BYE
6169 message to the bridge.
6170 59. The bridge responds by sending a 200 OK message to the transfer-to PSAP.
6171 60. The bridge then returns a NOTIFY message to the transfer-to PSAP indicating that
6172 the subscription to the conference has been terminated.
6173 61. The transfer-to PSAP returns a 200 OK in response to the NOTIFY message.
6174 62. The bridge sends a NOTIFY message to the caller indicating that the subscription to
6175 the conference has been terminated. (Optional)
6176 63. The caller responds with a 200 OK message. (Optional)

6177 *At this point, the transfer is complete, and the caller and the transfer-to PSAP are*
6178 *involved in a two-way call.*

6179 4.7.1.2 SIP Ad Hoc Method with B2BUA in the Ingress Call Path

6180 This scenario is the same as above with the addition of the B2BUA for calling devices that
6181 do not support the Replaces header field. In this example, the B2BUA anchors media,
6182 although not all B2BUAs will do that.

6183 4.7.1.2.1 Initial Call and Initial Conference Creation

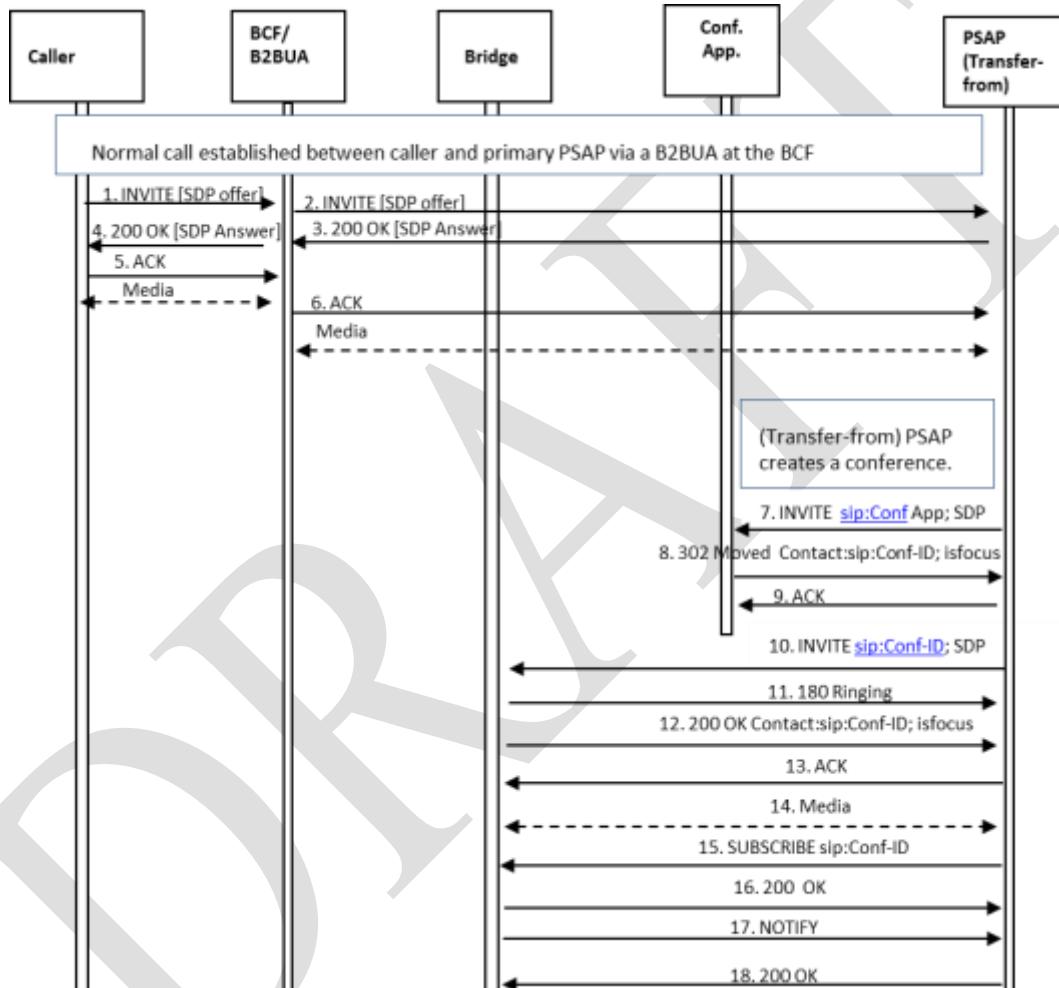


Figure 4-5 Ad Hoc Conference Call Flow Using SIP with B2BUA

- 6184
- 6185 1. The caller initiates an emergency session request by sending an INVITE message to
6186 the B2BUA. The INVITE contains callback information and a Geolocation header with
6187 caller location information. The Supported header field does not indicate support for
6188 the Replaces header field.
6189

- 6190 2. The B2BUA forwards the INVITE to the ESRP (the URI in the Route header field, which
6191 should contain the "lr" parameter to avoid Request-URI rewriting) after changing the
6192 Contact header field to point to itself and changing the offer SDP media endpoint
6193 address and port to be itself. The INVITE includes a Supported header field indicating
6194 support for Replaces. The call proceeds through the ESInet/NGCS normally, and arrives
6195 at a PSAP.
- 6196 3. The PSAP responds by returning a 200 OK message to the B2BUA, including its Contact
6197 URL and answer SDP in the response.
- 6198 4. The B2BUA responds to the receipt of the 200 OK from the PSAP by sending a 200 OK
6199 message to the caller's device, changing the Contact to be itself and the answer SDP
6200 address and port to be itself.
- 6201 5. The caller's device responds by sending an ACK to the B2BUA.
A media session is established between the caller and the B2BUA.
- 6202 6. The B2BUA sends an ACK to the PSAP in response to receiving an ACK from the caller's
6203 device.
- 6204 *A media session is established between the B2BUA and the transfer-from PSAP.*
- 6205 7. The transfer-from PSAP creates a conference by first sending an INVITE with specified
6206 Media in the SDP to a Conference Application, using a URI that is known by/provisioned
6207 at the transfer-from PSAP.
- 6208 8. The Conference Application responds by sending a 302 Moved message, which redirects
6209 the transfer-from PSAP to the conference bridge and provides the Conference URI that
6210 should be used for the conference.
- 6211 9. The transfer-from PSAP acknowledges the receipt of the 302 Moved message.
- 6212 10. The transfer-from PSAP generates an INVITE with specified Media in the SDP to
6213 establish a session with the conference bridge⁴³.
- 6214 11. The conference bridge responds to the INVITE by returning a 180 Ringing message.
- 6215 12. The conference bridge then returns a 200 OK message, and a media session is
6216 established between the transfer-from PSAP and the conference bridge.
- 6217 13. The transfer-from PSAP returns an ACK message in response to the 200 OK.
- 6218 14. Media. If SDP includes media-type specification for audio and/or video and/or RTT, then
6219 RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP
6220 messages are exchanged.
- 6221 15. through 18. Once the media session is established, the transfer-from PSAP subscribes to
6222 the conference associated with the URI obtained from the Contact header field provided
6223 in the 200 OK message from the conference bridge.
- 6224

⁴³ Note that, based on RFC 4579, the messages sent in Steps 2, 8, 9, and 10 are optional and may not be exchanged if the conference application and the media server are the same.

6225 **4.7.1.2.2 Transfer-from PSAP Asks Bridge to Invite the B2BUA to the**
6226 **Conference**

6227 This flow is based on Section 5.10 of RFC 4579 [39].

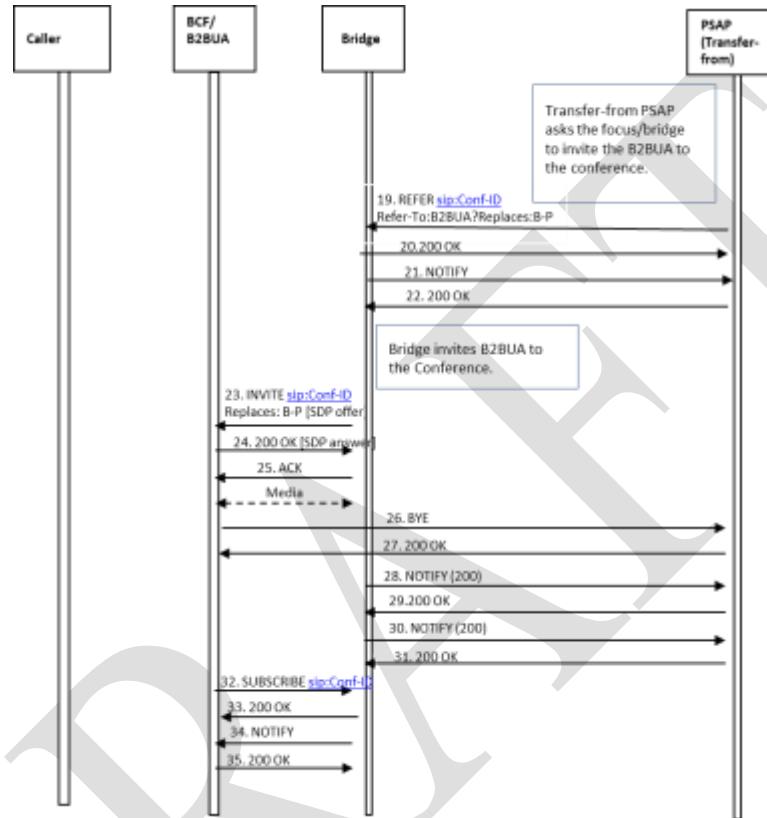


Figure 4-6 Transfer-from PSAP Asks Bridge to Invite the Caller/B2BUA to the Conference

- 6231 19. After the transfer-from PSAP establishes the conference, it sends a REFER method to
6232 the conference bridge asking it to invite the caller/B2BUA to the conference. The REFER
6233 method contains an escaped Replaces header field value in the URI included in the
6234 Refer-To header field.
6235 20. The bridge returns a 200 OK message to the transfer-from PSAP.
6236 21. The bridge then returns a NOTIFY message, indicating the subscription state of the
6237 REFER request (i.e., active).
6238 22. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
6239 23. The bridge invites the caller/B2BUA to the conference by sending an INVITE method
6240 containing the Conference URI and a Replaces header field that references the leg
6241 between the B2BUA and the transfer-from PSAP and an SDP offer.

- 6242 24. The INVITE arrives at the B2BUA. It does not forward the INVITE. Instead, it accepts
6243 the invitation by returning a 200 OK message containing an answer SDP with the media
6244 address and port of itself.
6245 25. The bridge acknowledges receipt of the 200 OK message by returning an ACK.
6246 *A media session is established between the B2BUA and the bridge. The media session*
6247 *between the caller and the B2BUA is not affected. If SDP includes media-type*
6248 *specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP*
6249 *includes media-type specification for MSRP, then MSRP messages are exchanged.*
- 6250 26. The B2BUA releases the connection to the transfer-from PSAP by sending a BYE
6251 message.
6252 27. The transfer-from PSAP responds by returning a 200 OK message.
6253 28. The bridge sends a NOTIFY message to the transfer-from PSAP to provide REFER
6254 processing status.
6255 29. The transfer-from PSAP responds by returning a 200 OK message.
6256 30. The bridge sends a NOTIFY message to the transfer-from PSAP to provide updated
6257 status associated with the conference state.
6258 31. The transfer-from PSAP responds by returning a 200 OK message.
6259 32. The B2BUA subscribes to the conference associated with the Conference URI provided
6260 in the INVITE message from the bridge by sending a SUBSCRIBE message to the
6261 bridge. (Optional)
6262 33. The bridge acknowledges the subscription request by sending a 200 OK message back
6263 to the B2BUA. (Optional)
6264 34. The bridge then returns a NOTIFY message to the B2BUA to provide subscription status
6265 information. (Optional)
6266 35. The B2BUA responds by returning a 200 OK message. (Optional)

6267 **4.7.1.2.3 Transfer-to PSAP is Invited to the Conference**

6268 This flow is based on Section 5.5 of RFC 4579 [39]. There are no differences (other than
6269 step numbers) between this flow and the comparable flow in the no-B2BUA case.

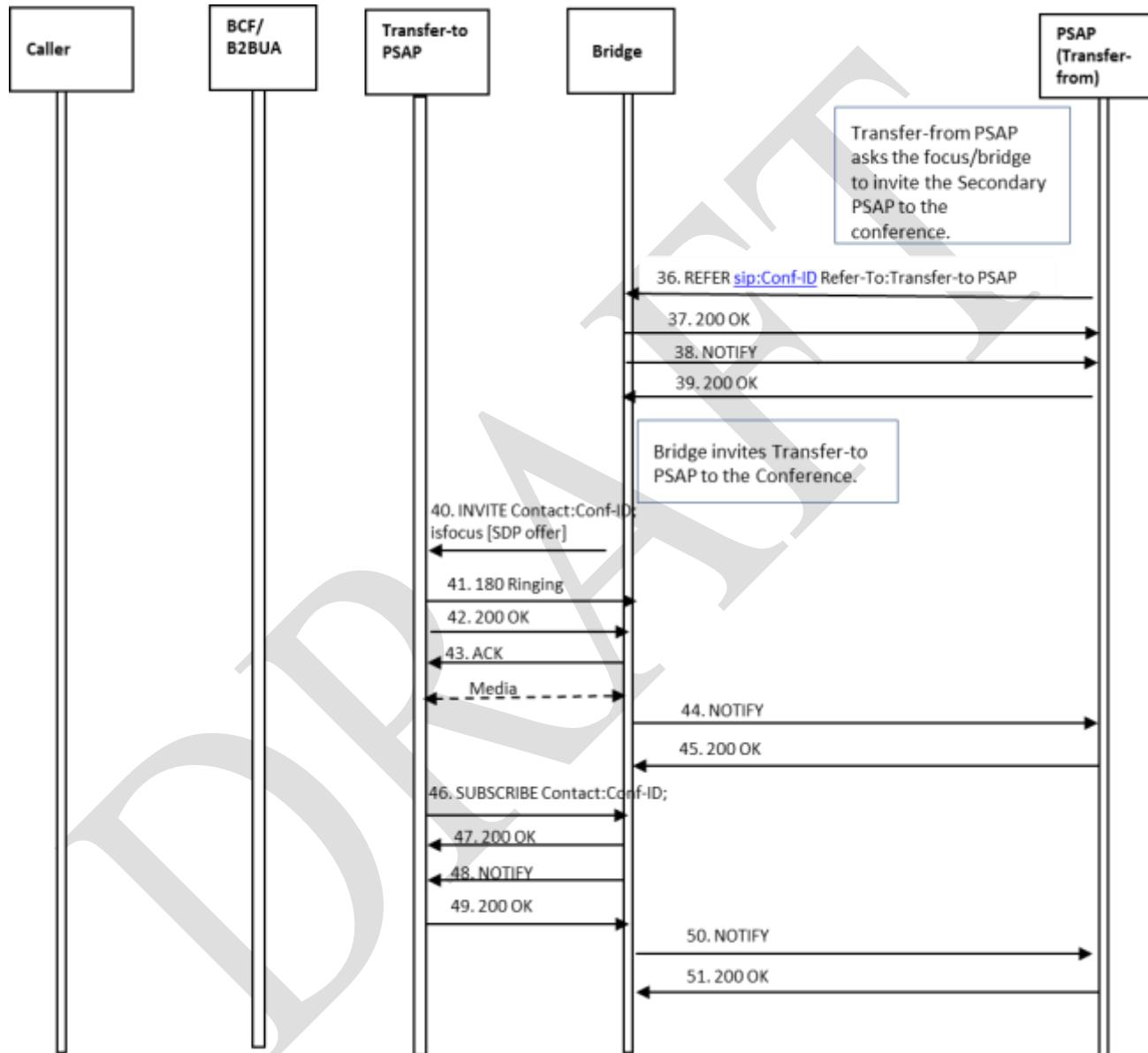


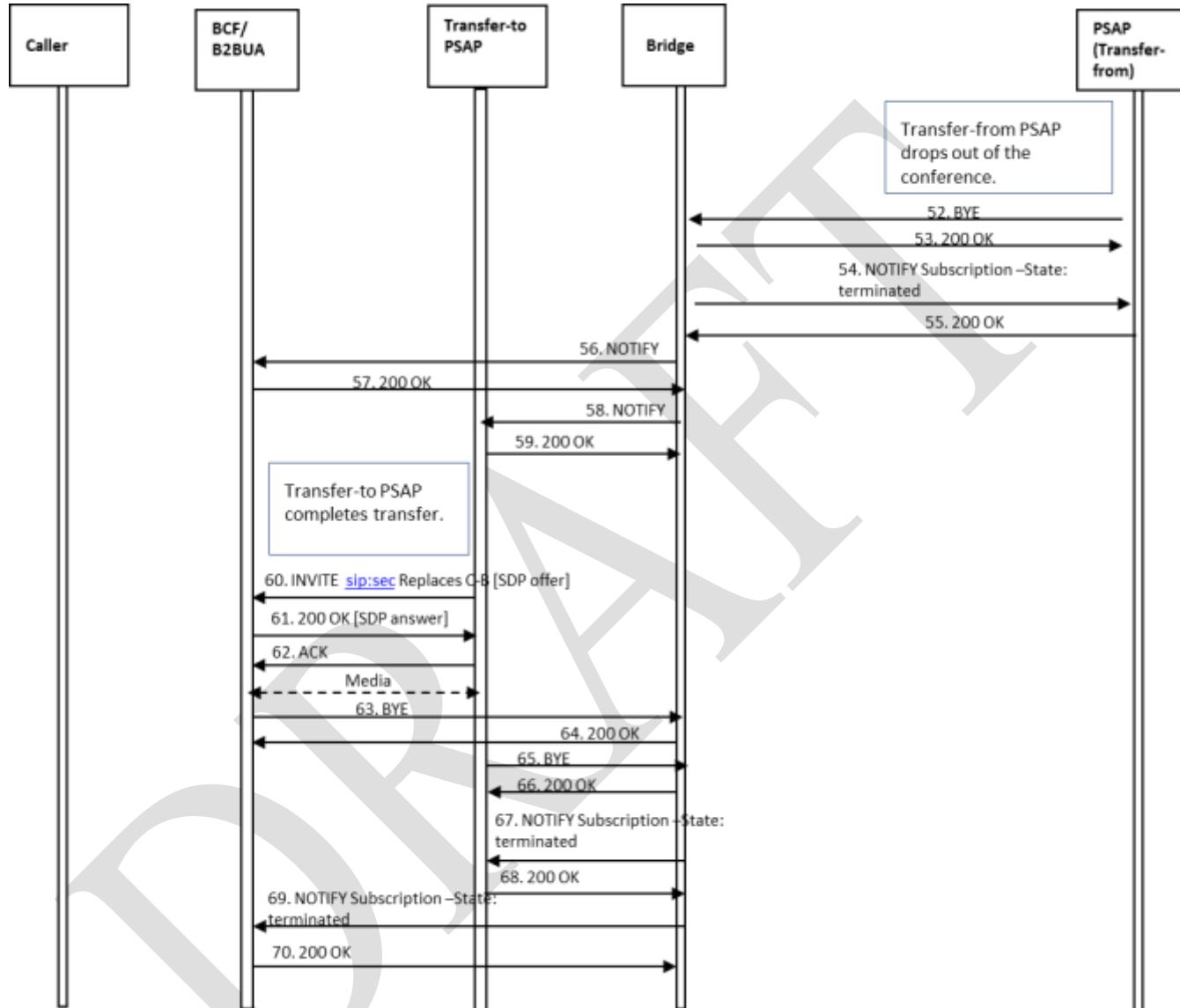
Figure 4-7 Transfer-to PSAP Invited to Conference

6270
6271 36. The transfer-from PSAP sends a REFER method to the conference bridge asking it to
6272 invite the transfer-to PSAP to the conference. The REFER method contains the
6273 Conference URI and a Refer-To header field that contains the URI of the transfer-to
6274 PSAP.

- 6275 PSAP. The REFER method also contains an escaped Call-Info header field value
6276 containing a reference URI that points to the EIDO data structure and a purpose
6277 parameter of "emergency-eido".
6278 37. The bridge returns a 200 OK message to the transfer-from PSAP.
6279 38. The bridge then returns a NOTIFY message, indicating that subscription state of the
6280 REFER request (i.e., active).
6281 39. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.
6282 40. The bridge invites the transfer-to PSAP to the conference by sending an INVITE
6283 method containing the Conference URI and Contact header field that contains the
6284 conference URI, the 'isfocus' feature parameter, and an SDP offer. The INVITE
6285 contains the Call-Info header field containing a reference URI that points to the
6286 EIDO data structure and a purpose parameter of "emergency-eido".
6287 41. The transfer-to PSAP UA responds by returning a 180 Ringing message to the
6288 bridge.
6289 42. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
6290 43. The bridge acknowledges receipt of the 200 OK message by returning an ACK.
6291 *A media session is established between the transfer-to PSAP and the bridge. If SDP*
6292 *includes media-type specification for audio and/or video and/or RTT, then RTP media is*
6293 *exchanged. If SDP includes media-type specification for MSRP, then MSRP messages*
6294 *are exchanged.*
- 6295 44. The bridge returns a NOTIFY message to the transfer-from PSAP to provide updated
6296 status of the subscription associated with the REFER request.
6297 45. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6298 message.
6299 46. The transfer-to PSAP subscribes to the conference associated with the Conference
6300 URI provided in the INVITE message from the bridge by sending a SUBSCRIBE
6301 message to the bridge.
6302 47. The bridge acknowledges the subscription request by sending a 200 OK message
6303 back to the transfer-to PSAP.
6304 48. The bridge then returns a NOTIFY message to the transfer-to PSAP to provide
6305 subscription status information.
6306 49. The transfer-to PSAP responds by returning a 200 OK message.
6307 50. The bridge sends a NOTIFY message to the transfer-from PSAP providing updated
6308 status for the subscription associated with the REFER request.
6309 51. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6310 message.
6311 *At this point the caller (via the B2BUA), transfer-from PSAP, and transfer-to PSAP are all*
6312 *participants in the conference.*

6313
6314

4.7.1.2.4 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP Completes Transfer



6315
6316
6317
6318
6319
6320
6321
6322

Figure 4-8 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

- 52.Upon determining that the emergency call transfer should be completed, the transfer-from PSAP disconnects from the call by sending a BYE message to the bridge.
- 53.The conference bridge responds by returning a 200 OK message.
- 54.The bridge then returns a NOTIFY message indicating that the subscription to the conference has been terminated.

[MM/DD/YYYY]

Page 224 of 675

- 6323 55. The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
6324 56. The bridge then returns a NOTIFY message to the B2BUA indicating that there has
6325 been a change to the subscription state. (Optional)
6326 57. The B2BUA returns a 200 OK in response to the NOTIFY. (Optional)
6327 58. The bridge returns a NOTIFY message to the transfer-to PSAP indicating that there
6328 has been a change to the subscription state.
6329 59. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.
6330 60. Upon recognizing that the caller (via the B2BUA) and the transfer-to PSAP are the
6331 only remaining participants in the conference, the transfer-to PSAP completes the
6332 transfer by sending an INVITE with an SDP offer to the B2BUA requesting that they
6333 replace their connection to the bridge with a direct connection to the transfer-to
6334 PSAP. The transfer-to PSAP learns the URI of the B2BUA through the entity attribute
6335 in the endpoint section of the user's container in the conference NOTIFY from the
6336 bridge.
6337 61. The B2BUA responds by returning a 200 OK message to the transfer-to PSAP.
6338 62. The transfer-to PSAP returns an ACK in response to the 200 OK.
- 6339 *A media session is established between the transfer-to PSAP, the B2BUA (acting as a
6340 media relay), and the caller. If SDP includes media-type specification for audio
6341 and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type
6342 specification for MSRP, then MSRP messages are exchanged.*
- 6343 63. The B2BUA then sends a BYE to the bridge to terminate the session.
6344 64. The bridge responds by sending the B2BUA a 200 OK message.
6345 65. The transfer-to PSAP also terminates its session with the bridge by sending a BYE
6346 message to the bridge.
6347 66. The bridge responds by sending a 200 OK message to the transfer-to PSAP.
6348 67. The bridge then returns a NOTIFY message to the transfer-to PSAP indicating that
6349 the subscription to the conference has been terminated.
6350 68. The transfer-to PSAP returns a 200 OK in response to the NOTIFY message.
6351 69. The bridge sends a NOTIFY message to the B2BUA indicating that the subscription
6352 to the conference has been terminated. (Optional)
6353 70. The B2BUA responds with a 200 OK message. (Optional)
- 6354 *At this point, the transfer is complete, and the caller (via the B2BUA) and the transfer-
6355 to PSAP are involved in a two-way call via the B2BUA.*

6356 **4.7.1.2.5 Call Termination**

6357 If the caller terminates the call, it would send a BYE to the B2BUA. The B2BUA would
6358 forward it to the transfer-to PSAP after modifying the Contact to itself. The transfer-to
6359 PSAP would respond with a 200 OK which it would send to the B2BUA. The B2BUA would

6360 then forward the BYE to the caller. If the PSAP terminates the call, it would send a BYE to
6361 the B2BUA, which would forward it to the caller after modifying the Contact. The caller
6362 would respond to the BYE with a 200 OK which it would send to the B2BUA. The B2BUA
6363 would forward that to the PSAP. (Steps not shown.)

6364 **4.7.1.3 Route All Calls Via a Conference Aware UA**

6365 All incoming 9-1-1 calls are routed via a conference-aware UA. The conference-aware UA
6366 initially acts as a B2BUA but inserts an 'isfocus' parameter in the INVITE forwarded to the
6367 PSAP, and in the 200 OK forwarded to the caller, possibly rewriting the SDP. The caller
6368 remains on the conference-aware UA to which it was first routed (but see Section 4.9
6369 below when transferring between ESInets). If the PSAP, or any other party, sends a REFER
6370 to the conference-aware UA, the conference-aware UA behaves as a normal bridge would.
6371 The call taker can add other parties to the bridge, other parties can add additional parties,
6372 parties can drop off the bridge, and the caller to bridge leg remains stable. There are
6373 options for how media is handled in this scenario. First, the initial call can be negotiated
6374 with the media flowing between the caller and the PSAP, with a media relay B2BUA in the
6375 path (in addition to the conference-aware UA) and no media mixer, or second, it can be
6376 negotiated with no media relay and a media mixer always in the path. In the second case,
6377 if a REFER is sent to the conference-aware UA when only two parties are on the call, the
6378 conference-aware UA re-INVITEs the parties, acting as a full bridge, and renegotiates the
6379 SDP to both parties to land on a media mixer. It then sends an INVITE to the transferred-to
6380 PSAP to add it to the bridge. If in the first case, the media was initially negotiated to a
6381 B2BUA acting as a media relay, the caller and transfer-from PSAP see no re-INVITE, and
6382 the conference-aware UA sends an INVITE to the transfer-to PSAP to add it to the bridge.

6383 **4.7.1.3.1 Call Established Between Caller and PSAP Via Conference-Aware UA.**

6384 This example shows the conference-aware UA handling media at the outset (second case
6385 above).

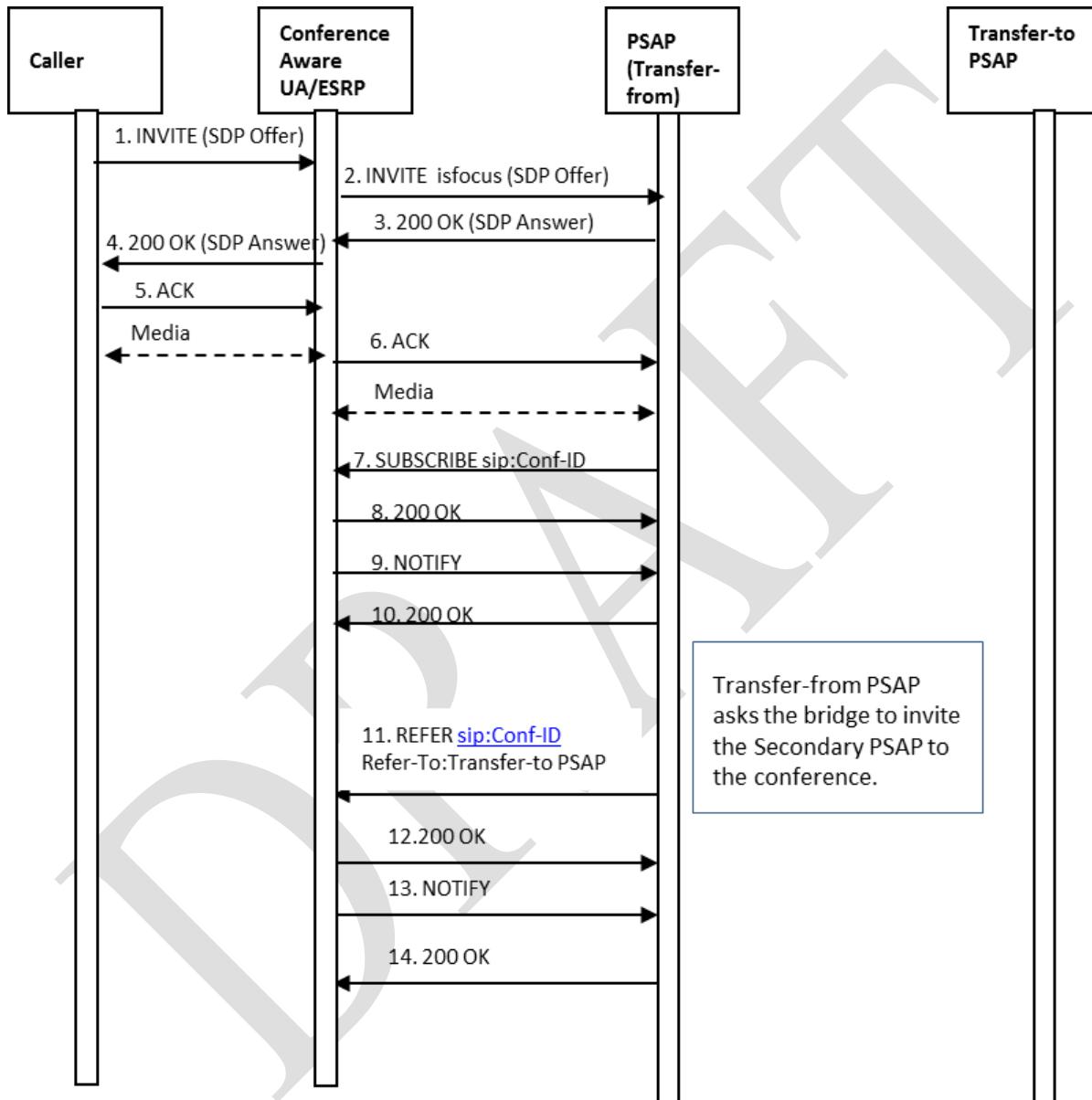


Figure 4-9 Call Established Via a Conference-aware UA

- 6386
6387 1. The caller initiates an emergency session request by sending an INVITE message to
6388 the conference-aware UA. The INVITE contains a Geolocation header field with
6389 caller location information.
6390

- 6391 2. The conference-aware UA forwards the INVITE to the ESRP (the URI in the Route
6392 header field, which should contain the "lr" parameter to avoid Request-URI
6393 rewriting) after changing the Contact header field to point to itself, adding an
6394 'isfocus' feature parameter and a ConferenceId as well as changing the offer SDP
6395 media endpoint address and port to be itself. The INVITE contains a Supported
6396 header field indicating support for Replaces. The call proceeds through the
6397 ESInet/NGCS normally and arrives at a PSAP.
- 6398 3. The PSAP responds by returning a 200 OK message to the conference-aware UA,
6399 including its Contact URL and answer SDP in the response.
- 6400 4. The conference-aware UA responds to the receipt of the 200 OK from the PSAP by
6401 sending a 200 OK message to the caller's device, changing the Contact to be itself
6402 and the answer SDP address and port to be itself, adding an 'isfocus' feature
6403 parameter and a Conference URI.
- 6404 5. The caller's device responds by sending an ACK to the conference-aware UA.
6405 *A media session is established between the caller and the conference-aware UA.*
- 6406 6. The conference-aware UA sends an ACK to the PSAP in response to receiving an
6407 ACK from the caller's device.
*A media session is established between the conference-aware UA and the PSAP. For
6409 both media legs, if SDP includes media-type specification for audio and/or video
6410 and/or RTT, then RTP media is exchanged. If SDP includes media-type specification
6411 for MSRP, then MSRP messages are exchanged.*
- 6412 7. Once the media session is established, the transfer-from PSAP sends a SUBSCRIBE
6413 message to the conference-aware UA to subscribe to the conference associated with
6414 the Conference URI identified when the conference was initially established with the
6415 conference-aware UA.
- 6416 8. The conference-aware UA responds to the SUBSCRIBE message by returning a 200
6417 OK message to the transfer-from PSAP.
- 6418 9. The conference-aware UA then returns a NOTIFY message to the transfer-from PSAP
6419 to provide it with status information regarding the conference.
- 6420 10. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6421 message.
- 6422 11. The transfer-from PSAP sends a REFER method to the conference-aware UA asking
6423 it to invite the transfer-to PSAP to the conference. The REFER method contains the
6424 Conference URI and a Refer-To header field that contains the URI of the transfer-to
6425 PSAP. The REFER method also includes an escaped Call-Info header field in the
6426 Refer-To header field containing a reference URI that points to the EIDO data
6427 structure with a purpose parameter of "emergency-eido".
- 6428 12. The conference-aware UA returns a 200 OK message to the transfer-from PSAP.

- 6429 13. The conference-aware UA then returns a NOTIFY message, indicating that
 6430 subscription state of the REFER request (i.e., active).
 6431 14. The transfer-from PSAP returns a 200 OK in response to the NOTIFY message.

6432 **4.7.1.3.2 Conference-aware UA Invites the Transfer-to PSAP to the**
 6433 **Conference**

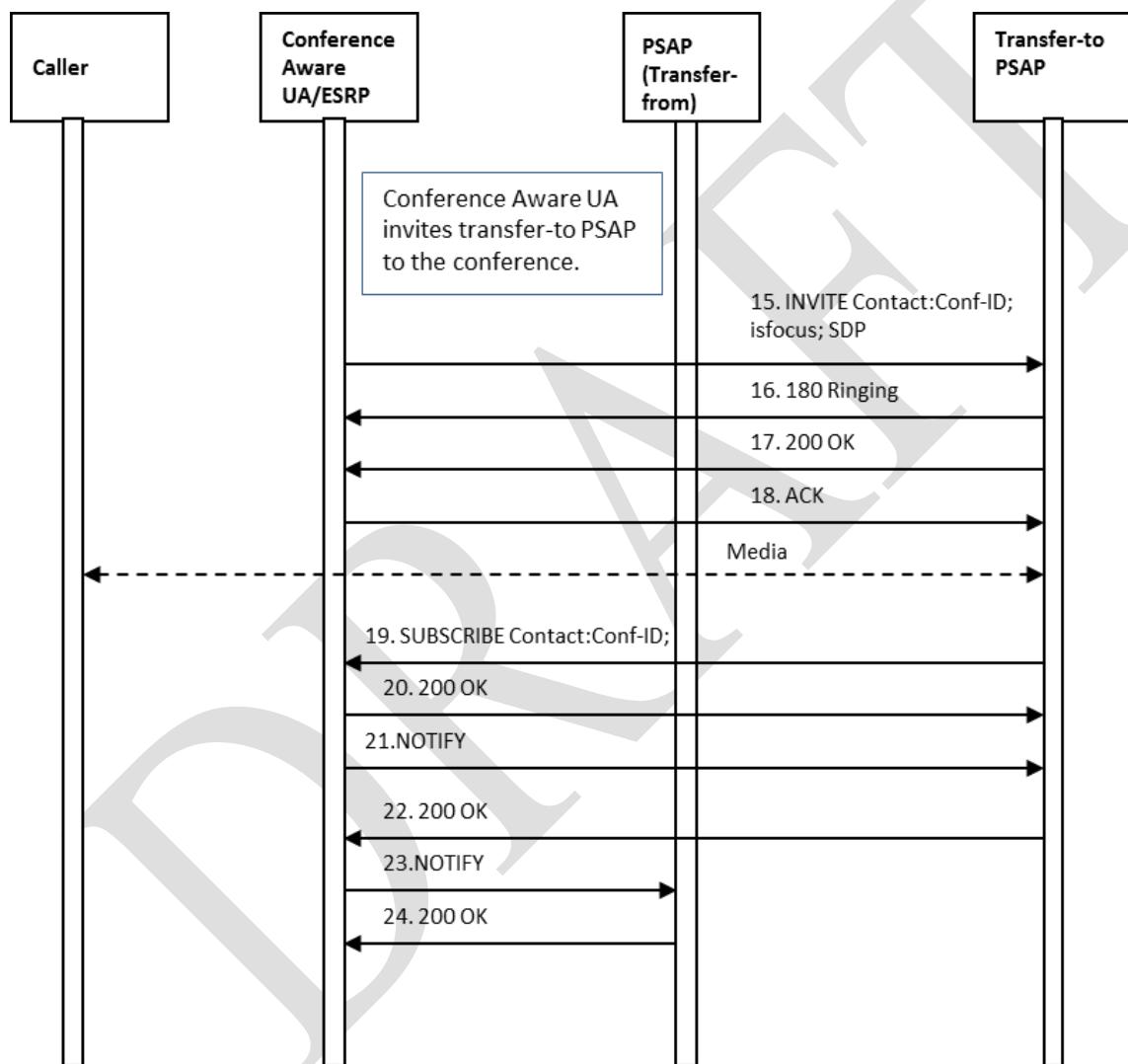


Figure 4-10 Secondary PSAP Invited to Conference

- 6435
 6436 15. The conference-aware UA invites the transfer-to PSAP to the conference by sending
 6437 an INVITE method containing the Conference URI and the 'isfocus' feature
 6438 parameter. The INVITE also contains a Call-Info header field containing a reference
 6439

- 6440 URI that points to the EIDO data structure and a purpose parameter of "emergency-
6441 eido".
6442 16. The transfer-to PSAP UA responds by returning a 180 Ringing message to the
6443 conference-aware UA.
6444 17. The transfer-to PSAP accepts the invitation by returning a 200 OK message.
6445 18. The conference-aware UA acknowledges receipt of the 200 OK message by
6446 returning an ACK.
6447 *A media session is established among the transfer-from PSAP, the transfer-to PSAP, and
6448 the caller.*
6449 19. The transfer-to PSAP subscribes to the conference associated with the Conference
6450 URI provided in the INVITE message from the conference-aware UA by sending a
6451 SUBSCRIBE message to the conference-aware UA.
6452 20. The conference-aware UA acknowledges the subscription request by sending a 200
6453 OK message back to the transfer-to PSAP.
6454 21. The conference-aware UA then returns a NOTIFY message to the transfer-to PSAP
6455 to provide subscription status information.
6456 22. The transfer-to PSAP responds by returning a 200 OK message.
6457 23. The conference-aware UA sends a NOTIFY message to the transfer-from PSAP
6458 providing updated status for the subscription associated with the REFER request.
6459 24. The transfer-from PSAP responds to the NOTIFY message by returning a 200 OK
6460 message.
6461 *At this point the caller, transfer-from PSAP, and transfer-to PSAP are all participants in
6462 the conference.*

6463 **4.7.1.3.3 Transfer-from PSAP Drops Out of Conference; Transfer-to PSAP**
6464 **Completes Transfer**

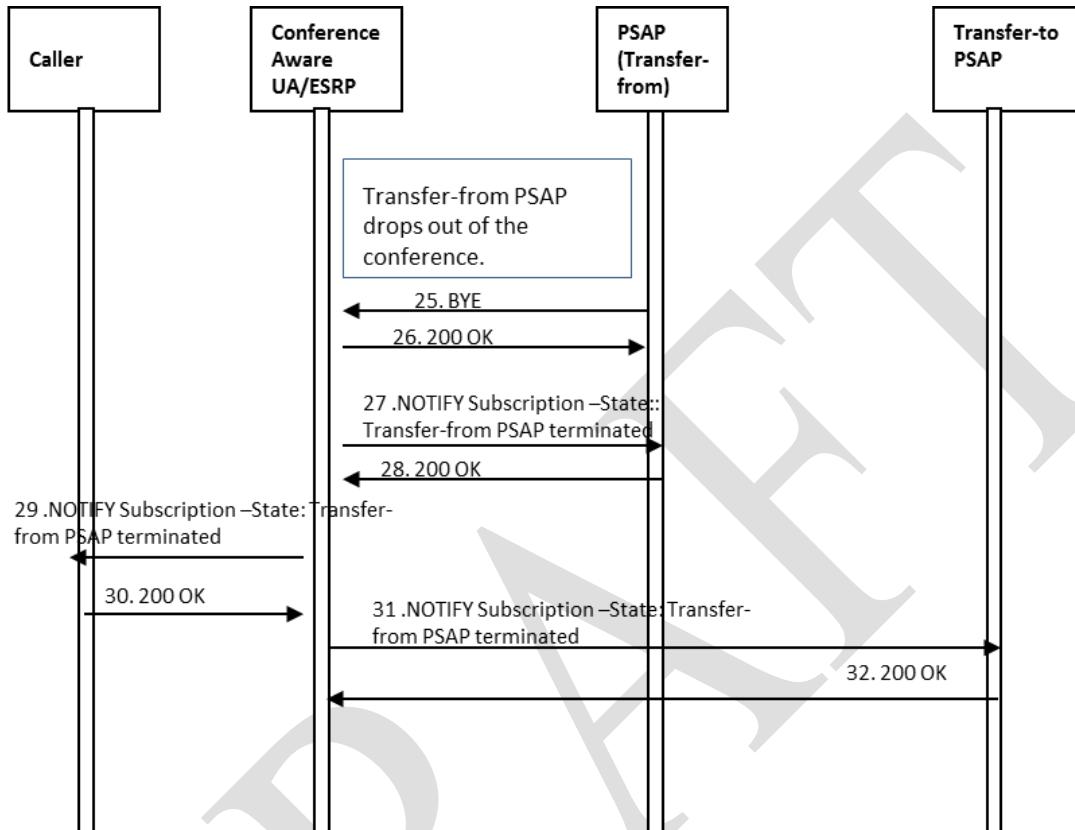


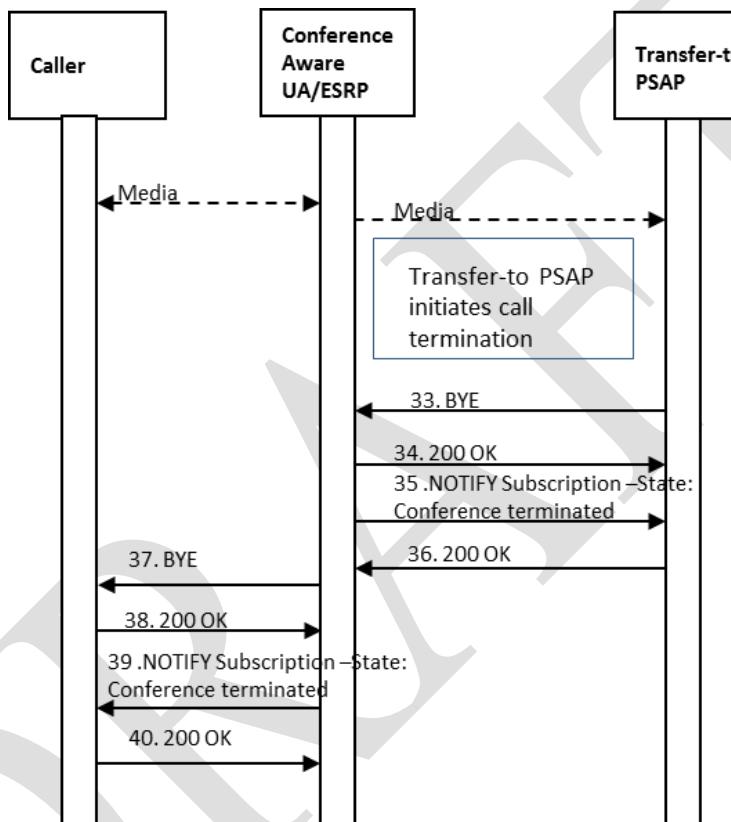
Figure 4-11 Transfer-from PSAP Drops, Transfer-to PSAP Completes Transfer

- 6465
6466 25.Upon determining that the emergency call transfer should be completed, the
6467 transfer-from PSAP disconnects from the call by sending a BYE message to the
6468 conference-aware UA.
6469
6470 26.The conference-aware UA responds by returning a 200 OK message.
6471 27.The conference-aware UA then returns a NOTIFY message to the transfer-from PSAP
6472 indicating that the subscription to the conference has been terminated.
6473 28.The transfer-from PSAP returns a 200 OK in response to the NOTIFY.
6474 29.The conference-aware UA then returns a NOTIFY message to the caller indicating
6475 that there has been a change to the subscription state. (Optional)
6476 30.The caller returns a 200 OK in response to the NOTIFY. (Optional)
6477 31.The conference-aware UA returns a NOTIFY message to the transfer-to PSAP
6478 indicating that there has been a change to the subscription state.
6479 32.The transfer-to PSAP returns a 200 OK in response to the NOTIFY.

6480 At this point, the transfer is complete. The caller and the transfer-to PSAP are involved
6481 in a two-way call via the conference-aware UA.

6482 **4.7.1.3.4 Transfer-to PSAP Terminates the Call**

6483 When the transfer-to PSAP determines that the call should be terminated, it will follow the
6484 flow illustrated below.



6485
6486 **Figure 4-12 Transfer-to PSAP Terminates Call**

- 6487 33. The transfer-to PSAP initiates call termination by sending a BYE message to the
6488 conference-aware UA.
6489 34. The conference-aware UA responds by returning a 200 OK message.
6490 35. The conference-aware UA then returns a NOTIFY message to the transfer-to PSAP
6491 indicating that the subscription to the conference has been terminated.
6492 36. The transfer-to PSAP returns a 200 OK in response to the NOTIFY.

6493 *At this point, the session between the bridge and the transfer-to PSAP is torn down.*

- 6494 37. The conference-aware UA sends a BYE message to the caller's device.

6495 38. through 40. The caller's device responds by returning a 200 OK message to the
6496 conference-aware UA.

6497 *At this point, the session between the caller and the conference-aware UA is torn down.*

6498 **4.7.2 Blind Transfers**

6499 Blind Transfer involves transferring a call without communication with the recipient. It is
6500 also known as unsupervised transfer or cold transfer. As opposed to Bridging and Attended
6501 transfer (section 4.7), the transferring PSAP Telecommunicator is not in communication
6502 with the transfer-to PSAP Telecommunicator during the transferring process. This transfer
6503 operation generally follows the sequence as shown in RFC 3515 [19].

6504 As noted in section 4.7, there are two methods of ESInet implementation. One method is
6505 termed "ad hoc" and is characterized by using a bridge only when it is needed during
6506 attended transferring or conferencing more than two parties. The other mechanism is
6507 "Route All Calls Via a Conference Aware UA". In this method, at least the signaling portion
6508 of a bridge is always in the call path. The implementation of blind transfer differs slightly
6509 between the methods. For a blind transfer in ESInets using the ad hoc method, the
6510 transferring PSAP SHALL NOT seize the bridge prior to initiating a blind transfer.

6511 The transfer-from PSAP MUST send a REFER where the Request Line contains the caller
6512 information. The Refer-To header field MUST specify the transfer-to PSAP (or any other
6513 entity): for consistency with Bridging and Attended transfer, the transfer-from PSAP
6514 SHOULD include the EIDO URI in an escaped parameter in the Refer-To header field. See
6515 the example of the associated header fields in 4.7.1 above.

6516 A REFER request implicitly establishes a subscription to the refer event as defined in RFC
6517 3515 [19], but not regarding the conference as a whole. Once the REFER is successfully
6518 acknowledged with a 200 OK, the recipient of the REFER will send notifications of the
6519 status of the adding the target participant. It MAY send a notification containing a 100
6520 Trying to indicate the transfer is pending. It MAY also send additional provisional
6521 messages, e.g. 183 Session Progress. It MUST send a 200 OK indicating that the party was
6522 successfully added. At this point the transferring PSAP MUST send a BYE to end its
6523 participation in the call. If the transferring PSAP receives an error code in the notification,
6524 e.g. 503 Service Unavailable, it MUST assume that the transfer did not occur, and MUST
6525 NOT terminate the call.

6526 **4.7.3 Premature abandonment of a transfer by the Primary PSAP**

6527 Normally an emergency call completes the entire consultative transfer operation described
6528 above. There are circumstances where, for example a 9-1-1 call turns out not to be an
6529 emergency call, in which case blind transfer as described in Section 4.7.2 is used. If for any

6530 reason a consultative transfer must be terminated early, the following procedures MUST be
6531 used.

6532 A REFER request implicitly establishes a subscription to the refer event as defined in RFC
6533 3515 [19], but not regarding the conference as a whole. Once the REFER is successfully
6534 acknowledged with a 200 OK, the recipient of the REFER will send notifications of the
6535 status of the adding the target participant. It MAY send a notification containing a 100
6536 Trying to indicate the transfer is pending. It MAY also send additional provisional
6537 messages, e.g. 183 Session Progress. It MUST send a 200 OK indicating that the party was
6538 successfully added. At this point the transferring PSAP MUST send a BYE to end its
6539 participation in the call. If the transferring PSAP receives an error code in the notification,
6540 e.g. 503 Service Unavailable, it MUST assume that the transfer did not occur and MUST not
6541 terminate the call.

6542 **4.7.4 Passing Data to Agencies via Bridging**

6543 When another PSAP is bridged to a 9-1-1 call there are separate "legs" for each participant
6544 in the bridge. The 9-1-1 call itself terminates at the bridge, with the call taker and the
6545 transfer target (e.g., transfer-to PSAP) having separate legs into the bridge. When the
6546 transfer target receives the initial SIP transaction it is an INVITE from the bridge to
6547 establish a conference. It is critical that the transfer target receives (or has access to) the
6548 location of the original caller, as well as any Additional Data that the transferring PSAP call
6549 taker may have received during the processing of the emergency call or was generated by
6550 the call taker as a result of processing the incoming emergency call. Caller location
6551 information along with any Additional Data MUST be populated in an Emergency Incident
6552 Data Object (EIDO) structure (see Section 7 for further discussion of Additional Data
6553 structures). When an emergency call is transferred, the transferring PSAP will request that
6554 the bridge insert a reference to the EIDO via an embedded Call-Info header field with a
6555 URI that points to the EIDO data structure in the REFER method sent to the bridge, and a
6556 purpose parameter of "emergency-eido". See the example of the associated header fields
6557 in 4.7.1 above. The bridge MUST subsequently include this Call-Info header field in the
6558 INVITE it sends to the transfer target.

6559 The EIDO MUST be passed by reference when the Call-Info header field contains a URL
6560 that, when dereferenced, yields the EIDO. While the EIDO normally could be passed by
6561 value (in which case the Call-Info header field in an INVITE would contain a Content
6562 Identifier URI and the body of the INVITE would contain the EIDO in a MIME type of
6563 Application/EmergencyCallData.eido+json), such a construct could not be invoked at the
6564 bridge by an embedded header field in the Refer-To from the transferring PSAP. To
6565 dereference the URI and obtain the EIDO, the recipient initiates an HTTPS: GET on the URI
6566 and the EIDO [111] is returned. The GET request MUST contain an 'Accept:' header field

6567 which specifies the MIME type assigned to EIDO (application/emergency.eido+json) and
6568 MUST include as a parameter a comma-delimited list of the major version(s) of the schema
6569 the client supports (for example 'Accept:
6570 application/emergency.eido+json;version="1,2,3"'). If the server can fulfil the request, the
6571 response MUST include one and only one EIDO instance in the body of the reply. The
6572 version of the EIDO instance must be the highest mutually compatible major version. The
6573 server SHOULD send the highest minor version it supports of that major version. The client
6574 MUST expect to receive an object derived from any minor version of the specified EIDO
6575 schema, including a higher minor version than it currently supports. The client MUST
6576 ignore any fields it does not understand. If the server does not support any of the major
6577 versions found in the 'Accept:' header field of the GET request, it MUST return a 406 Not
6578 Acceptable response.

6579 The EIDO contains a snapshot of the state of the Incident, as known by the sending
6580 Agency at the time it was sent.

6581 **4.7.5 Interoperability Between Transfer Models**

6582 An NGCS service provider chooses to support one of the transfer models described above.
6583 Transfers within the ESInet will consistently use that model. See Section 4.9 for inter-
6584 ESInet transfers.

6585 Note that the calling device can work with either model. With the Ad Hoc method, if the
6586 calling device supports the Replaces header field, it will receive an INVITE with Replaces as
6587 the transfer proceeds. If the Ad Hoc method is implemented and the calling device does
6588 not support the Replaces header, a B2BUA in the call path will receive an INVITE with
6589 Replaces, without any impact on the calling device. With the Route All Calls Via a
6590 Conference-aware UA model, the caller may encounter a re-INVITE with a change in media
6591 endpoints. It could notice that the initial call is answered with the conference indication
6592 (isfocus feature parameter), but it need not take any action as a result.

6593 PSAPs MUST implement both transfer models. A particular deployment would use only one
6594 model, as determined by the NGCS operator. The model choice is made by provisioning at
6595 the PSAP.

6596 **4.7.6 Conference Bridging for MSRP Text**

6597 As mentioned above (in Section 4.7), bridges in NG9-1-1 support multimedia. This includes
6598 voice and/or text and/or video. All bridges enable multi-party conferences that can be used
6599 to perform transfers. For MSRP text, this is equally true, except that the text media
6600 streams are not mixed, and kept independent. This is accomplished via the use of the
6601 Common Profile for Instant Messaging (CPIM) (RFC 3860) [176] (RFC 3862) [177]
6602 extensions to SIP. As specified in RFC 7701 [123], SIP/MSRP session + CPIM based

6603 protocols allow each individual message of an MSRP session to be sent to a group of
6604 participants or privately to a specific participant.

6605 The manner in which transfers are orchestrated is important. Transfers for voice
6606 communication can typically be divided into two approaches: Supervised /Attended or Non-
6607 supervised/Unattended. Sometimes these are also referred to as Hold/No Hold transfers.
6608 This section describes only the Supervised/Attended transfer scenario as applied to MSRP
6609 text sessions.

6610 When an MSRP text session must be transferred, a conference is set up. For text, a
6611 conference consists of forwarding messages to one or more parties. The result is a
6612 conference within the text part of the bridge that is commonly referred to as a Chat Room,
6613 where complete messages from each participant are interleaved and labeled by the
6614 participant before being sent to other participants.

6615 Because some user devices do not currently support CPIM, the NG9-1-1 conference bridge
6616 MUST emulate what a CPIM-enabled device would do to appropriately interwork (e.g.,
6617 label) text from other participants. User interface issues of how associated with the way
6618 that this appears to the conference participants are out of scope for this document.

6619 For MSRP text transfers, a text conference is initially established between the end user and
6620 the call taker using the same SIP call flows shown for voice. The CPIM protocol is then
6621 used for initiating a supervised transfer to a third participant (e.g., transfer-to PSAP). The
6622 text conference bridge supports “private” messaging for transfer coordination between the
6623 original call-taker and the transfer-to call-taker. The private messaging is kept out-of-view
6624 of the other participants. Once the transfer has been completed, new text messaging from
6625 all parties is visible within the text conference bridge based on “regular/public” CPIM
6626 enabled marking.

6627 All ESInet/NGCS CPIM-enabled endpoints MUST implement the nickname negotiation
6628 feature of RFC 7701 [123] and offer a nickname. There is no mechanism that allows a user
6629 to use that nickname to contact the PSAP outside the current conversation.

6630 SIP/MSRP session setup with CPIM is specified within the SDP of an INVITE message in the
6631 initial conference setup. All endpoints and media intermediaries within an ESInet/NGCS
6632 MUST support CPIM.

6633 The NGCS includes a conference bridge that anchors the MSRP media. We refer to this
6634 generally as a text part of the conference bridge. The text part supports a multi-party “chat
6635 room” which is invoked by a SIP REFER as part of a text transfer request modeling an ad
6636 hoc conference call flow.

6637 **Note:** An ad hoc transfer call flow involving MSRP may be provided in a future version of
6638 this document.

6639 **4.8 Media Mixing**

6640 Identification of participants uses RTCP SDES CNAME and NAME reports per Section 6.5 of
6641 RFC 3550 [11]. The RTCP SDES report SHOULD contain identification of the source
6642 represented by the CSRC identifier. This identification MUST contain the CNAME field and
6643 MAY contain the NAME field and other defined fields of the SDES report. All NG9-1-1
6644 implementations MUST supply identity information in this manner to the bridge. Callers
6645 SHOULD do so. The bridge MUST convey SDES information received from the sources of
6646 the session members. When such information is not available, the focus UA MUST compose
6647 CSRC, CNAME, and NAME information from available information from the SIP session
6648 (From and P-A-I) with the participant.

6649 All session participants observe the incoming RTP packets and make note of what source
6650 they came from in order to be able to present text in a way that identifies the source
6651 where possible.

6652 **4.8.1 Mixing of Real-time Text**

6653 Section 4.8 describes inter-PSAP conferencing capabilities involving a media mixer
6654 responsible for mixing media streams from the caller, the transferor and the transfer-to
6655 target. Mixing of audio and video is well understood. Mixing of Instant Messages is
6656 accomplished with “group chat” functions. Mixing of real-time text has, however originally
6657 been implemented without multi-party support; these implementations have been “multi-party
6658 unaware”.

6659 Receivers of true multi-party real-time text must actively identify the source of each received
6660 text block and place it appropriately for presentation. Multi-party unaware endpoints do not
6661 have that functionality. Therefore, there is a need to introduce a negotiation between mixers
6662 and endpoints for multi-party RTT capability so that mixers will send truly mixed real-time text
6663 only to endpoints who understand the mixed format. Endpoints without capability for true
6664 multi-party mixing of RTT are supported with a lower functionality providing a simulated
6665 grouped view of multi-party real-time text.

6666 Transport of real-time text is originally specified in RFC 4103 [85]. Multi-party handling for real-
6667 time text is described in draft-ietf-avtcore-multi-party-rtt-mix [219], which updates RFC 4103.
6668 The Mixer function of the Bridge MUST implement these mechanisms for both multi-party
6669 aware and multi-party unaware end devices.

6670 Negotiation of multi-party awareness SHALL be performed by mixers and endpoints at
6671 session initiation and modification. If both parties declare multi-party capability awareness,
6672 the mixer SHALL apply the mixing procedures for multi-party awareness as defined in draft-
6673 ietf-avtcore-multi-party-rtt-mix [219]. In all other cases, the mixer SHALL apply the limited

6674 functionality mixing procedures for multi-party unaware participants as defined in draft-ietf-
6675 avtcore-multi-party-rtt-mix.
6676 Using the original procedures in RFC 4103 [85] in a single stream in multi-party sessions
6677 results in text delays that would impede the real-time experience when two or more
6678 participants send text simultaneously. The multi-party extension defined in draft-ietf-
6679 avtcore-multi-party-rtt-mix [219] enables a number of participants to send text
6680 simultaneously while maintaining real-time experience for the receivers.
6681 As specified in RFC 4103 [85] and in draft-ietf-avtcore-multi-party-rtt-mix [219], RTT is
6682 typically sent with two repetitions in order to reduce the risk of losing text in the case of packet
6683 loss. This applies for both multi-party aware and multi-party unaware cases.
6684 The receiving endpoint with presentation functions, which has completed the negotiation for
6685 multi-party RTT awareness, SHALL use the source information to present text from the
6686 different sources separated in readable groups placed in an approximate relative time order.
6687 This way, new text from a number of different sources can be received and presented
6688 simultaneously or with negligible delay.
6689 The format for multi-party RTT specified in draft-ietf-avtcore-multi-party-rtt-mix [219] is
6690 suitable also for two-party calls.
6691 For the case when the multi-party awareness negotiation was unsuccessful, the mixer SHALL
6692 compose a simulated limited multi-party RTT view suitable for presentation. With this
6693 presentation, the time for source switching is depending on the actions of the users. In order
6694 to expedite source switching, a user can, for example, end its turn with a new line.
6695 Mixers SHALL be capable of handling both multi-party aware and multi-party unaware
6696 endpoints in the same multi-party session.

6697 **4.9 Inter-ESInet Transfers**

6698 Most transfers will be between PSAPs within an ESInet and will implement a consistent
6699 model. However, there will occasionally be a requirement to transfer from an Upstream
6700 ESInet, serving the Upstream (transfer-from) PSAP to a Downstream ESInet, serving the
6701 Downstream (transfer-to) PSAP and the models implemented on both sides of the transfer
6702 may not be the same. The principles that guided the requirements of this section are:

- 6703 1. Transfers between any PSAPs anywhere must be possible, and any differences in
6704 the transfer methods used by the Upstream ESInet vs. the Downstream ESInet
6705 should be transparent to the Downstream PSAP.
- 6706 2. The complexity of the inter-ESInet transfer is placed primarily on the
6707 bridge/conference-aware UA and PSAP behavior is dictated by the SIP signaling
6708 delivered by the ESInet provider.

- 6709 3. Once a transfer completes, it is desirable that resources in the Upstream ESInet no
6710 longer be engaged. This is especially true of media mixer resources. A B2BUA in the
6711 signaling path to support calling devices that do not implement the Replaces header
6712 field could be an exception.
6713 4. Whenever possible, media “tromboning⁴⁴” is to be avoided. For example, a wildly
6714 incorrectly routed call from New York that is initially answered at a PSAP in California
6715 and subsequently transferred to the correct New York PSAP should not have its
6716 media routed from New York to California and back to New York following
6717 completion of the transfer.

6718 With two models, there are four possibilities.

- 6719 • Upstream Ad Hoc Method to Downstream Ad Hoc Method
6720 • Upstream Route All Calls Via a Conference-aware UA Method to Downstream Ad Hoc
6721 Method
6722 • Upstream Ad Hoc Method to Downstream Route All Calls Via a Conference-aware UA
6723 Method
6724 • Upstream Route All Calls Via a Conference-aware UA Method to Downstream Route
6725 All Calls Via a Conference-aware UA Method

6726 **4.9.1 Upstream Ad Hoc Method to Downstream Ad Hoc Method**

6727 The Upstream Ad Hoc method to Downstream Ad Hoc method is the most straightforward:
6728 the sequence in Sections 4.7.1.1 or 4.7.1.2 will work without change. Note that a B2BUA
6729 that anchors media would have the effect of tromboning the media, which is undesirable.
6730 The PSAP in the Downstream ESInet may subscribe to the Upstream conference bridge.
6731 Note that the Upstream PSAP is provisioned with the URL of its local conference bridge and
6732 if the Downstream PSAP initiates a transfer or conference while the conference is still
6733 active, it will use the Upstream bridge. If the Upstream PSAP drops from the conference,
6734 the Downstream PSAP will receive a notification. The Downstream PSAP may then send an
6735 INVITE with Replaces to reconfigure the media to remove the Upstream conference bridge.
6736 If the Downstream PSAP initiates a conference after the Upstream conference bridge is
6737 removed (e.g., the Upstream PSAP dropped), it will use its local bridge and not the bridge
6738 involved in the initial transfer.

⁴⁴ Tromboning is where RTP media traffic originates at a certain point and follows a path out into the network and back to a destination close to where the RTP traffic originated.

6739 **4.9.2 Upstream Route All Calls Via a Conference Aware UA Method to**
6740 **Downstream Ad Hoc Method**

6741 The transfer in this case starts exactly as in Section 4.7.1.3.2. The Downstream PSAP MAY
6742 subscribe to the Upstream conference-aware UA to learn the identity of the conference
6743 participants and changes in the state of the conference. If the Upstream PSAP drops, the
6744 Downstream PSAP will receive a NOTIFY to that effect. The Downstream PSAP MAY send
6745 an INVITE with Replaces toward the caller (which it learns from the conference roster) to
6746 reconfigure the call to remove the Upstream conference-aware UA. The caller/ingress BCF
6747 in the Upstream ESInet MAY return a “not supported” because the Upstream ESInet may
6748 not be configured to remove the conference-aware UA from the conference. In this case,
6749 the Downstream PSAP continues to use the Upstream bridge to perform any subsequent
6750 bridge/attended transfer operations. That is, the Downstream PSAP completes the
6751 sequence as described in Section 4.7.1.3.3, Steps 25 to 32.

6752 If the Upstream ingress BCF is configured to support INVITE with Replaces, it will accept
6753 the INVITE with Replaces from the Downstream PSAP and send a BYE to the Upstream
6754 conference-aware UA. If the Downstream PSAP initiated a conference after the Upstream
6755 conference-aware UA is removed (e.g. the Upstream PSAP dropped), it will use its local
6756 bridge and not the bridge involved in the initial transfer. The sequence will be as described
6757 in Section 4.7.1.2.4, Steps 36 to 51.

6758 **4.9.3 Upstream Ad Hoc Method to Downstream Route All Calls Via a**
6759 **Conference-aware UA Method**

6760 The Downstream ESInets that implement Route All Calls Via a Conference-aware UA make
6761 use of a mechanism whereby the conference-aware UA in the Downstream ESInet acts as
6762 a B2BUA for all legs of a conference in the Upstream ESInet that terminate in the
6763 Downstream ESInet. This means that the Contact header which reflects the Upstream
6764 conference server, and the Conference ID, will be changed to reflect the Downstream
6765 conference-aware UA and Conference ID in the INVITE that is sent to the Downstream
6766 PSAP. The Downstream PSAP may subscribe to its local conference-aware UA, which may
6767 in turn subscribe to the Upstream conference server. If the Upstream PSAP drops, the
6768 NOTIFY will be sent by the Upstream conference server to the Downstream conference-
6769 aware UA, which will forward it to the Downstream PSAP. However, while the NOTIFY will
6770 be sent to the Downstream PSAP, there will be no attempt to reconfigure the media (i.e.,
6771 the Downstream UA will not send an INVITE with Replaces). Regardless of whether the
6772 conference is active or the Upstream PSAP has dropped, if the Downstream PSAP adds
6773 another party it will use its local Downstream conference-aware UA.

6774 At the completion of a transfer in which only the caller and the transfer-to PSAP remain in
6775 the conference, the Downstream conference-aware UA takes over the call, meaning it

6776 Replaces the connection between the caller (or a B2BUA in the path from the caller) and
6777 the transfer-from PSAP's bridge with a connection between the caller/B2BUA and itself. The
6778 B2BUA in the Upstream ESInet may need to remain in place if the calling device does not
6779 support Replaces. The downstream bridge MUST release the upstream bridge resources
6780 when no active call legs in the Upstream ESInet remain.

6781 The initial sequence is the same as that in Sections 4.7.1.1 or 4.7.1.2 depending on
6782 whether a B2BUA is in the path). The remaining sequences associated with this inter-
6783 ESInet transfer configuration are described below.

6784 **4.9.3.1 Secondary PSAP is Invited to the Conference**

- 6785 1. The transfer-from PSAP in the Upstream ESInet sends a REFER method to its
6786 conference bridge asking it to invite the transfer-to PSAP to the conference, where
6787 the transfer-to PSAP is hosted in a Downstream ESInet. The REFER method contains
6788 the Upstream Conf-ID and a Refer-To header field that contains the URI of the
6789 transfer-to PSAP. The REFER method also contains an escaped Call-Info header field
6790 containing a reference URI that points to the EIDO data structure and a purpose
6791 parameter of "emergency-eido".
- 6792 2. The Upstream conference-aware UA returns a 200 OK message to the Upstream/
6793 transfer-from PSAP.
- 6794 3. The Upstream conference-aware UA then returns a NOTIFY message, indicating that
6795 subscription state of the REFER request (i.e., active).
- 6796 4. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY
6797 message.
- 6798 5. The Upstream conference-aware UA invites the Downstream/transfer-to PSAP to the
6799 conference by sending an INVITE method with SDP containing the Upstream Conf-
6800 ID and Contact header field that contains the conference URI and the 'isfocus'
6801 feature parameter. The INVITE contains the Call-Info header field containing a
6802 reference URI that points to the EIDO data structure and a purpose parameter of
6803 "emergency-eido". The URL obtained from the ECRF or other mechanisms for the
6804 Downstream/transfer-to PSAP is chosen to route to the conference-aware UA in the
6805 Downstream ESInet.
- 6806 6. The Downstream conference-aware UA acts as a B2BUA, forwarding the INVITE to
6807 the Downstream/transfer-to PSAP after modifying the Contact to itself and
6808 substituting the Downstream Conf-Id it creates for the conference.
- 6809 7. The Downstream PSAP UA responds by returning a 180 Ringing message to the
6810 conference aware UA.
- 6811 8. The Downstream conference-aware UA forwards the 180 Ringing to the Upstream
6812 conference-aware UA after changing the Contact address to itself.

- 6813 9. The Downstream/transfer-to PSAP accepts the invitation by returning a 200 OK
6814 message to the conference-aware UA.
6815 10. The Downstream conference-aware UA forwards the 200 OK to the Upstream
6816 conference-aware UA after changing the Contact address to itself.
6817 11. The Upstream conference-aware UA acknowledges receipt of the 200 OK message
6818 by returning an ACK to the Downstream conference-aware UA.
6819 12. The Downstream conference-aware UA forwards the ACK to the
6820 Downstream/transfer-to PSAP.
- 6821 *Depending upon implementation, a media session is established among the
6822 Downstream/transfer-to PSAP, the Upstream conference-aware UA, and the
6823 Downstream conference-aware UA. Optionally, the Downstream conference-aware
6824 UA is not placed in the media path until an additional action (e.g., the
6825 Downstream/transfer-to PSAP requests to add another party) occurs. If SDP includes
6826 media-type specification for audio and/or video and/or RTT, then RTP media is
6827 exchanged. If SDP includes media-type specification for MSRP, then MSRP messages
6828 are exchanged.*
- 6829 13. The Upstream conference-aware UA returns a NOTIFY message to the
6830 Upstream/transfer-from PSAP to provide updated status of the subscription
6831 associated with the REFER request.
6832 14. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a
6833 200 OK message.
6834 15. The Downstream conference-aware UA subscribes to the Upstream conference-
6835 aware UA associated with the Conf-ID provided in the INVITE message from the
6836 conference-aware UA by sending a SUBSCRIBE message to it.
6837 16. The Upstream conference-aware UA acknowledges the subscription request by
6838 sending a 200 OK message back to the Downstream conference-aware UA.
6839 17. The Upstream conference-aware UA then returns a NOTIFY message to the
6840 Downstream conference-aware UA to provide subscription status information.
6841 18. The Downstream conference-aware UA responds by returning a 200 OK message.
6842 19. The Downstream/transfer-to PSAP subscribes to the Downstream conference-aware
6843 UA associated with the Conf-ID provided in the INVITE message from the
6844 Downstream conference-aware UA by sending a SUBSCRIBE message to the
6845 Downstream conference-aware UA.
6846 20. The Downstream conference-aware UA acknowledges the subscription request by
6847 sending a 200 OK message back to the Downstream/transfer-to PSAP.
6848 21. The Downstream conference-aware UA then returns a NOTIFY message to the
6849 Downstream/transfer-to PSAP to provide subscription status information obtained
6850 from the bridge, modified appropriately.
6851 22. The Downstream/transfer-to PSAP responds by returning a 200 OK message.

- 6852 23. The Upstream conference-aware UA sends a NOTIFY message to the
 6853 Upstream/transfer-from PSAP providing updated status for the subscription
 6854 associated with the REFER request.
 6855 24. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a
 6856 200 OK message.
 6857 *At this point the caller, Upstream/transfer-from PSAP, and Downstream/transfer-to*
 6858 *PSAP (via the Upstream and Downstream conference aware-UAs) are all participants*
 6859 *in the conference.*

6860 **4.9.3.2 Upstream PSAP Drops Out of Conference; Downstream PSAP**
 6861 **Completes Transfer**

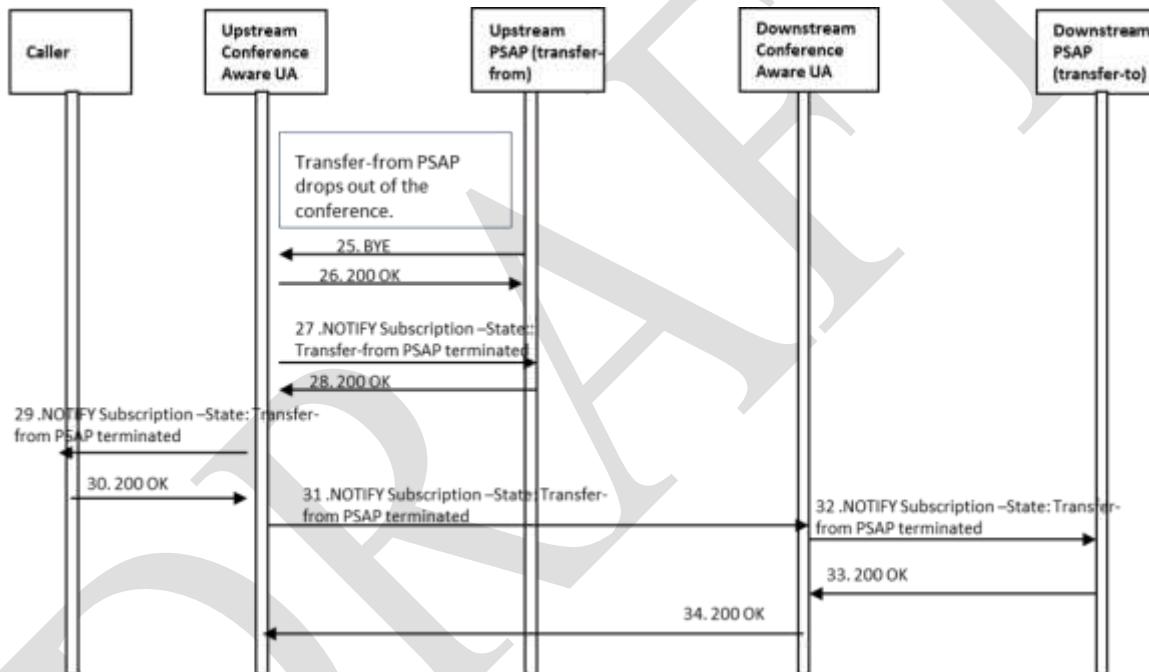


Figure 4-13 Upstream PSAP Drops, Downstream PSAP Completes Transfer

- 6862
 6863 25. Upon determining that the emergency call transfer should be completed, the
 6864 Upstream/transfer-from PSAP disconnects from the call by sending a BYE message
 6865 to the Upstream conference-aware UA.
 6866
 6867 26. The Upstream conference-aware UA responds by returning a 200 OK message.
 6868 27. The Upstream conference-aware UA then returns a NOTIFY message indicating that
 6869 the subscription to the conference has been terminated.
 6870 28. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY.
 6871 29. The Upstream conference-aware UA may send a NOTIFY message to the caller
 6872 indicating that there has been a change to the subscription state. (Optional)
 6873 30. The caller returns a 200 OK in response to the NOTIFY. (Optional)

6874 31. The Upstream conference-aware UA sends a NOTIFY message to the Downstream
6875 conference-aware UA indicating that there has been a change to the subscription
6876 state.

6877 32. The Downstream conference-aware UA sends a NOTIFY message to the
6878 Downstream/transfer-to PSAP indicating the state change.

6879 33. The Downstream/transfer-to PSAP returns a 200 OK in response to the NOTIFY,
6880 however it takes no other action (i.e., it does not send an INVITE with replaces).

6881 34. The Downstream conference-aware UA forwards the 200 OK to the Upstream
6882 conference-aware UA.

6883 *At this point, the Upstream/transfer-from PSAP has dropped and the caller and the
6884 Downstream/transfer-to PSAP are communicating via the Upstream and
6885 Downstream conference-aware UAs.*

6886 **4.9.4 Upstream Route All Calls Via a Conference Aware UA Method to 6887 Downstream Route All Calls Via a Conference Aware UA Method**

6888 The sequence for this case is very similar to the prior sequence. The Upstream and
6889 Downstream ESInets that implement Route All Calls Via a Conference Aware UA make use
6890 of a mechanism whereby the conference aware UA acts as a B2BUA for all legs of a
6891 conference in their ESInet. This means that the Upstream isfocus will be changed to the
6892 Downstream isfocus in the INVITE that is sent to the Downstream PSAP. The Downstream
6893 PSAP may subscribe to its local conference aware UA, which may in turn subscribe to the
6894 Upstream conference aware UA. If the Upstream PSAP drops, the NOTIFY will be sent by
6895 the Upstream conference aware UA to the Downstream conference aware UA, which will
6896 forward it to the Downstream PSAP. The NOTIFY will be sent to the Downstream PSAP, but
6897 there will be no attempt to reconfigure the media (i.e., the Downstream UA will not send
6898 an INVITE with Replaces). Regardless of whether the conference initiated by the Upstream
6899 PSAP is still active or in which the Upstream PSAP has dropped, if the Downstream PSAP
6900 adds another party it will use its local Downstream conference aware UA.

6901 The initial sequence is the same as that in Sections 4.7.1.3.1. The remaining sequences for
6902 this inter-ESInet transfer configuration are described below.

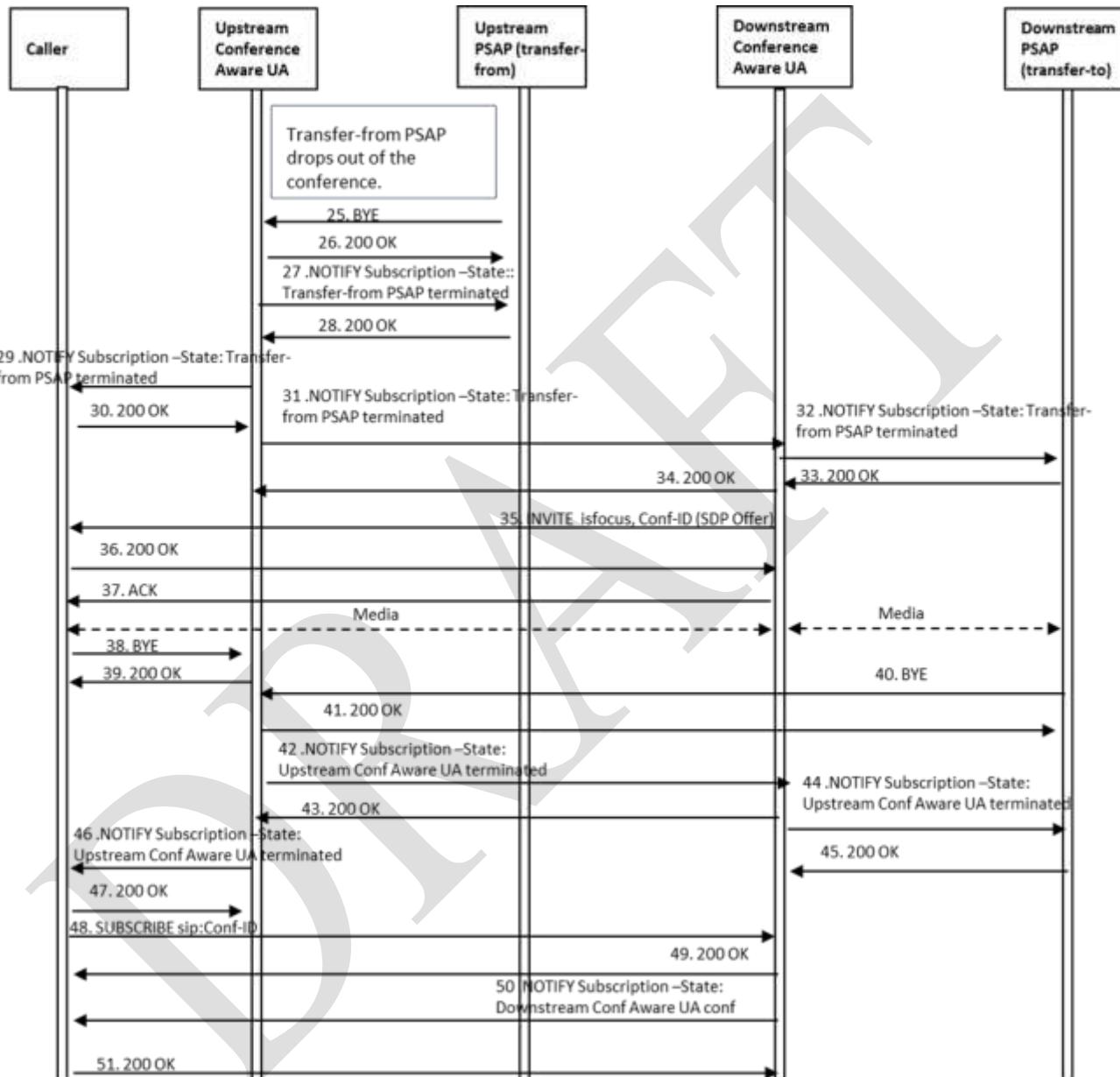
6903 **4.9.4.1 Downstream PSAP is Invited to the Conference**

- 6904 1. The Upstream/transfer-from PSAP sends a REFER method to the Upstream
6905 conference aware UA asking it to invite the Downstream/transfer-to PSAP to the
6906 conference. The REFER method contains the Conf-ID and a Refer-To header field
6907 that contains the URI of the Downstream/transfer-to PSAP. The REFER method also
6908 contains an escaped Call-Info header field containing a reference URI that points to
6909 the EIDO data structure and a purpose parameter of "emergency-eido".

- 6910 2. The Upstream conference aware UA returns a 200 OK message to the
6911 Upstream/transfer-from PSAP.
6912 3. The Upstream conference aware UA then returns a NOTIFY message, indicating that
6913 subscription state of the REFER request (i.e., active).
6914 4. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY
6915 message.
6916 5. The Upstream conference aware UA invites the Downstream/transfer-to PSAP to the
6917 conference by sending an INVITE method with SDP that includes: the Conf-ID, a
6918 Contact header field that contains the conference URI, the 'isfocus' feature
6919 parameter, and a Call-Info header field that contains a reference URI pointing to the
6920 EIDO data structure along with a purpose parameter of "emergency-eido". The URL
6921 obtained from the ECRF or other mechanisms for the Downstream/transfer-to PSAP
6922 is chosen to route to the Downstream conference aware UA in the transfer-to
6923 ESInet.
6924 6. The Downstream conference aware UA acts as a B2BUA, forwarding the INVITE to
6925 the Downstream/transfer-to PSAP after modifying the Contact to itself and
6926 substituting a Conf-Id it creates for the conference.
6927 7. The Downstream PSAP UA responds by returning a 180 Ringing message to the
6928 downstream conference aware UA.
6929 8. The Downstream conference aware UA forwards the 180 Ringing to the Upstream
6930 conference aware UA after changing the Contact address to itself.
6931 9. The Downstream/transfer-to PSAP accepts the invitation by returning a 200 OK
6932 message to the Downstream conference aware UA.
6933 10. The Downstream conference aware UA forwards the 200 OK to the Upstream
6934 conference aware UA after changing the Contact address to itself.
6935 11. The Upstream conference aware UA acknowledges receipt of the 200 OK message
6936 by returning an ACK to the Downstream conference aware UA.
6937 12. The Downstream conference aware UA forwards the ACK to the
6938 Downstream/transfer-to PSAP.
- 6939 *A media session is established between the Downstream/transfer-to PSAP and the
6940 media mixer in the primary conference aware UA. If SDP includes media-type
6941 specification for audio and/or video and/or RTT, then RTP media is exchanged. If
6942 SDP includes media-type specification for MSRP, then MSRP messages are
6943 exchanged.*
- 6944 13. The Upstream conference aware UA returns a NOTIFY message to the
6945 Upstream/transfer-from PSAP to provide updated status of the subscription
6946 associated with the REFER request.
6947 14. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a
6948 200 OK message.

- 6949 15. The Downstream conference aware UA subscribes to the conference associated with
6950 the Conf-ID provided in the INVITE message from the Upstream conference aware
6951 UA by sending a SUBSCRIBE message to the Upstream conference aware UA. Note
6952 that the Downstream conference aware UA always subscribes to the event package
6953 even if the Downstream/transfer-to PSAP does not subscribe.
6954 16. The Upstream conference aware UA acknowledges the subscription request by
6955 sending a 200 OK message back to the Downstream conference aware UA.
6956 17. The Upstream conference aware UA then returns a NOTIFY message to the
6957 Downstream conference aware UA to provide subscription status information.
6958 18. The Downstream conference aware UA responds by returning a 200 OK message.
6959 19. The Downstream/transfer-to PSAP subscribes to the conference associated with the
6960 Conf-ID provided in the INVITE message from the Downstream conference aware
6961 UA by sending a SUBSCRIBE message to the Downstream conference aware UA.
6962 20. The Downstream conference aware UA acknowledges the subscription request by
6963 sending a 200 OK message back to the Downstream/transfer-to PSAP.
6964 21. The Downstream conference aware UA then returns a NOTIFY message to the
6965 Downstream/transfer-to PSAP to provide subscription status information obtained
6966 from the Upstream conference aware UA, modified appropriately.
6967 22. The Downstream/transfer-to PSAP responds by returning a 200 OK message.
6968 23. The Upstream conference aware UA sends a NOTIFY message to the
6969 Upstream/transfer-from PSAP providing updated status for the subscription
6970 associated with the REFER request.
6971 24. The Upstream/transfer-from PSAP responds to the NOTIFY message by returning a
6972 200 OK message.
- 6973 *At this point the caller, Upstream/transfer-from PSAP, and Downstream/transfer-to
6974 PSAP (via the conference aware UA) are all participants in the conference.*

6975 **4.9.4.2 Upstream PSAP Drops Out of Conference; Downstream PSAP Completes Transfer**
6976



6977
6978
6979
6980
6981

Figure 4-14 Primary PSAP Drops, Secondary Completes Transfer

- 25.Upon determining that the emergency call transfer should be completed, the Upstream/transfer-from PSAP disconnects from the call by sending a BYE message to the Upstream conference aware UA.

- 6982 26. The Upstream conference aware UA responds by returning a 200 OK message.
6983 27. The Upstream conference aware UA then returns a NOTIFY message indicating that
6984 the subscription to the conference has been terminated.
6985 28. The Upstream/transfer-from PSAP returns a 200 OK in response to the NOTIFY.
6986 29. The Upstream conference aware UA then returns a NOTIFY message to the caller
6987 indicating that there has been a change to the subscription state. (Optional)
6988 30. The caller returns a 200 OK in response to the NOTIFY. (Optional)
6989 31. The Upstream conference aware UA sends a NOTIFY message to the Downstream
6990 conference aware UA indicating that there has been a change to the subscription
6991 state.
6992 32. The Downstream conference aware UA sends a NOTIFY message to the
6993 Downstream/transfer-to PSAP indicating the state change, however the PSAP takes
6994 no further action (e.g., doesn't send an INVITE with replaces).
6995 33. The Downstream/transfer-to PSAP returns a 200 OK in response to the NOTIFY.
6996 34. The Downstream conference aware UA forwards the 200 OK to the Upstream
6997 conference aware UA.
6998 35. Upon recognizing that the caller and the Downstream/transfer-to PSAP (via the
6999 Downstream conference aware UA) are the only remaining participants in the
7000 conference, the Downstream conference aware UA completes the transfer by
7001 sending an INVITE with Replaces, SDP, an iffocus feature parameter, and the
7002 conference aware UA's Conf-ID to the caller/B2BUA requesting that they replace
7003 their connection to the bridge with a connection to the Downstream conference
7004 aware UA. The Downstream conference aware UA learns the URI of the caller
7005 through the entity attribute in the endpoint section of the user's container in the
7006 conference NOTIFY from the Upstream conference aware UA.
7007 36. The caller responds by returning a 200 OK message to the Downstream conference
7008 aware UA.
7009 37. The Downstream conference aware UA returns an ACK in response to the 200 OK.
7010 *A media session is established between the Downstream/transfer-to PSAP and the caller
7011 using the Downstream conference aware UA's media mixer. If SDP includes media-
7012 type specification for audio and/or video and/or RTT, then RTP media is exchanged.
7013 If SDP includes media-type specification for MSRP, then MSRP messages are
7014 exchanged.*
7015 38. The caller then sends a BYE to the Upstream conference aware UA to terminate the
7016 session.
7017 39. The Upstream conference aware UA responds by sending the caller a 200 OK
7018 message.

- 7019 40. The Downstream conference aware UA also terminates its session with the
7020 Upstream conference aware UA by sending a BYE message to the Upstream
7021 conference aware UA.
7022 41. The Upstream conference aware UA responds by sending a 200 OK message to the
7023 Downstream conference aware UA.
7024 42. The Upstream conference aware UA then returns a NOTIFY message to the
7025 Downstream conference aware UA indicating that the subscription to the conference
7026 has been terminated.
7027 43. The Downstream conference aware UA returns a 200 OK in response to the NOTIFY
7028 message.
7029 44. The Downstream conference aware UA then returns a NOTIFY message to the
7030 Downstream/transfer-to PSAP indicating that the conference state has changed.
7031 45. The Downstream conference aware UA returns a 200 OK in response to the NOTIFY
7032 message.
7033 46. The Upstream conference aware UA sends a NOTIFY message to the caller
7034 indicating that the subscription to its conference has been terminated. (Optional)
7035 47. The caller responds with a 200 OK message. (Optional)
7036 48. The caller subscribes to the conference associated with the Conf-ID provided in the
7037 INVITE message from the Downstream conference aware UA by sending a
7038 SUBSCRIBE message to the Downstream conference aware UA. (Optional)
7039 49. The Downstream conference aware UA acknowledges the subscription request by
7040 sending a 200 OK message back to the caller. (Optional)
7041 50. The Downstream conference aware UA then returns a NOTIFY message to the caller
7042 to provide subscription status information. (Optional)
7043 51. The Downstream/transfer-to PSAP responds by returning a 200 OK message.
7044 (Optional)
- 7045 *At this point, the Upstream/transfer-from PSAP has dropped and the caller and the
7046 Downstream/transfer-to PSAP are communicating via the Downstream conference
7047 aware UA.*
- 7048 The Downstream/transfer-to PSAP can terminate the call using the sequence in Section
7049 4.7.1.3.4. If the Upstream ESInet (with Route All Calls Via a Conference Aware UA)
7050 employed a B2BUA, the B2BUA would replace the caller in the above sequence. Note as
7051 before if the B2BUA anchored media, a possible tromboning of the media path could occur.
- 7052 Note that if, at some point, the transfer-from PSAP adds another transfer-to PSAP in the
7053 same Downstream ESInet to the call prior to the transfer-from PSAP dropping out of the
7054 call, it would transit the Downstream conference aware UA, and the Downstream
7055 conference aware UA would act as a B2BUA to that leg also (not illustrated).

7056 **4.10 Location Information Server (LIS)**

7057 A Location Information Server supplies location in the form of a PIDF-LO (location by
7058 value) or a location URI (location by reference). The LIS also provides a “dereference”
7059 service for a location URI it supplies: given the URI, the LIS provides the location value as
7060 a PIDF-LO. A LIS MAY be a database, or MAY be a protocol interworking function to an
7061 access network-specific protocol.

7062 In NG9-1-1, the LIS supplies location (by value or reference) to the endpoint, or to a proxy
7063 operating on behalf of the endpoint. The ESInet is not directly involved in that transaction:
7064 the resulting PIDF-LO or location URI must appear in the initial SIP message in a
7065 Geolocation header field. If the LIS supplies location by reference, it MUST also provide
7066 dereferencing service for that location URI. Elements in the ESInet, including the ESRP,
7067 and the PSAP may dereference a location URI as part of processing a call.

7068 If the LIS supplies location by reference, it MUST support HELD (RFC 5985) [7], HELD
7069 Dereferencing (RFC 6753) [55], and/or SIP Presence Event Package (RFC 3856) [25]. The
7070 SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing,
7071 especially when tracking of the caller is needed. However, HELD is acceptable on any
7072 location URI. LISs supporting SIP MUST support location filters (RFC 6447) [72] and event
7073 rate control (RFC 6446) [80].

7074 If the broadband access network supports true mobility, it SHOULD supply location by
7075 reference. If the broadband network is a fixed network like a cable modem network or
7076 DSL, location by value is preferred, but location by reference is acceptable.

7077 The LIS MAY support SIP Presence to provide location-by-reference as defined by RFC
7078 5808 [54]. Using SIP Presence, the entity desiring location subscribes to the SIP Presence
7079 Event Package (RFC 3856 [25]) at the location URI provided⁴⁵. The LIS sends NOTIFY
7080 transactions (RFC 6665 [14]) containing a PIDF document that will include the location in
7081 the Location Object (LO) part, forming the PIDF-LO. An immediate NOTIFY will be
7082 generated by the LIS upon acceptance of a subscription request. This would represent the
7083 current location of the target. The SUBSCRIBE includes an Expires header field (RFC 3261)
7084 [10] which represents the subscribers requested expiration, and the 2XX response contains
7085 one that represents the server’s actual expiration (which may be shorter, but not longer,
7086 than the subscriber’s requested time). An Expires of zero indicates a request for exactly

45 The entity providing a SIP Presence-based location URI should always provide a sips: URI and not a sip: URI, although calls must not fail if credentials are not available. pres: URIs must never be used for this application.

7087 one NOTIFY (that is the current location) with no further updates. Subscriptions expire
7088 when the call terminates if the LIS is call-aware.

7089 The querier can limit how often further NOTIFYs are sent (before expiration of the
7090 subscription) using a filter (RFC 4661 [92]). Rate limits (RFC 6446 [80]) and Location filters
7091 (RFC 6447 [72]) are useful for this application and must be supported by the LIS if it
7092 supplies a SIP location URI⁴⁶.

7093 A LIS MUST validate locations prior to entering them into the LIS using the LVF (see
7094 Section 4.3).

7095 A LIS MAY support the validation of location around planned changes as defined by draft-
7096 ecrit-lost-planned-changes [178].

7097 A LIS MUST accept credentials traceable to the PCA for authenticating queries for a
7098 location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely
7099 on any other credential source to authorize location dereferencing.

7100 When location is provided by reference there is a need for the reference to be valid at least
7101 for the length of the call. Since the call may be transferred to a transfer-to PSAP for
7102 handling, the transfer-to PSAP must have the ability to dereference the location reference
7103 provided with the call. It is therefore critical that the location URI not expire before the
7104 transfer-to PSAP has the opportunity to dereference it. RFC 6753 [55] suggests that there
7105 SHOULD be an expiration time associated with location URIs, and RFC 5985 [7] provides
7106 that it SHOULD be set at a minimum of 30 minutes, with a maximum of 24 hours. To be
7107 consistent with these recommendations, any LIS that provides a dereferencing service for a
7108 location URI MUST provide an expiration time associated with that URI set at a minimum of
7109 30 minutes, with a maximum of 24 hours.

7110 Providing location beyond the length of the call raises privacy concerns. Sometimes, users
7111 can control access to their location by means of a privacy policy that they can specify.
7112 During an emergency call, there is no universal expectation of privacy of location. When
7113 the call completes, privacy should be restored. Some LISes do not have an explicit privacy
7114 policy but consider access to user's location on a case-by-case basis, often with commercial
7115 implications.

7116 While there are some circumstances in which it is desirable that location be made available
7117 to 9-1-1 after a call completes, it cannot be required without a change in law. Therefore, it

⁴⁶ If an entity receives a SIP URI for location by reference and specifies an expiration time greater than zero, it will usually get more than one NOTIFY. If it specifies a filter, then the filter determines when and how often the NOTIFYs are generated. If no filter is specified, the entity will determine how often to send NOTIFYs using an algorithm of its choice.

7118 is not required that a LIS honor any request from NG9-1-1 entities following completion of
7119 a call. LIS operators who do not give their users control of privacy should consider
7120 balancing privacy needs with the occasional requirement of NG9-1-1 entities to get a
7121 location update. The NG9-1-1 authentication processes provide mechanisms to determine
7122 the role of the agent making a request, and restricting access after a call to supervisory
7123 personnel could be considered. NG9-1-1 entities cannot assume location will be available
7124 after a call.

7125 **4.11 Additional Data Repository (ADR)**

7126 An Additional Data Repository is a source of Additional Data. URIs pointing to the ADR may
7127 be passed in a call, in an EIDO, or by other mechanisms. Each URI could point to a
7128 different ADR. In response to an HTTPS GET of the URI, the ADR returns the
7129 referenced Additional Data block.

7130 An emergency call MUST have at least two⁴⁷ Call-Info header fields, each with a URI that
7131 resolves to an Additional Data structure (RFC 7852) [107] (the required block types are
7132 EmergencyCallData.ProviderInfo and EmergencyCallData.ServiceInfo). Each URI may be a
7133 Content Identifier (CID) that references an Additional Data block in the in the body of an
7134 INVITE or MESSAGE, or an HTTPS URI to an external source. Additionally, the <provided-
7135 by> element of a PIDF-LO may contain an Additional Data URI or an Additional Data block.
7136 The external database that dereferences external Additional Data URIs is an Additional
7137 Data Repository (ADR). There is a minimum amount of information listed as Mandatory for
7138 EmergencyCallData.ProviderInfo and EmergencyCallData.ServiceInfo that, when combined
7139 with information from the PIDF-LO and the SIP INVITE or MESSAGE, is minimally
7140 equivalent to the information currently provided by all originating networks in the ALI.

7141 All originating networks and service providers⁴⁸ are expected to provide at least this
7142 minimum set of information either by reference or value. Access networks are expected to
7143 provide the same minimum set of information. Each Call-Info header field with a purpose
7144 parameter value starting with "EmergencyCallData", a dot, and a block name references an
7145 Additional Data block (either by value or by reference). It is important that ALL originating
7146 networks and service providers handling the call add Call-Info header fields when they can
7147 be reasonably expected to determine they are handling an emergency call. It is also
7148 important that ALL entities that provide a PIDF-LO when they can be reasonably expected

⁴⁷ Wireline and other legacy networks that historically provide subscriber information are expected to continue to do so using the SubscriberInfo block of Additional Data.

⁴⁸ In the context of Additional Data, the term "service provider" refers to a 3rd party, in the path of an emergency call or not, and which is not the originating network presenting the call to the ESInet.

7149 to determine it is for an emergency call include a <provided-by> element in the PIDF-LO to
7150 indicate the source of the PIDF-LO. The transaction to dereference the Additional Data URI
7151 MUST be protected with TLS. The dereferencing entity, which may be an ESRP, LPG, PSAP,
7152 or responding agency, uses its credentials (traceable to the PCA for NG9-1-1 entities) to
7153 dereference the Additional Data URI. The originating network or service provider can use
7154 any credential, as long as the domain listed in the URI is the domain of the SubjectAltName
7155 in the credential.

7156 ADRs can host sensitive data for which the disclosure may be subject to legal, regulatory,
7157 privacy and confidentiality requirements, and/or local policy. Such requirements may
7158 supersede the stated requirements herein. All ADR queries originating within an ESInet
7159 MUST include authentication by credentials traceable to the PCA. An ADR MAY serve less-
7160 sensitive data in the event PCA-traceable authentication fails. All ADRs MUST serve data for
7161 any valid query. A call-stateful ADR MAY limit the length of time that it will serve data after
7162 the end of the associated emergency call. Such a time limit SHOULD be at least five
7163 minutes. ADRs may not have the data themselves, but may know where the data can be
7164 found. The response to a dereference request can be redirected to another ADR with an
7165 HTTPS 333 response (Iterative Refer).

7166 Devices such as those within telematics-equipped vehicles and medical monitoring devices
7167 that can place emergency calls may provide Additional Data blocks by value or by reference
7168 within the INVITE or MESSAGE. When provided by reference, devices could have the
7169 capability to respond to an ADR query themselves or could publish data to an external
7170 ADR. A service provider (such as a telematics service provider) could provide the ADR
7171 instead of the device. Other devices could also provide an ADR for use in an emergency
7172 call. There may be multiple Additional Data blocks, each of which may be provided by
7173 reference or by value by the device, originating network, or service provider. (See Section
7174 3.1.19 for more information about telematics calls and datasets.)

7175 Additional Data blocks may be provided by reference or by value by the access network,
7176 originating network, or service provider. When service providers, access and originating
7177 networks only provide the minimal data called for in RFC 7852 [107], the ADR could be
7178 provided by a third party. For Additional Data provided by the calling entity itself, the data
7179 could be conveyed by value within the INVITE or MESSAGE, or by reference via an ADR
7180 that could be provided by the calling entity or a third party.

7181 Interaction with the ADR MUST be protected by TLS. The ADR MUST accept certificates
7182 traceable to the PCA. ESInet entities may only accept certificates for the ADR signed by a
7183 CA recognized by common web browsers.

7184 A class of ADRs provides an additional capability to be searched by an identity. See Section
7185 4.11.1 for specifications for this capability.

[MM/DD/YYYY]

Page 253 of 675



7186 **4.11.1 Identity Searchable Additional Data Repository (IS-ADR)**

7187 Some Additional Data Repositories have an optional feature that allows the repository to be
7188 searched by identity. This capability is needed when data is stored by an entity that is not
7189 in the path of the call or access network. For example, personal medical data provided by
7190 the caller may be stored by an entity trusted by the caller to keep such data. The caller
7191 provides the identity it uses on calls, and the IS-ADR is searched. An IS-ADR is an ADR and
7192 MUST conform to Section 4.11.

7193 The IS-ADR provides a web service. When queried with a caller's From address or P-
7194 Asserted-Identity (as retrieved from the SIP header field)⁴⁹, the IS-ADR returns one of the
7195 following in response:

- The caller's Additional Data (by value);
- A URI that can be used to dereference the caller's Additional Data;
- An HTTP 307 Temporary Redirect instructing the client to direct an Additional Data query to the resource specified in the response;
- An indication that no data was found for the provided From or P-A-I URI.

7201 The OpenAPI definition of this web service may be found in Appendix E.2.

7202 **IdentitySearchRequest**

7203 HTTP method: GET

7204 Resource name .../AdditionalData

7205 Request Parameters:

Name	Condition	Description
CallerURI	MANDATORY	URI of caller From/P-A-I

7206 A successful query returns an Additional Data Value in a string

7207 Status Codes

7208	200	OK
7209	307	Temporary Redirect
7210	404	Not Found
7211	454	Unspecified Error

⁴⁹ The "From" SIP header field may be used if the P-Asserted-Identity field (P-A-I) is not present, as P-A-I may not be retained on SIP calls which cross untrusted domains.

7212 It is anticipated that a number of third parties will choose to host an IS-ADR. A registry of
7213 recognized IS-ADRs is defined. PSAPs and other responsible parties can then use the IANA
7214 IS-ADR registry as input into the configuration of the NG9-1-1 functional elements under
7215 their control.

7216 **Note:** A privacy issue was identified associated with this mechanism. Since it will require
7217 substantive changes, this will be addressed in a future version of this document.

7218 **4.12 Logging Service**

7219 The Logging Service in NG9-1-1 is a standardized functional element used by all elements
7220 in an ESInet to log all significant events; logging is not restricted to events within a PSAP.
7221 All significant steps in processing a call are logged. NG9-1-1 defines an external Logging
7222 Service interface so that the logging function can be provided in the ESInet (i.e., external
7223 to a PSAP). Logging includes external events, internal events, media, and messages. All
7224 forms of media described in this document MUST be logged (see the Media section for
7225 details). Media recording SHOULD begin at the earliest point possible, which can be before
7226 the call has been answered if early media are available; recording media both at or near
7227 ESInet ingress and within a PSAP is desirable. The Logging Service is sometimes referred
7228 to as simply "the Logging Service" in this document. Each agency can have its own Logging
7229 Service, or Logging Services can be shared. Since incidents may involve multiple agencies,
7230 obtaining logging records from multiple Logging Services may be required. The Agency
7231 Locator record includes the URI to the Logging Service for a particular agency.

7232 The Versions entry point of the Logging Web Service MUST include, in the "serviceInfo"
7233 parameter, the parameter "requiredAlgorithms" whose value is an array of JWS algorithms
7234 (as described in 5.10) acceptable to the Logging Service. The following example is from a
7235 Logging Service whose currently in force policy permits unsigned LogEvents as well as
7236 signed LogEvents using the "EdDSA" algorithm:

```
7237 {  
7238     "fingerprint": "Woof-FurrySuite-v8-8c439e",  
7239     "versions":  
7240         [  
7241             { "major": 6, "minor": 3,  
7242                 "vendor": "burby-magic",  
7243                 "serviceInfo": { "requiredAlgorithms": [ "EdDSA", "none" ] }  
7244             }  
7245         ]  
7246     }  
7247 }
```

7248 **4.12.1 Logging Introduction**

7249 The Logging Service incorporates a web service that supports logging and retrieving
7250 events. In addition to the web service interface, Logging Services MUST implement a
7251 Session Recording Protocol (SIPREC - RFC 7866) interface [116] for recording the media
7252 and, if provided, the associated metadata. Logging Services MUST provide a Real-time
7253 Streaming Protocol (RTSP) interface compliant with RTSP 2.0 (RFC 7826 [98]) to play back
7254 the media. RTSP 1.0 MUST NOT be used. The web service includes the functions described
7255 in the LogEvent section.

7256 Clients to the Logging Service MUST support logging to at least two Logging Services for
7257 redundancy purposes, with support for three (3) or more RECOMMENDED, and some
7258 jurisdictions might require four or more. The Logging Service is NOT intended to support
7259 other kinds of devices that may wish to operate from the LogEvent records. See
7260 LogEventReplicator, Section 4.12.3.9.

7261 Each Logging Service FE MUST implement the server-side of the ElementState event
7262 notification package. The Logging Service FE MUST promptly report changes in its state to
7263 its subscribed elements.

7264 The set of Logging Service FEs within an NGCS MUST implement the server-side of the
7265 ServiceState event notification package for the Logging Service. ESInets can be built with
7266 Logging Services either local or centralized, and less commonly a mix of both local and
7267 state level Logging Services. Accordingly, it is recommended that each NGCS that provides
7268 a Logging service implement ServiceState for that NGCS.

7269 **4.12.2 Media Recording Interface**

7270 The Logging Service acts as a Session Recording Server (SRS), and accepts media and
7271 metadata from a Session Recording Client (SRC) as defined in the Session Recording
7272 Protocol (RFC 7866) [116]. The Logging Service MUST implement the SRS interface. Any
7273 element that has RTP-transported call media, including MSRP, MAY deploy the SRC
7274 interface and at least one element in the call path MUST deploy the SRC interface. All
7275 Bridge elements (Section 5.7), Gateway elements (Section 7), BCF elements that anchor
7276 media, and PSAP Call Handling elements, MUST implement the SRC interface. Overall
7277 ESInet design determines which elements may be provisioned to record. Such designs
7278 MUST assure that media are always recorded, even when calls are handled out-of-area,
7279 which may make different assumptions than the local ESInet on such matters. Elements
7280 that implement the SRC interface MUST be capable of supporting redundant
7281 implementations of the SRS (RFC 7866) [116] and MUST insert the Call Identifier and
7282 Incident Tracking Identifier (Call-Info header fields) defined in this document into the
7283 INVITE sent to the Logging Service.

- 7284 The logging recorder that supports the Session Recording Server (SRS) functionality
7285 defined in the SIPREC specification (RFC 7866) [116] interfaces to any Functional Elements
7286 that support a Session Recording Client (SRC).
- 7287 The Logging Service and its SRC interface MUST log the SIPREC Metadata LogEvent (see
7288 the LogEvent section for details). An SRC MAY support sending SIPREC Metadata (RFC
7289 7865) [117]. When an SRC sends SIPREC Metadata, it MUST generate a SiprecMetadata
7290 LogEvent to the Logging Service. The SRC MUST include the CallId and IncidentId for the
7291 emergency call being recorded in the SIPREC INVITE it generates and when generating an
7292 associated SiprecMetadata LogEvent.
- 7293 Each emergency call (that is, each Communication Session), MUST result in a separate
7294 Recording Session. More than one Recording Session MAY be logged for a single call.
- 7295 All SRCs and SRSes MUST implement RTCP on the recording session. The SRC MUST send
7296 wall clock time in sender reports, which MUST be recorded by the SRS. This allows media
7297 synchronization of multiple media streams on playback.
- 7298 SRCs MUST support recording of media to at least two SRSes.
- 7299 The flow diagrams are informative and do not attempt to show every case.
- 7300 The following events have been omitted for clarity:
- 7301 • The OK on the BYE
7302 • Provisional messages
7303 • ACKs
- 7304 In the below example, "Answering Point" is an element inside a PSAP and may not have a
7305 standardized interface. "Ring", "Answer", and "Dial" are used as the names of the
7306 messages, as the Answering Point protocol is out of scope.
- 7307 RS = Recording Session as defined in SIPREC.
- 7308 CS= Communication Session as defined in SIPREC.
- 7309 The call MUST go on even if there is no recorder.
- 7310 **4.12.2.1 Incoming Call**
- 7311 The SRC opens a recording session with the logging recorder. The call between the Caller
7312 and Answer-Point is recorded for its duration. The call flow for this scenario is:
- 7313 • Call hits the SRC
7314 • SRC opens a recording session with the recorder, including the call identifier
7315 • Call is answered
7316 • Call stream is added to the recording session

- 7317 • Both parties communicate
7318 • Caller hangs up
7319 • Answer-Point hangs up
7320 • SRC closes the recording session.

7321 **Note:** All additional information about the call can be retrieved from the Logging Service
7322 using the call identifier.

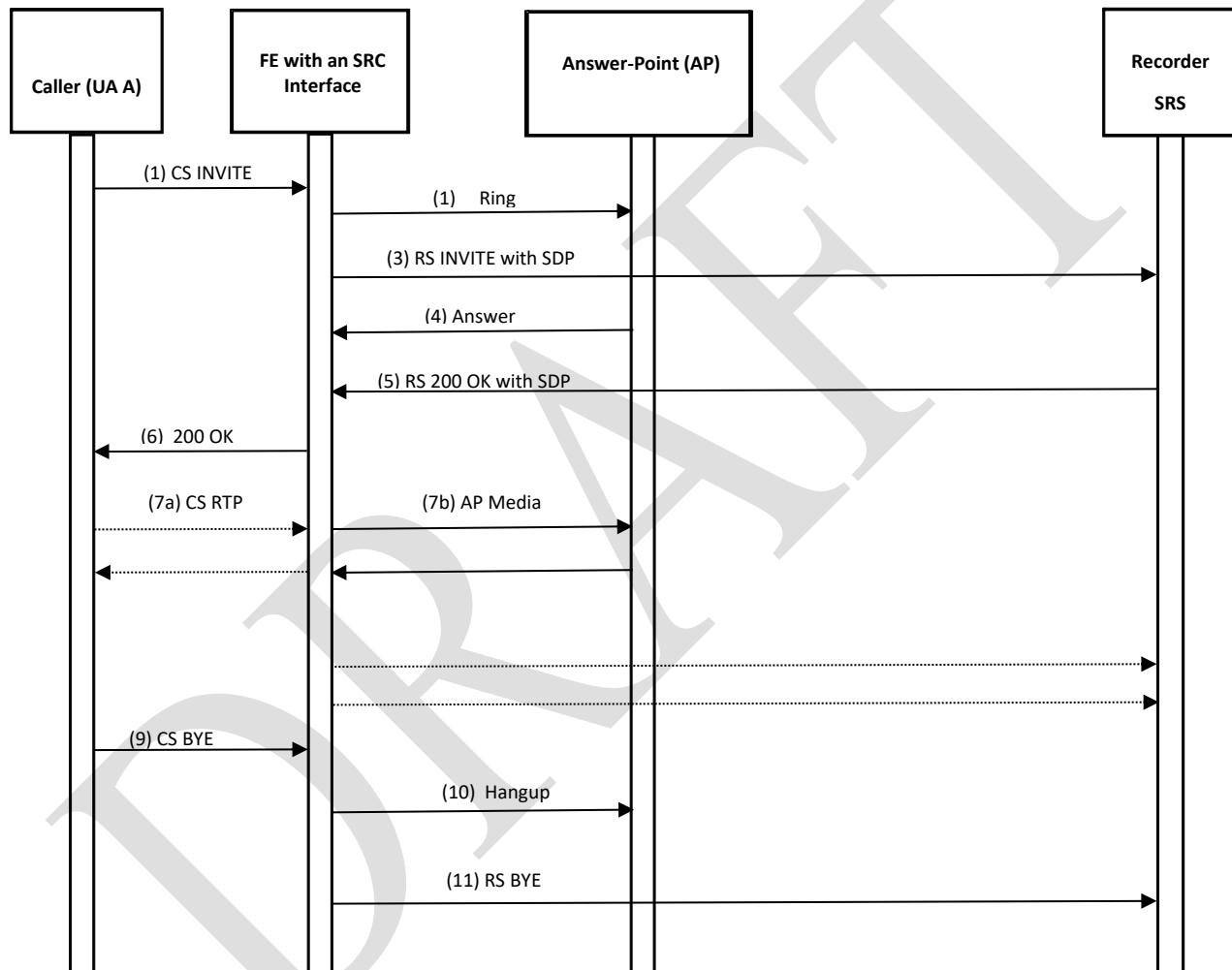


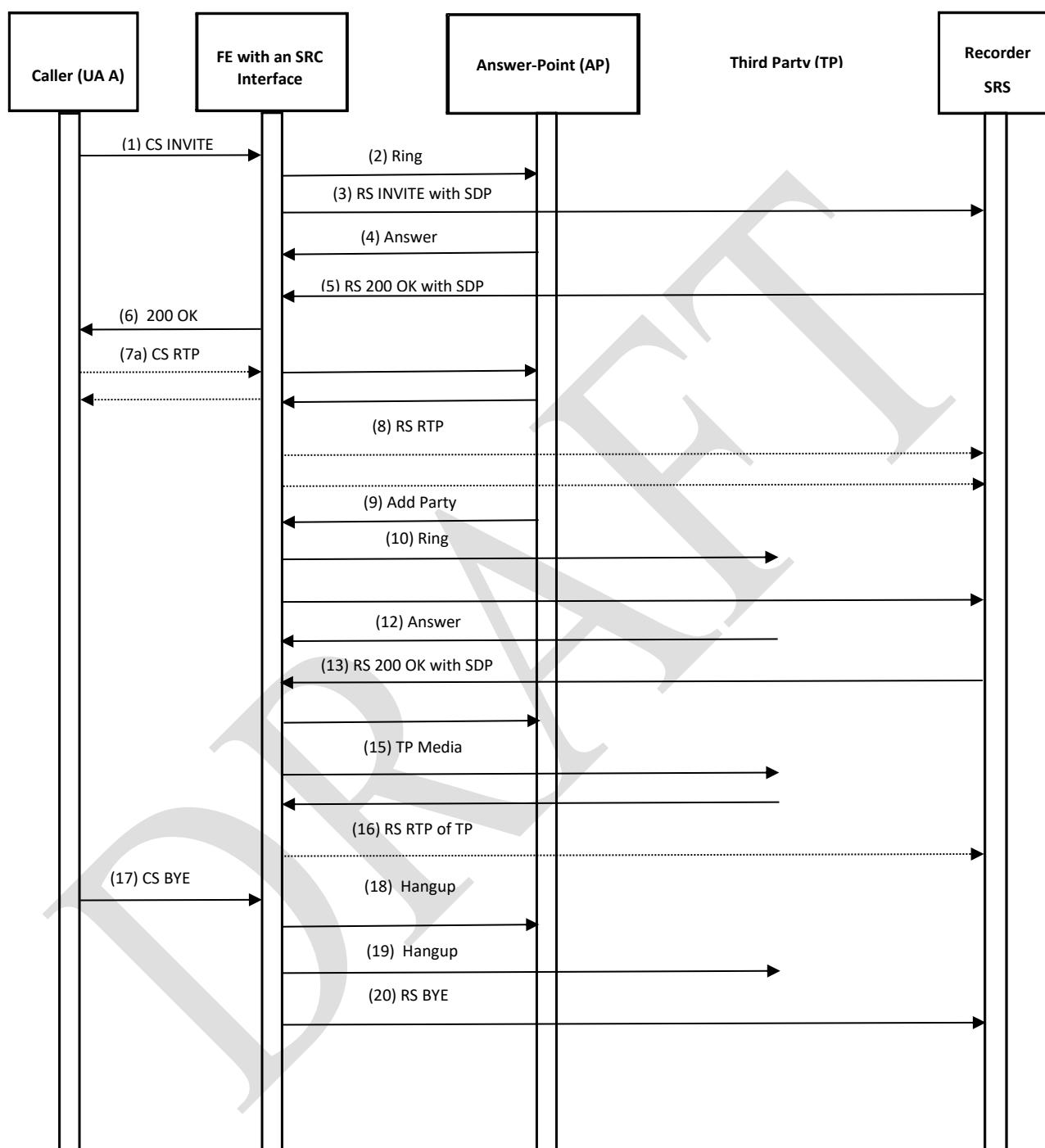
Figure 4-15 Incoming Call

7325 **4.12.2.2 Three Party Call (e.g. translator)**

7326 The Answer-Point establishes a two-party call and conferences in a third party. The call
7327 MUST still be recorded while the third party is being added as well as when all three parties
7328 are on the call.

- 7329 • Call hits the SRC
- 7330 • SRC opens a recording session with the recorder, including the call identifier
- 7331 • Call is answered
- 7332 • Call stream is added to the recording session
- 7333 • Both parties communicate
- 7334 • Answer-Point calls 3rd Party
- 7335 • Call is answered by 3rd Party
- 7336 • Re-invite is sent to the recorder with the call identifier 3rd Party stream is added to
7337 the recording session
- 7338 • All parties communicate
- 7339 • Caller hangs up
- 7340 • 3rd Party hangs up
- 7341 • Answer-Point hangs up
- 7342 • SRC closes the recording session.

7343 **Note:** All additional information about the call can be retrieved from the Logging Service
7344 using the call identifier.



7345

7346

Figure 4-16 Three-Party Call

[MM/DD/YYYY]

Page 260 of 675

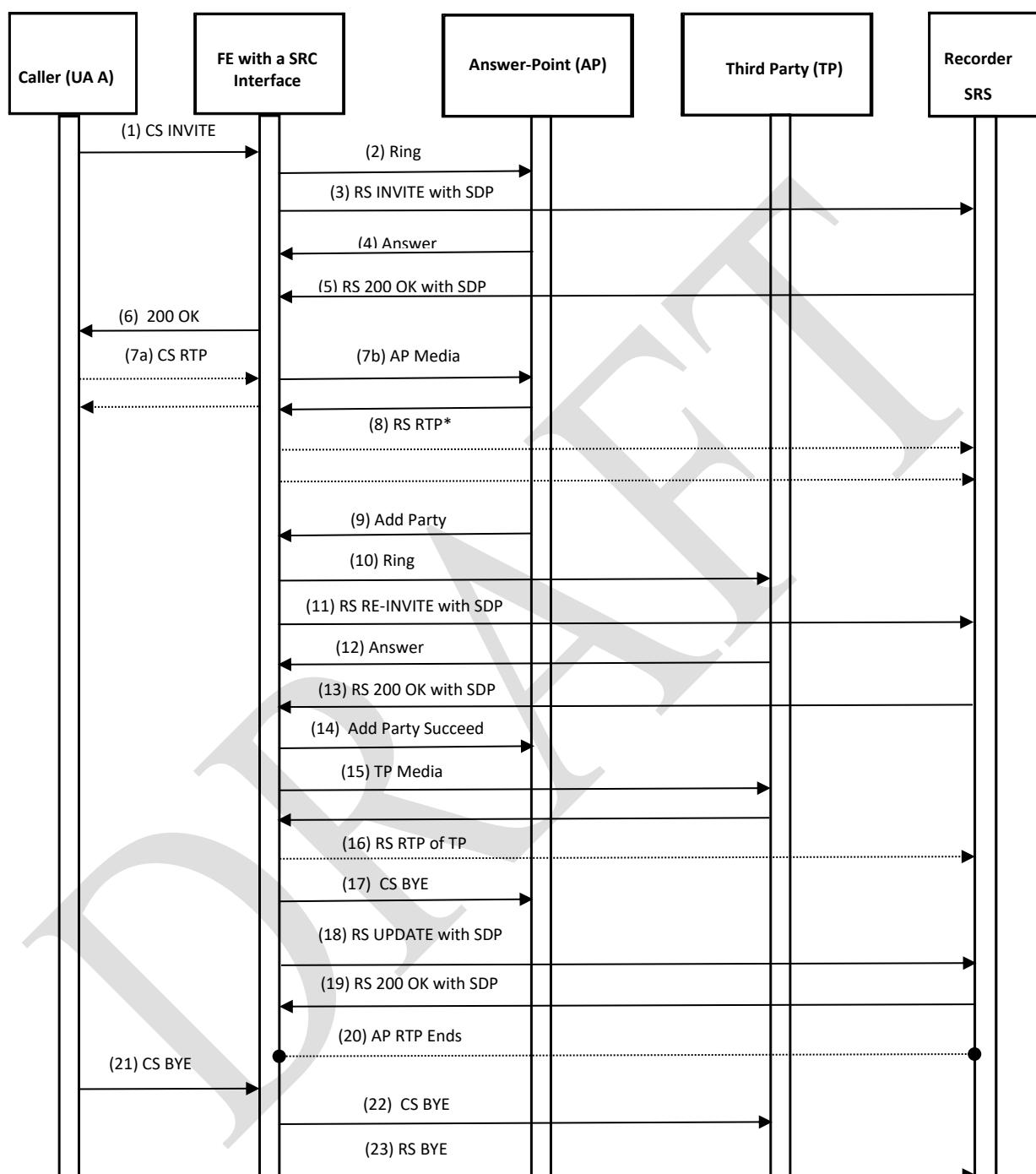


7347 **4.12.2.3 Attended Transfer**

7348 The Answer-Point transfers the call to a third party. The call MUST still be recorded if it is
7349 bridged by the SRC.

- 7350 • Call hits the SRC
7351 • SRC opens a recording session with the recorder, including the call identifier
7352 • Call is answered
7353 • Call stream is added to the recording session
7354 • Both parties communicate
7355 • Answer-Point calls 3rd Party
7356 • Call is answered by 3rd Party
7357 • Re-invite is sent to the recorder with the call identifier
7358 • 3rd Party stream is added to the recording session
7359 • Answer-Point hangs up
7360 • Remaining parties continue to communicate
7361 • Caller hangs up
7362 • 3rd Party hangs up
7363 • SRC closes the recording session.

7364 **Note:** All additional information about the call can be retrieved from the Logging Service
7365 using the call identifier.



7366

7367

7368 * RTP stream from Answer-Point to Recording Server in Step 8 stops.

[MM/DD/YYYY]

Page 262 of 675

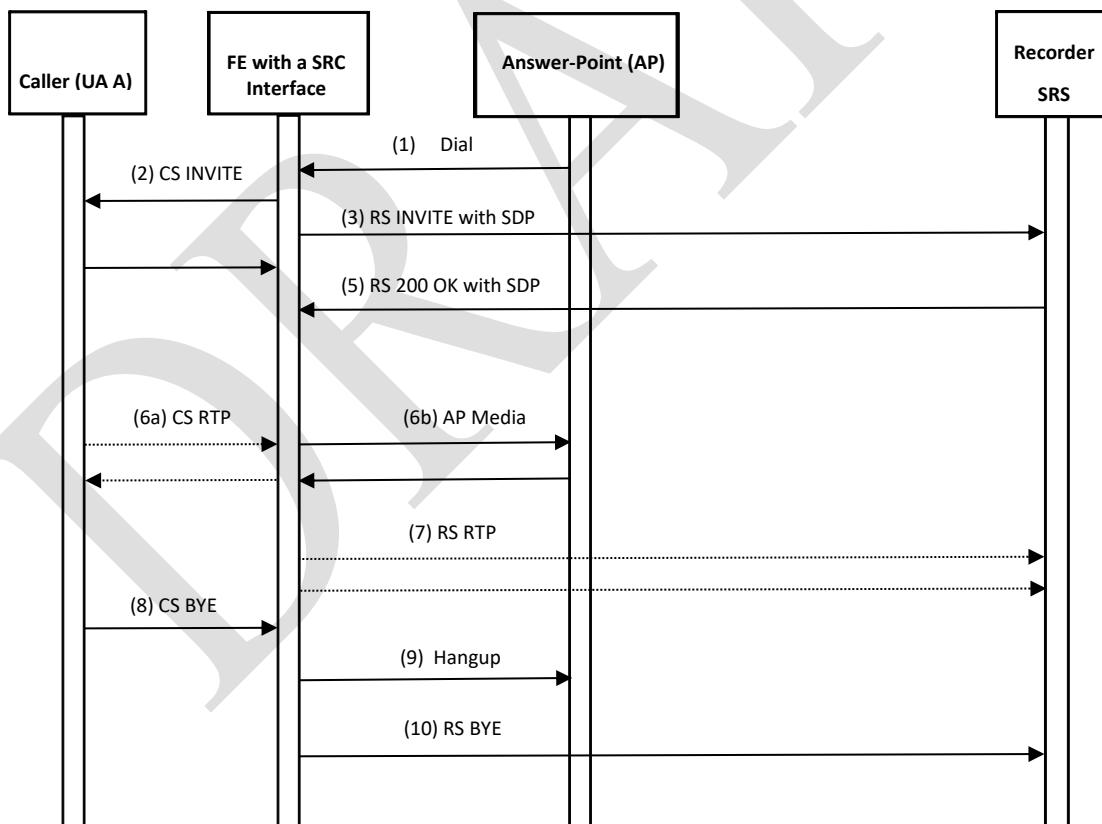


7369 **4.12.2.4 Call Back (Outbound Call)**

7370 The SRC initiates an outbound call via recorded administrative line in response to a 9-1-1
7371 hang-up or dropped call. The call between the Originating-Point and the Caller is recorded
7372 for its duration. The call flow for this scenario is:

- 7373 • Call is initiated in response to 9-1-1 call that was disconnected due to hang-up or drop
- 7374 • SRC opens a recording session with the recorder, including the call identifier
- 7375 • Call is answered by the previously disconnected caller
- 7376 • Call stream is added to the recording session
- 7377 • Both parties communicate
- 7378 • Called party hangs up
- 7379 • SRC Originating Point hangs up
- 7380 • SRC closes the recording session.

7382 **Note:** All additional information about the call can be retrieved from the Logging Service
7383 using the call identifier.



7384 **Figure 4-18 Call-Back**

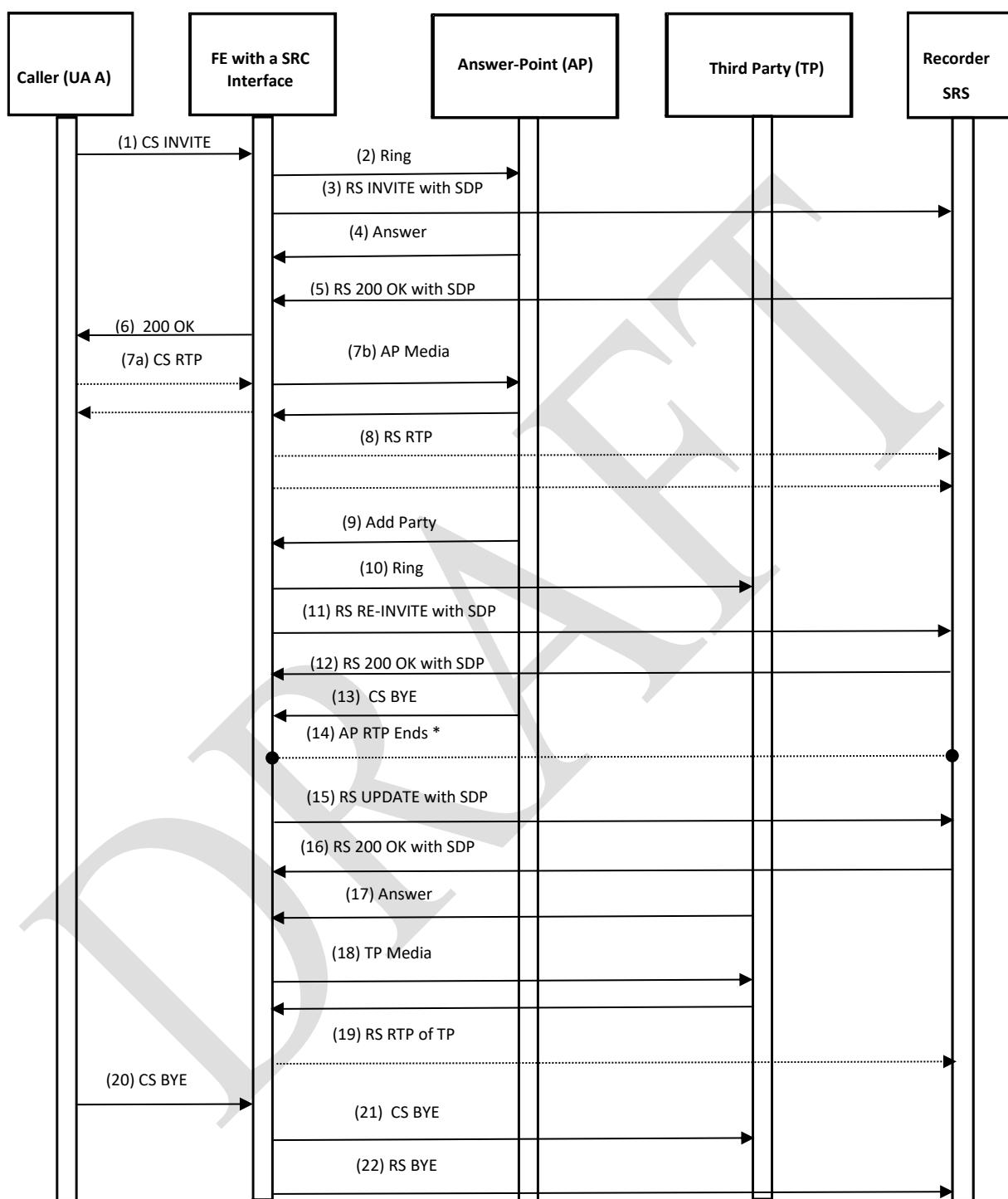
7385

7386 **4.12.2.5 Blind Transfer**

7387 The Answer-Point transfers the call to a third party as an unsupervised transfer. The call
7388 MUST still be recorded by the SRC.

- 7389 • Call hits the SRC
7390 • SRC opens a recording session with the recorder, including the call identifier
7391 • Call is answered
7392 • Call stream is added to the recording session
7393 • Both parties communicate
7394 • Answer-Point calls 3rd Party
7395 • Answer-Point hangs up
7396 • Re-invite is sent to the recorder with the call identifier
7397 • 3rd Party stream is added to the recording session
7398 • All parties communicate if and when 3rd party answers
7399 • Caller hangs up
7400 • 3rd Party hangs up
7401 • SRC closes the recording session.

7402 **Note:** All additional information about the call can be retrieved from the Logging
7403 Service using the call identifier.



7404

7405

Figure 4-19 Blind Transfer

[MM/DD/YYYY]

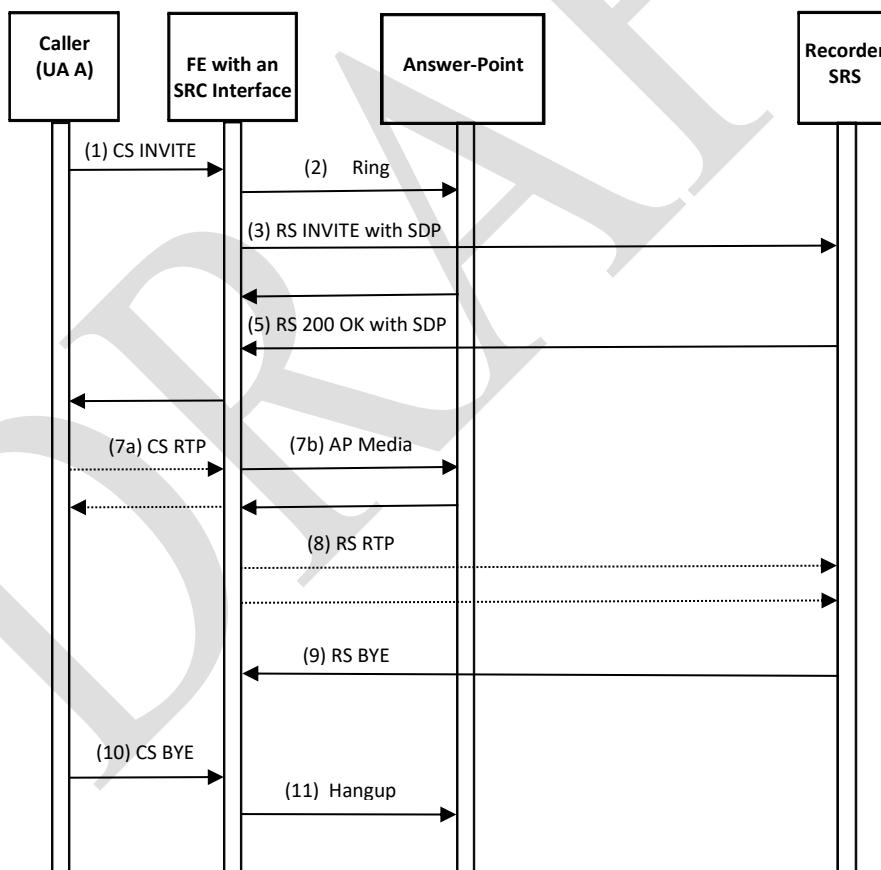
Page 265 of 675

7406 4.12.2.6 Clean Logging Service Shutdown

7407 The Logging Recorder MUST be able to provide a clean shut down by sending a BYE as
7408 specified in Section 3.1.1.3, for example when one SRS in a redundant pair is going out of
7409 service. The SRC MUST respond with a 200 OK.

- 7410 • Call hits the SRC
7411 • SRC opens a recording session with the recorder, including the call identifier
7412 • Call is answered
7413 • Answer-Point stream is added to the recording session
7414 • Both parties communicate
7415 • Recorder sends a BYE
7416 • SRC responds with a 200 OK.

7417 **Note:** All additional information about the call can be retrieved from the Logging Service
7418 using the call identifier.



7419

7420

Figure 4-20 Logging Service Shutdown

7421 **4.12.3 Log Recording**

7422 The OpenAPI definition of this web service may be found in Appendix E.8. The Logging
7423 Service has a policy (LogServiceAllowedToLog) of which entities are permitted to
7424 LogEvents, and a policy (LogServiceAllowedToRetrieve) of which entities are allowed to
7425 retrieve logged events.

7426 **Note:** A future edition of this document will describe how policies can restrict retrieval by
7427 more fine-grained criteria, for example allowing only agencies participating in a multi-
7428 agency incident to retrieve LogEvents about that incident.

7429 Entities might periodically review signed events to verify that their signatures are correct
7430 and they have an accessible and valid certificate (and thumbprint for certificates provided
7431 by reference). An entity that does so generates a Log Signature/Certificate Discrepancy
7432 Report (Section 3.7.22) to report problems to the logging entity. (As examples, a Logging
7433 Service might perform this process when it is under light load, or another entity might be
7434 configured to do this at certain intervals.)

7435 **4.12.3.1 LogEvents**

7436 The Logging Service stores LogEvents as a JWS. A LogEvent object contains:

Name	Condition	Description
clientAssignedIdentifier	OPTIONAL	An identifier assigned by the client
logEventType	MANDATORY	LogEvent type as described in Section 4.12.3.7
timestamp	MANDATORY	A Timestamp as defined in Section 2.3
elementId	MANDATORY	Element identifier (Section 2.1.3) of the element that logged the event
agencyId	MANDATORY	AgencyId (Section 2.1.1) of the agency that logged the event
agencyAgentId	Conditional: REQUIRED if the log record is traceable to an agent. If the log record is only attributable to an element or agency, this element will not be included.	The Agent Identifier (Section 2.1.2) of an agent that logged the event.

[MM/DD/YYYY]

Page 267 of 675



Name	Condition	Description
agencyPositionId	OPTIONAL	Identifier for the position that is handling a call.
callId	Conditional: REQUIRED if event is associated with a call	The Call Identifier of a call, see Section 2.1.6
incidentId	Conditional: REQUIRED if event is associated with an Incident	The Incident Tracking Identifier associated with the call, see Section 2.1.7
callIdSIP	Conditional: REQUIRED if event is associated with a SIP call	CallId from SIP
ipAddressPort	Conditional: REQUIRED if logging element knows the identity of the other element	Normalized IP address and port number string or Fully Qualified Domain Name of another element that participated in a transaction that triggered this LogEvent (e.g., an element that sent or responded to a query). This is not the address of the element that logs the event. For IPv6 addresses, the maximum uncompressed form is recommended and may be required in a future version of this document. (See <i>A Recommendation for Ipv6 Address Text Representation</i> , RFC 5952 [196].)
extension	OPTIONAL, occurs 0 or more times	Optional private extension parameters

7437

- 7438 The Logging Service stores and retrieves a JWS [171] of the entire LogEvent (see Section 5.10), including all extensions. The signer (using its credentials traceable to the PCA) is: the Agent if an agencyAgentId is provided, otherwise it is the Element.
- 7441 The signature is optional, but policy of the agency may require its use.
- 7442 The clientAssignedIdentifier is not used by the Logging Service but is preserved by it.

[MM/DD/YYYY]

Page 268 of 675



7443 The callId and incidentId are provided on all legs of a dialog-forming SIP transaction initial
7444 message (INVITE or MESSAGE). Stateless proxies may not know the IDs and thus may not
7445 be able to provide them, and some implementations may not be able to provide the IDs on
7446 other messages in the transaction. The Logging Service will need to find such messages via
7447 callIdSIP.

7448 This document specifies very detailed logging, often requiring an event to be logged by
7449 both the sender and receiver of data. This detail is invaluable for troubleshooting errors in
7450 processing after the fact. The amount of data being logged is typically a small fraction of
7451 the size of the media for the same call.

7452 The LogEvent object contains an “extension” member which is used to log any desired
7453 proprietary data in a Logging Service. The size of any object, with all its extensions, may
7454 be limited to a provisonable value by the Logging Service, and the operator of a Logging
7455 Service may have an approved list or disallowed list of allowed extensions.

7456 Logging services MUST NOT require any specific extension to provide services conformant
7457 to this document. FEs that use a Logging Service MUST NOT depend on a Logging Service
7458 accepting an extension to provide services conformant to this document. Each EventType
7459 contains additional data specific to the EventType.

7460 The parameters are sent as a JWS [171] (see Section 5.10).

7461 As described in Section 5.10, the Logging Service MUST be capable of handling signed and
7462 unsigned LogEvents and certain signing algorithms. The policy currently in force at the
7463 Logging Service determines the Logging Service’s acceptance of signed and unsigned
7464 LogEvents, which could require only signed LogEvents, only unsigned LogEvents, or could
7465 allow either. This policy is communicated to logging clients by the “requiredAlgorithms”
7466 parameter, which as described above (Section 4.12) specifies the currently acceptable
7467 signing algorithms. If “requiredAlgorithms” contains only the value “none”, then only
7468 unsigned LogEvents are acceptable; if “requiredAlgorithms” does not contain the value
7469 “none”, unsigned LogEvents are not acceptable. A LogEvent request containing a LogEvent
7470 whose JWS “alg” element value is not contained in “requiredAlgorithms” is rejected with an
7471 “Unacceptable Algorithm” error. This is an error response; the LogEvent is not recorded
7472 (although the Logging Service might log or record that it received such a request with
7473 details); the client needs to resubmit the request with an acceptable algorithm.

7474 Logging Services MUST be capable of verifying the signature of a signed LogEvent during
7475 the processing of the LogEvent request (i.e., before returning the response). The currently
7476 in force policy of the agency operating the Logging Service determines if the Logging
7477 Service does so. If the signature verification fails, it MUST return a “Signature Verification
7478 Failed” status code as a warning and SHOULD generate (subject to throttling) a

7479 Signature/Certificate Discrepancy Report (Section 3.7.22) to the logging entity. This is a
7480 warning, not an error; the LogEvent MUST be recorded, and the client MUST NOT retry the
7481 request. An entity receiving this warning should generate an internal DR or otherwise alert
7482 its operational staff to the problem and might choose to fall back to a previous certificate
7483 until the problem is corrected.

7484 Verifying LogEvent signatures requires access to the certificate used to sign the event (and
7485 all intermediate certificates to a trusted root). The entity creating a signed LogEvent
7486 specifies the certificate either by value or by reference, as described in Section 5.10. A
7487 Logging Service MUST support both mechanisms (e.g., by using a certificate cache
7488 indexable by thumbprint and loaded by resolving the certificate URL).

7489 The CallId and IncidentId are provided on all legs of a dialog-forming SIP transaction initial
7490 message (INVITE or MESSAGE). Stateless proxies may not know the IDs and thus may not
7491 be able to provide them, and some implementations may not be able to provide the IDs on
7492 other messages in the transaction. The Logging Service will need to track such messages
7493 (via the SIP call identifier) and log the Call and Incident IDs.

7494 This document specifies very detailed logging, often requiring an event to be logged by
7495 both the sender and receiver of data. This detail is invaluable for troubleshooting errors in
7496 processing after the fact. The amount of data being logged is typically a small fraction of
7497 the size of the media for the same call.

7498 To allow including proprietary data in LogEvents, the LogEvent object MAY contain
7499 additional elements not defined in this document. The size of any object, with all its
7500 extensions, may be limited to a provisonable value by the Logging Service, and the
7501 operator of a Logging Service may have an approved or disallowed list of allowed extension
7502 elements.

7503 Logging services MUST NOT require any specific extension to provide services conformant
7504 to this document. FEs that use a Logging Service MUST NOT depend on a Logging Service
7505 accepting an extension to provide services conformant to this document. Each
7506 LogEventType contains additional data specific to the LogEventType.

7507 **4.12.3.1.1 Retrieve LogEvents**

7508 Retrieves LogEvents from the Logging Service. For a GET operation the response is the log
7509 record for all events. Limit and start parameters are supported for pagination.
7510 HTTP method: GET
7511 Resource name .../LogEvents
7512 When the event is a RecMediaStartEvent, the returned events will have one or more "rtsp"
7513 parameters inserted by the Logging Service that MUST be RTSP URIs. The RTSP URI can

7514 be used to play back the call session. The "sdp" and "mediaLabel" are also returned to
7515 indicate which media stream in the session the event refers to. These "rtsp" parameters
7516 MUST NOT refer to media from other SIPREC sessions that recorded the same call.
7517 Because the IRR functionality uses this interface, the Logging Service MUST ensure that it
7518 can return a usable RTSP URL as soon as recording starts. The Logging Service MUST
7519 ensure that any RTSP URL it returns remains valid for at least one hour.

7520 The Retrieve Events includes the following parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
logEventType	OPTIONAL	Type of LogEvent, if not provided, events of any type are returned
startTime	OPTIONAL	If provided, only events timestamped at or after this time will be returned
endTime	OPTIONAL	If provided, only events timestamped at or before this time will be returned

7521 Status Codes

7522 200 LogEvents found
7523 404 Not Found

7524 On a successful GET, a logEventContainerArray is returned:

7525 **logEventArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
logEventContainers	MANDATORY	Array of LogEventContainer objects

7526 A LogEventContainer contains:

[MM/DD/YYYY]

Page 271 of 675



logEventId	MANDATORY	LogEvent Identifier assigned by the logging service as described in Section 2.1.8
rtsp	CONDITIONAL	rtsp parameters returned from RecMediaStartEvent. MUST be returned if media was recorded
logEvent	MANDATORY	A LogEvent in JWS format

7527

7528 **4.12.3.1.2 Post Event**

7529 Logs a new event into the Logging Service.

7530 HTTP method: POST

7531 Resource name .../LogEvent

7532 The body of the Post contains the JWS of a LogEvent as a Base64 encoded header, payload and signature

7534 The LogEvent entry point assigns a globally unique LogEvent Identifier (per Section 2.1.8) to each LogEvent and returns it in the logEventId in its response.

7536 Status Codes

7537 201 LogEvent successfully logged

7538 434 Signature Verification Failure

7539 438 Unacceptable Algorithm

7540 454 Unspecified Error

7541 460 Bad LogEvent

7542 461 LogEvent too big

7543 462 LogEvent extension not on approved list

7544 463 LogEvent extension on disallowed list

7545 **4.12.3.1.3 LogEvents by LogEvent Identifier**

7546 Retrieves a log event by its logEventId. Event is returned as a LogEventContainer (See Section 4.12.3.1.1.

7548 HTTP method: GET

7549 Resource name .../LogEvents/{logEventId}

7550 Parameters:

[MM/DD/YYYY]

Page 272 of 675



Name	Condition	Description
logEventId	MANDATORY	logEventId of the LogEvent data to retrieve (see Section 2.1.8 LogEvent Identifier)

7551 A successful response returns the LogEvent as a JWS

7552 Status Codes

7553 200 LogEvent found

7554 404 Not found

7555 4.12.3.2 Conversations

7556 Returns an HTML formatted record suitable for human consumption of the text portion of a call, including all text sent by all parties.

7558 HTTP method: GET

7559 Resource name .../Conversations

7560 Parameters:

Name	Condition	Description
callId	MANDATORY	Call ID of the call

7561 A successful response includes the conversation as a string in the response body.

7562 Status Code

7563 200 Conversation found

7564 404 Not found

7565 454 Unspecified Error

7566 464 No Text in this Call

7567 4.12.3.3 LogEventIds

7568 Retrieves LogEventIds. Use limit and start parameters for pagination.

7569 HTTP method: GET

7570 Resource name .../LogEventIds

7571 Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return

Name	Condition	Description
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
callId	OPTIONAL	Call ID of the call
incidentId	OPTIONAL	Incident ID of the call

7572 Status Codes

7573 200 LogEvents found

7574 404 Not Found

7575 454 Unspecified Error

7576 On a successful GET, a LogEventIdArray is returned:

7577 **LogEventIdArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
logEventIds	MANDATORY	Array of LogEvent identifiers

7578

7579 **4.12.3.4 Call IDs**

7580 Returns a list of Call Identifiers associated with a specific Incident Tracking Identifier, occurred within a time range or within a specified geographic region.

7582 HTTP method: GET

7583 Resource name .../ListCalls

7584 Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
incidentId	OPTIONAL	Incident ID of the call
startTime	OPTIONAL	Start time
endTime	OPTIONAL	End time
area	OPTIONAL	Area of interest

7585 Status codes

7586 200 Calls found

[MM/DD/YYYY]

Page 274 of 675



7587	404	Not Found
7588	454	Unspecified Error
7589	465	Bad Timestamp
7590	466	EndTime occurs before StartTime
7591	467	Bad Geoshape

7592 On a successful GET, a CallIdArray is returned:

7593 **CallIdArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
callIds	MANDATORY	Array of Call IDs

7594 **4.12.3.5 Incident IDs**

7595 Returns a list of Incident Tracking Identifiers occurring within a time/date range. Returns a list of Incidents that occurred within a specified geographic region.

7597 HTTP method: GET

7598 Resource name .../IncidentIds

7599 Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
startTime	OPTIONAL	Start time
endTime	OPTIONAL	End time
area	OPTIONAL	Area of interest

7600 Status codes

7601	200	Incidents found
7602	404	Not found
7603	454	Unspecified Error
7604	465	Bad Timestamp
7605	466	EndTime occurs before StartTime
7606	467	Bad Geoshape

7607 On a successful GET, an IncidentIdArray is returned:

7608 **IncidentIdArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
incidentIds	MANDATORY	Array of Incident IDs

7609

7610 **4.12.3.6 Agency IDs**

7611 Returns a list of agencies involved in a Call or an Incident.

7612 HTTP method: GET

7613 Resource name .../AgencyIds

7614 Parameters

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
incidentId	OPTIONAL	Incident ID of the call
callId	OPTIONAL	Call ID of the call

7615 Status codes

7616 200 Agencies found

7617 404 Not found

7618 454 Unspecified Error

7619 On a successful GET, an AgencyIdArray is returned:

7620 **AgencyIdArray**

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
agencyIds	MANDATORY	Array of Agency IDs

7621

[MM/DD/YYYY]

Page 276 of 675



7622 **4.12.3.7 LogEvent Types**

7623 This document creates a registry for LogEvent types. See Section 10.21.

7624 **Note:** A description of which elements generate which LogEvent types will be described in
7625 a future version of this document.

7626 This document defines the following EventTypes:

7627 **CallProcessLogEvent:** Each element that is not call stateful, but handles a call logs the
7628 fact that it saw the INVITE or MESSAGE pass through by logging a CallProcessLogEvent
7629 event. There are no parameters to "Call Process". Elements that log CallProcessLogEvent
7630 also log the actual SIP message with CallSignalingMessageLogEvent.

7631 **CallStartLogEvent:** Each element that is call stateful logs the beginning and end of its
7632 processing of a call, including non-interactive calls, with Start Call and End Call events.
7633 Elements that log CallStartLogEvent/CallEndLogEvent MUST also log the actual SIP
7634 message with CallSignalingMessageLogEvent for SIP parts of a call and
7635 GatewayCallLogEvent for TDM parts of a call. For CallStartLogEvent and CallEndLogEvent,
7636 the Timestamp MUST be the time the INVITE, MESSAGE, BYE or equivalents to these
7637 messages, or the final status code was received or sent by the element logging the event.
7638 Within CallStartLogEvent, a CallLogEvent object contains "direction",
7639 "standardPrimaryCallType", "standardSecondaryCallType", "localCallType" and "localUse".
7640 The "direction" member has one of two values, "incoming" or "outgoing", where
7641 "incoming" means a call received from the ESInet and "outgoing" means a call placed by,
7642 for example, a PSAP towards some caller. Optional "standardPrimaryCallType",
7643 "standardSecondaryCallType" and "localCallType" members MAY be included. The
7644 "standardPrimaryCallType" and "standardSecondaryCallType" members are limited to
7645 values found in the LogEvent Call Type Registry (see Section 10.23) "localCallType" can
7646 have any value defined locally. Optional "localUse" elements are also available (limited to
7647 128 bytes each). When "CallStartLogEvent" is used with non-SIP interfaces, "to" and
7648 "from" members are used to capture the participants in the call.

7649 **CallEndLogEvent:** Each element that is call stateful logs the beginning and end of its
7650 processing of a call, including non-interactive calls, with Call Start and Call End events.
7651 Elements that log CallStartLogEvent/CallEndLogEvent MUST also log the actual SIP
7652 message with CallSignalingMessageLogEvent for SIP parts of a call and
7653 GatewayCallLogEvent for TDM parts of a call. For CallStartLogEvent and CallEndLogEvent,
7654 the Timestamp MUST be the time the INVITE, MESSAGE, BYE or equivalents to these
7655 messages, or the final status code was received or sent by the element logging the event.
7656 Within CallEndLogEvent, a CallEventLogEvent object contains "direction",
7657 "standardPrimaryCallType", "standardSecondaryCallType", "localCallType" and "localUse" as

[MM/DD/YYYY]

Page 277 of 675



7658 defined above in CallStartLogEvent. When CallEndLogEvent is used with non-SIP interfaces,
7659 "to" and "from" members are used to capture the participants in the call.

7660 **RecCallStartLogEvent** is identical to CallStartLogEvent but is logged by the Logging
7661 Service (SRS) and the client (SRC) for the SPIREC recording session.

7662 **RecCallEndLogEvent** is identical to CallEndLogEvent but is logged by the Logging Service
7663 (SRS) and the client (SRC) for the SPIREC recording session.

7664 **CallTransferLogEvent:** When a call is transferred, the transfer is logged by the transferor
7665 (the entity that had the call prior to transferring it). The transfer target URI is logged in a
7666 target member. Elements that log CallTransferLogEvent MUST also log the actual SIP
7667 targetCallIdSIP member that contains the SIP CallId of the new session with the transfer
7668 target, when known. Note that the PSAP may not know this CallId, but the bridge would.

7669 **RouteLogEvent:** A proxy server that makes routing decisions (ESRPs or other SIP proxy
7670 servers in the path of the call) logs the route it selected with the RouteLogEvent
7671 EventType. The LogEvent contains the URI to which it decided to send the call (encoded in
7672 a "recipientUri" member), an optional text string "cause" stating why it chose the route, the
7673 policy owner (in a "policyOwner" member), policy type (in a "policyType" member), policy
7674 ID if policyType is "OtherRoutePolicy" (in a "policyID" member), policy queue name if
7675 policyType is "OriginationRoutePolicy" or "NormalNextHopRoutePolicy" (in a
7676 "policyQueueName" member), and the rule ID (in a "ruleId" member).

7677 **MediaStartLogEvent:** MediaStartLogEvent contains information about one call medium
7678 (voice, video, or RTT/MSRP text). The media event includes a text string "sdp" member that
7679 contains an RFC 2327 Session Description Protocol [12] description of the media codecs as
7680 negotiated. The MediaStartLogEvent event MUST include one or more "mediaLabel"
7681 members that MUST match the SDP labels [99] if they exist. More than one
7682 MediaStartLogEvent can occur for a call. Recorded media streams include integral time
7683 reference data within the stream. This event is logged by any media anchor (call recipient
7684 for an emergency call, caller for a callback, bridge, or BCF if the BCF anchors media) when
7685 at the start of media reception or transmission as appropriate. A "direction" member has
7686 one of two values: "incoming" or "outgoing".

7687 **MediaEndLogEvent:** MediaEndLogEvent signals that media streams stopped. The
7688 MediaEndLogEvent MUST include one or more "mediaLabel" members that must match the
7689 SDP labels in the corresponding MediaStartLogEvent. More than one MediaEndLogEvent
7690 (with different "mediaLabel"s) MAY occur for a call. This event is logged by any media
7691 anchor (call recipient for an emergency call, caller for a callback, bridge, or BCF if the BCF
7692 anchors media) for the communication session media. A "mediaQualityStats" member
7693 contains tags that give QoS statistics about the media stream. The content of

7694 "mediaQualityStats" MUST be a "SessionReport" element from RFC 6035 [43].
7695 "mediaQualityStats" SHOULD be supported by all media anchors.

7696 **RecMediaStartLogEvent** and RecMediaEndLogEvent are identical to
7697 MediaStartLogEvent/MediaEndLogEvent but apply to the SIPREC recording session. Both
7698 the SRC and SRS log RecMediaStartLogEvent/RecMediaEndLogEvent. If an entity receives a
7699 media stream that it transcodes to another stream, including receiving TTY tones as audio,
7700 the entity transcoding creates a SIPREC recording stream for the transcoded media it
7701 creates, and logs RecMediaStartLogEvent for it. The "mediaLabel" members MUST be the
7702 same as those in the MediaStartLogEvent/MediaEndLogEvent so that matching of streams
7703 is possible. If the SRC mixes audio from multiple streams, the mediaLabel is composed
7704 from the mediaLabels used in the originating streams, concatenated with a "+" between
7705 them. A "mediaTranscodeFrom" member is used in this case containing the RFC 4575 [40]
7706 label of the original incoming stream. Absence of the tag indicates no transcode is
7707 performed. For TTY received as audio, the recorded stream would be Real-time Text.

7708 **RecordingFailedLogEvent:** RecordingFailedLogEvent indicates that the entity logging
7709 this event attempted to record media, but the media recording mechanism failed. This
7710 event contains an SDP description of the media that failed to be recorded in a "sdp"
7711 member, and "reasonCode" and "reasonText" parameters that specify why recording could
7712 not complete. "reasonCode" MUST be a value from the IANA
7713 LoggingServiceMediaErrorReasonCodes registry. The Session Recording Client in a SIPREC
7714 media recording session is responsible for logging this event.

7715 **MessageLogEvent:** A SIP Message is logged with a MessageLogEvent. Elements that log
7716 Message MUST also log the actual SIP message with CallSignalingMessageLogEvent. The
7717 text of the message is included as a "text" parameter. A "direction" member has one of two
7718 values: "incoming" or "outgoing".

7719 **AdditionalAgencyLogEvent:** When an agency becomes aware that another agency may
7720 be involved, in any way, with a call, it MUST log an AdditionalAgencyLogEvent. The
7721 AdditionalAgencyLogEvent includes an "agencyId" member which is an Agency Identifier
7722 (see Section 2.1.1). Among other uses, this event is used by PSAP management to query
7723 all Logging Services that may have records related to a call or incident.

7724 **IncidentMergeLogEvent:** More than one call may be received about the same real world
7725 Incident. Since each call is initially assigned its own Incident Tracking Identifier, the
7726 Agency SHOULD merge them by assigning the subsequent call to the first call's Incident
7727 Tracking Identifier so that it's clear that both calls are about the same Incident. Also, while
7728 handling two incidents, it may become apparent later that the incidents are in fact, the
7729 same real world Incident. The Ids are merged with IncidentMergeLogEvent. The
7730 IncidentMergeLogEvent record contains the IncidentId of the incorrectly assigned incident

7731 in the "incidentId" member in the header field of the log record, and the Incident Id of the
7732 actual Incident in a "IncidentIdMerge" member. After a merge, the Id in the
7733 "incidentIdMerge" member SHOULD be used to refer to this Incident. Note that other
7734 agencies may not know that the Incidents are being merged, and therefore could log
7735 events against the originally assigned IncidentId.

7736 **IncidentUnMergeLogEvent:** When a IncidentMergeLogEvent is found to have been
7737 done in error, IncidentUnMergeLogEvent will undo the operation. The
7738 IncidentUnMergeLogEvent record contains the IncidentId of the Merged incident in the
7739 "incidentId" member in the header field of the log record, and the IncidentId of the other
7740 Incident in an "incidentIdUnmerge" member.

7741 **IncidentSplitLogEvent:** When an agency creates a new Incident by cloning the data
7742 from an existing Incident, and then assigning a new Incident Tracking Identifier to the new
7743 one, it logs the IncidentSplitLogEvent. IncidentSplitLogEvent requires the agency splitting
7744 the incident to create two records, one with the old Incident Id in the header field and the
7745 new Incident Id in the tag, and another IncidentSplitLogEvent record with the new Incident
7746 Id in the header field and the old one in the tag. The old or new Id is included in an
7747 "incidentId" member, which contains the Id and a "type" attribute that specifies whether
7748 this tag contains the "old" Id or the "new" Id.

7749 **IncidentLinkLogEvent:** Incidents are linked when two different incidents are not the
7750 same real world event but are related in some way. The IncidentLinkLogEvent record
7751 contains the Incident Tracking Identifier of the new Incident in the "incidentId" member in
7752 the header field, and the Incident Tracking Identifier of the original Incident being linked to
7753 in a "incidentIdLinked" member. The "relationship" member specifies the relationship
7754 between the incidents. Values include "parent", "child", "peer", and "unspecified". For
7755 "parent" and "child", the incidentId in the header field is the one described by the
7756 "relationship" member.

7757 **IncidentUnLinkLogEvent:** When a IncidentLinkLogEvent is found to have been done in
7758 error, IncidentUnLink will undo the operation. The IncidentUnLinkLogEvent record contains
7759 the IncidentId of the Linked incident in the "incidentId" member in the header field of the
7760 log record, and the IncidentId of the other Incident in an "IncidentIdunlinkedFrom"
7761 member.

7762 **IncidentClearLogEvent:** When an agency finishes its handling of an Incident, it logs a
7763 IncidentClearLogEvent record. Other agencies may still be processing the Incident.

7764 **IncidentReopenLogEvent:** If an agency needs to LogEvents on an Incident for which it
7765 has logged a IncidentClearLogEvent, it logs a IncidentReopenLogEvent.

7766 **LostQueryLogEvent:** Both the element that queries the ECRF/LVF and the ECRF/LVF
7767 itself generate a LostQueryLogEvent. The LogEvent includes the entire LoST query in the
7768 "queryAdapter" member. A "direction" member tag has one of two values: "incoming" or
7769 "outgoing". The ECRF/LVF will obtain the CallId and IncidentId from the LoST extension
7770 defined in Section 3.4.10.4. A "queryId" member is used to relate the request to the
7771 response. The id is generated locally, MUST be globally unique, and it is suggested that it
7772 be of the form: "urn:emergency:uid:queryid: 'globally unique id'". If the element is logging
7773 a malformed query it has received, it includes it in a "malformedQuery" member.

7774 **LostResponseLogEvent:** Both elements that query the ECRF/LVF, and the ECRF/LVF
7775 itself generate the LostResponseLogEvent. The entire response is logged using
7776 "responseAdapter" member. Malformed, invalid, or responses not received from the server
7777 are logged in a "responseStatus" member that contains a status code from the Status
7778 Codes Registry (Section 10.29). A "direction" member has one of two values: "incoming" or
7779 "outgoing". A "responseId" member is used to relate the request to the response, and
7780 MUST match the id used in the LostQueryLogEvent. If the element is logging a malformed
7781 response it has received, it includes it in a "malformedResponse" member.

7782 **CallSignalingMessageLogEvent:** Call Signaling (e.g., SIP) messages are logged with the
7783 CallSignalingMessageLogEvent. The entire message is included in a "text" member. A
7784 "direction" member has one of two values: "incoming" or "outgoing". An element MUST
7785 always log messages it receives (with "direction" set to "incoming"). If an element sends a
7786 signaling message as a result of an incoming logged message, it need only log the
7787 outgoing message (with "direction" set to "outgoing") if it changes any part of the signaling
7788 message. An element MUST log outgoing messages it originates. A "protocol" member
7789 indicates the protocol. Absence of the "protocol" member defaults to "sip". A registry of
7790 protocol values is defined in Section 10.22.

7791 **SipRecMetadataLogEvent:** The SRS MUST create LogEvents for any metadata received
7792 via the SIPREC metadata interface (RFC 7865) [117]. It does this by logging a
7793 SIPRECMetadataLogEvent to itself. The metadata included is a "siprecMetadataText" tag.
7794 The SRS MUST fill in the header fields for which the values are known, such as the CallId
7795 and IncidentId supplied by the Session Recording Client. The sipCallId in the header field
7796 will be set to the SIP callId from the communication session, not the SIP callId from the
7797 recording session.

7798 **NonRtpMediaMessageLogEvent:** Some media, for example MSRP, do not use RTP to
7799 transport the media. The messages that transport this media are logged with
7800 NonRtpMediaMessageLogEvent. The entire message is included in a "text" member. A
7801 "direction" member has one of two values: "incoming" or "outgoing". An element MUST
7802 always log messages it receives (with "direction" set to "incoming"). If an element sends a
7803 media message as a result of an incoming logged message, it need only log the outgoing

7804 message (with “direction” set to “outgoing”) if it changes any part of the media message.
7805 An element MUST log outgoing messages it originates. A “protocol” member indicates the
7806 protocol. Absence of the “protocol” member defaults to “sip”. A registry of protocol values
7807 is defined in Section 10.22.

7808 **AliLocationQueryLogEvent:** An LSRG [114] logs the query it sends to or receives from
7809 an ALI server with the AliLocationQueryLogEvent. An LPG also uses this LogEvent when it
7810 receives an ALI query from the legacy PSAP. The text of the query is included in a “text”
7811 member, and any message delimiter control characters such as STX/ETX are not included.
7812 The CallId and IncidentId MAY be left blank if they are not known by the LSRG (because
7813 the LSRG is outside the ESInet and does not assign these IDs). A “directionValuesCode”
7814 member has one of two values: “incoming” or “outgoing”. A “queryId” member is used to
7815 relate the request to the response. The id is generated locally, MUST be globally unique,
7816 and it is suggested that it be of the form: “urn:emergency:uid:queryid:’globally unique id’”.

7817 **AliLocationResponseLogEvent:** An LSRG MUST log the response it sends to or receives
7818 from its query to an ALI server with the AliLocationResponseLogEvent. An LPG MUST also
7819 use this LogEvent when it responds to an ALI query from the legacy PSAP. The text of the
7820 response is included in a “text” member, and any message delimiter control characters
7821 such as STX/ETX are not included. Malformed, invalid, or responses not received from the
7822 server are logged in a “responseStatus” member that contains a status code from the
7823 Status Codes Registry (Section 10.29). A “direction” member has one of two values:
7824 “incoming” or “outgoing”. A “responseId” member is used to relate the request to the
7825 response and MUST match the id used in the AliLocationQueryLogEvent.

7826 **MalformedMessageLogEvent:** An element that receives a malformed SIP message logs
7827 it with the MalformedMessageLogEvent. The malformed message is included in a “text”
7828 member. An “ipAddress” member is included, which contains the IP address of the sender
7829 of the message. An optional “eventExplanationText” member contains a human-readable
7830 explanation of why the SIP message was flagged as malformed. If the element believes it
7831 is under a DOS attack, then it MAY not log all malformed messages to avoid overloading
7832 the Logging Service.

7833 **EidoLogEvent:** Any element that sends or receives an Emergency Incident Data
7834 Document [111] MUST log it with the EidoLogEvent. If the EIDO is sent by value, the value
7835 is logged in a “body” member. If an EIDO is sent or received by reference, the EIDO URI
7836 MUST be logged with a “reference” member. When the URI is dereferenced, another
7837 EIDOLogEvent MUST be created with the “reference” and “body” by both the client and
7838 server. A “direction” member has one of two values: “incoming” or “outgoing”.

7839 **DiscrepancyReportLogEvent:** Any element that sends or receives a Discrepancy Report,
7840 or that sends or receives an update (Status, Resolution, etc.) for one, logs what it sent or

7841 received with the DiscrepancyReportLogEvent. The body of the report or response is
7842 included in a "contents" member. A "direction" member has one of two values: "incoming"
7843 or "outgoing". A "type" member identifies the name of the Discrepancy Reporting web
7844 service function that was called to make the report or response
7845 (DiscrepancyReportRequest, StatusUpdateResponse, etc.). See the Discrepancy Reporting
7846 section of this document for the full list of function names and details.

7847 **ElementStateChangeLogEvent:** When an element sends a notification of state change
7848 as described in the Element State section of this document, it MUST log the
7849 ElementStateChangeLogEvent. The event contains the body of the notification message in
7850 a "notificationContents" member. Elements that receive changes in ElementState MAY log
7851 receipt of such changes. The new state is logged with "StateChangeNotificationContents"
7852 member. The element ID (FQDN) of the element whose state changed is logged in the
7853 "affectedElementId" member. This tag is optional if the element that provides the state
7854 change is the element whose state is changed. A "direction" member has one of two
7855 values: "incoming" or "outgoing". Note that a Call Identifier, SIP Call Id, and Incident
7856 Tracking Identifier usually won't be available for an ElementStateChangeLogEvent. Devices
7857 that have proprietary interfaces may implement ElementStateChangeLogEvent even though
7858 they may not emit the notification defined in this document. Their states SHOULD be
7859 mapped to the closest state defined by the notification and logged with that state using
7860 ElementStateChangeLogEvent.

7861 **ServiceStateChangeLogEvent:** When a Service sends a notification of state change as
7862 described in the Service State section of this document, which includes Security Posture, it
7863 MUST log the ServiceStateChangeLogEvent. Elements that receive changes in serviceState
7864 MAY log receipt of such changes. The new state is logged with "newState" member for
7865 service state changes and in the "newSecurityPosture" member for security posture
7866 changes, if Security Posture is supported by the service. The service ID (FQDN) of the
7867 service whose state changed is logged in the "affectedServiceIdentifier" member. A
7868 "direction" member has one of two values: "incoming" or "outgoing". Note that a Call
7869 Identifier, SIP Call Id, and Incident Tracking Identifier usually won't be available for a
7870 ServiceStateChangeLogEvent.

7871 **AdditionalDataQueryLogEvent:** A query for Additional Data MAY be logged with the
7872 AdditionalDataQueryLogEvent. The URI the request was sent to is logged in a "uri"
7873 member. The event contains the body of the query in a "text" member. Logging queries at
7874 the client is optional but is RECOMMENDED because it shows the time lapse between query
7875 and response and provides for better troubleshooting. A server for AdditionalData that is
7876 located inside an ESInet, or LNG, or LSRG operated by, or on behalf of, a 9-1-1 Authority,
7877 MUST log all queries it receives. A "direction" member has one of two values: "incoming" or
7878 "outgoing". A "queryId" member is used to relate the request to the response. The id is

7879 generated locally, MUST be globally unique, and it is suggested that it be of the form:
7880 "urn:emergency:uid:queryid:'globally unique id'".

7881 **AdditionalDataResponseLogEvent:** Any Additional Data that is retrieved by a client
7882 MUST be logged using the AdditionalDataResponseLogEvent. The body of the retrieved
7883 data is included in "text" members, one per block of Additional Data. Malformed, invalid, or
7884 responses not received from the server are logged in a "responseStatus" member that
7885 contains a status code from the Status Codes Registry (Section 10.29). A server for
7886 AdditionalData that is located inside an ESInet, and an LNG, LPG, or LSRG operated by, or
7887 on behalf of, a 9-1-1 Authority, MUST log all responses it sends. A "direction" member has
7888 one of two values: "incoming" or "outgoing". A "queryId" member is used to relate the
7889 request to the response and MUST match the id used in the AdditionalDataQueryLogEvent.

7890 **LocationQueryLogEvent:** A HELD dereference request (RFC 6753) [55] or SIP Presence
7891 SUBSCRIBE message (RFC 3856) [25] MAY be logged with the LocationQueryLogEvent.
7892 The URI the request was sent to is logged in a "uri" member. The body of the request or
7893 SUBSCRIBE is included in a "text" member. Logging these is OPTIONAL at the client and
7894 REQUIRED at the server if the server is located inside an ESInet, or is an LNG or LSRG
7895 operated by, or on behalf of, a 9-1-1 Authority. A "direction" member has one of two
7896 values: "incoming" or "outgoing". A "queryId" member is used to relate the request or
7897 subscription to the response or notifications. The id is generated locally, MUST be globally
7898 unique, and it is suggested that it be of the form: "urn:emergency:uid:queryid:'globally
7899 unique id'".

7900 **LocationResponseLogEvent:** A HELD dereference response, a SIP Presence NOTIFY
7901 message, and a re-INVITE with a new location are logged with the
7902 LocationResponseLogEvent message. The body of the response or message is included in a
7903 "text" member. Malformed, invalid, or responses not received from the server are logged in
7904 a "responseStatus" member that contains a status code from the Status Codes Registry
7905 (Section 10.29). All clients and servers, if the server is located inside an ESInet, or is an
7906 LNG or LSRG operated by, or on behalf of, a 9-1-1 Authority, MUST log responses. A
7907 "direction" member has one of two values: "incoming" or "outgoing". A "responseId"
7908 member is used to relate the request or subscription to the response or notifications and
7909 MUST match the id used in the LocationQueryLogEvent.

7910 **CallStateChangeLogEvent:** This is used by an element to log a state change, such as
7911 logging an "answered" event by a device. The new state is included in a "state" member.
7912 The CallId, IncidentId, and sipCallId in the header field are from the emergency call whose
7913 state has changed. For state changes that involve another "leg" of a call, such as AddParty,
7914 a "legCallId" member contains the call id of that leg. If the leg is a SIP leg, this Id is the
7915 SIP Call Id of the leg otherwise it may be another identifier for that call.
7916 CallStateChangeLogEvent MUST be logged by all elements that change the state of the call,

[MM/DD/YYYY]

Page 284 of 675



7917 which would include a bridge and all entities within the ESInet that request bridge actions
7918 when an emergency call is on a bridge. A “direction” member has one of two values:
7919 “incoming”, meaning the element logging the state change received a message or other
7920 notice that changed the state; and “outgoing”, meaning this element caused the state
7921 change. If the target involved in the state change is not the element identified in the
7922 header field, the identifier of the target whose state changed must be included in a
7923 “targetId” member. If the target is a SIP device, this must be the sip URI of the target. An
7924 optional “changeReason” member contains the reason why the state changed. The content
7925 of this tag is not standardized at this time. A registry for these call states is defined in
7926 Section 10.24.

7927 **GatewayCallLogEvent:** This is used by an LNG, LPG, or LSRG to log a call entering or
7928 leaving on a legacy interface. It contains the following parameters which are OPTIONAL,
7929 but MUST be included if known:

- 7930 • portTrunkGroup – the port or trunk group
- 7931 • pAni – 10-digit number when LNG or LSRG handles a call from a legacy wireless or
7932 legacy VoIP network, or the pANI an LPG creates.
- 7933 • digits – what the LNG/LSRG received from the network (8, 10, or 20 digits) or what
7934 the LPG sent. If 20 digits, the first 10 are the calling party id, and the second 10 are
7935 the pANI, separated by a comma.
- 7936 • direction – “incoming” or “outgoing”
- 7937 • signalingProtocol – “SS7” or “CAMA”
- 7938 • legacyCallId

7939 **HookflashLogEvent:** An LPG logs a “hookflash” event with the HookflashLogEvent. An
7940 identifier for the line on which the event occurred is included in a “lineId” member, which is
7941 OPTIONAL but MUST be provided if known. It is not used when already logged as part of a
7942 GatewayCallLogEvent.

7943 **LegacyDigitsLogEvent:** An LPG logs DTMF or MF digits with the LegacyDigitsLogEvent. A
7944 “sentReceived” member, with values of “sent” or “received”, identifies the direction of the
7945 digits. A “type” member, with a value of “DTMF” or “MF” identifies the type of digits that
7946 were received. “digits” carries the digit or digits that were transmitted or received. These
7947 are not used when already logged by GatewayCallLogEvent (such as sending pANI digits at
7948 an LPG).

7949 **AgentStateChangeLogEvent:** An element logs a change in agent device state with the
7950 AgentStateChangeLogEvent. There are two tags “primaryAgentState” and
7951 “secondaryAgentState”. “primaryAgentState” has two values: Available and Not Available. A
7952 registry for secondary agent device states is defined, see Section 10.21. If the device
7953 whose state has changed is not the element identified in the header field, the identifier of

7954 the device MUST be included in a "deviceID" member. All elements supporting agents
7955 MUST support the "primaryAgentState"; "secondaryAgentState" support is OPTIONAL.

7956 Several of these secondary states (e.g., Active and Hold) make sense with both Available
7957 and Not Available primary states.

7958 **QueueStateChangeLogEvent:** A queue manager MUST log a change in the state of the
7959 queue with the QueueStateChangeLogEvent. The event contains the body of the
7960 notification message in a "notificationContents" member. Elements that receive changes in
7961 QueueState MAY log receipt of such changes and MUST log a state change to
7962 "unreachable". The queue ID whose state changed is logged in the "queueId" member. A
7963 "direction" member has one of two values: "incoming" or "outgoing". Note that a Call
7964 Identifier, SIP Call Id, and Incident Tracking Identifier usually won't be available for a
7965 QueueStateChangeLogEvent.

7966 **KeepAliveFailureLogEvent:** The OPTIONS request is the "keep alive" mechanism
7967 specified in this document (Section 3.1.2.3). An element that gets a normal response to its
7968 OPTIONS request does not log the response. Malformed, invalid, or responses not received
7969 from the other element MUST be logged in a "responseStatus" member that contains text
7970 and a status code from the Status Codes Registry (Section 10.29). There is a TimeOut
7971 status in that registry that is used for a timeout failure of OPTIONS.

7972 **RouteRuleMsgLogEvent:** The LogMessageAction object (see Section 3.3.3.2.4 Log
7973 Message Action) generates a RouteRuleMsgLogEvent containing the policy owner (in a
7974 "policyOwner" member), policy type (in a "policyType" member), policy ID if policyType is
7975 "OtherRoutePolicy" (in a "policyID" member), policy queue name if policyType is
7976 "OriginationRoutePolicy" or "NormalNextHopRoutePolicy" (in a "policyQueueName"
7977 member), the rule ID (in a "ruleId" member), rule priority (in a "priority" member), and the
7978 contents of the action's "message" member if present (in a "message" member).

7979 **PolicyChangeLogEvent:** Policy changes are logged in a PolicyChangeLogEvent. The type
7980 of the Policy is specified in a "type" member. "queueName" and "policyId" are provided as
7981 appropriate and the owner is specified in an "owner" member. The type of change is
7982 specified in a "changeType" member, and has one of three values: "CREATE", "UPDATE",
7983 or "DELETE". "CREATE" is used when the policy store did not have a policy with the
7984 "policyType", "policyId" or "policyQueueName", "UPDATE" is used when it does. The policy
7985 being "CREATE"ed or "UPDATE"ed is specified in a "policyContent" member. The name of the
7986 Policy Store, or the URL of the Policy Store web service, is specified in a "policyStoreId"
7987 member. The name of the application used to make the change is specified in a
7988 "policyEditor" member.

7989 **VersionsLogEvent:** Records the response to a web service Versions request (See Section
7990 2.8). A "source" member has the URL used to query versions and the "response" member
7991 has the response received.

7992 **SubscribeLogEvent:** When a subscription request is processed for any defined Event
7993 Package, the transaction is logged with SubscribeLogEvent. A "package" member is a
7994 selection from the Event Package Registry (See Section 10.35). A "peer" member contains
7995 the URI or FQDN of the other party. An array of type/value "parameter" members contain
7996 any parameters in the subscribe. The "expiration" member contains the final expiration
7997 time negotiated. A "response" member records the response code the subscription
7998 received/sent. The "purpose" flag is set to "initial" for a new subscription, "refresh" for a
7999 refresh of an existing subscription, and "terminate" for a terminated subscription. The
8000 Server MUST log this event, the client MAY log. A "direction" member tag has one of two
8001 values: "incoming" or "outgoing". A "subscriptionId" member is used to relate the correlate
8002 transactions on this subscription. The id is generated locally, MUST be globally unique, and
8003 it is suggested that it be of the form: "urn:emergency:uid:subid:'globally unique id'".

8004 A registry for LogEvents is defined. See Section 10.21. A registry for the Event Package is
8005 defined, see Section 10.35.

8006 **Note:** A description of which elements generate which LogEvent types will be described in
8007 a future version of this document.

8008 **4.12.3.8 Instant Recall Recorder**

8009 The ability to quickly review current or recent emergency communications content is
8010 important. The Logging Service's Web Service interface supports this capability with the
8011 query, retrieval, and streaming media functions described in Section 4.12. This interface
8012 supports recall of all defined media types. A client application may use these functions to
8013 retrieve media for display or playback. The client is expected to impose any additional
8014 limitations required by local policy, such as limiting recall to communications the user has
8015 handled, to specific communications types, and/or limiting the time period from which
8016 recent communications can be recalled. The client is also responsible for providing
8017 functionality that allows the user to navigate within and between recalled communications.
8018 Access to media for instant recall is subject to the same security restraints as all log
8019 records. The PSAP may impose additional constraints as to which agents may access
8020 media.

8021 **4.12.3.9 LogEventReplicator**

8022 Devices or services may be created that use LogEvents to provide some benefit. An
8023 example is a readerboard that shows a call queue. Such devices may wish to receive a
8024 clone of the LogEvent stream going to the Logging Service. A LogEventReplicator has

8025 interfaces identical to LogEvent (Section 4.12.3). It can take a stream of LogEvents on its
8026 input port(s) and replicate them to each of its provisioned output ports. One of the output
8027 ports may be connected to the Logging Service, in which case all FEs that log would send
8028 their LogEvents to the replicator, which would copy them to the Logging Service and the
8029 other devices connected to the replicator. The replicator may be integrated into the
8030 Logging Service, may be stand-alone, or may be integrated into another FE.

8031 The replicator MUST replicate LogEvents exactly as they were received without modifying
8032 any field. For example, if a replicator inserted its own ElementID or Timestamp in the
8033 header field, it would destroy the original data the elements subscribing to the event would
8034 need.

8035 Replicators may have filtering capability to restrict which events are sent to which ports,
8036 but such filtering is not otherwise standardized. Each event received by the replicator
8037 MUST be sent to each of the output ports, subject to such filtering, if implemented. One of
8038 the output ports is designated the “master” port. When a transaction is started on the input
8039 port, the replicator starts the transaction on all of its output ports. Whatever response is
8040 returned from the master port is used as the response from the replicator to the input port.
8041 All other responses are ignored. If the Logging Service is connected to a replicator output
8042 port, normally it would be on the master port.

8043 **4.12.4 Roles and Responsibilities**

8044 Any agency, including a PSAP, may run its own Logging Service. The ESInet may have one
8045 or more Logging Services. All agencies and NG9-1-1 functional elements MUST have access
8046 to a conformant Logging Service and log all relevant events in that service. Media are
8047 recorded as specified in Section 4.12, with recording at more than one point in the call
8048 path desirable. Recording of media at the BCF can be substituted for recording of media at
8049 the endpoints if the BCF is always in the path of all media. Recording media is subject to
8050 legal and privacy restrictions that may govern where media is recorded and who has access
8051 to such recordings.

8052 **4.12.5 Operational Considerations**

8053 Because events and media related to an Incident may be logged in several different
8054 Logging Services during the life of the Incident, it will sometimes be necessary to query
8055 multiple Logging Services to reconstruct what happened. Similarly, a Logging Service may
8056 be in the ESInet and shared among several agencies. This implies the need for policies and
8057 agreements between different jurisdictions to control what can be retrieved, and under
8058 what circumstances. These policies must find a balance between the desire to protect
8059 potentially sensitive media, and the need to provide access to those media for legal
8060 reproduction and troubleshooting purposes.

8061 It is anticipated that the same media may be recorded in more than one Logging Service
8062 along the call chain, thus providing some redundancy. It is not anticipated that the same
8063 LogEvents will be logged in more than one Logging Service; an element will LogEvents to
8064 the Logging Service that serves its own network.

8065 The data stored in a Logging Service contain a wealth of raw statistical information that
8066 can be collated and compared with data from other systems and Logging Services to
8067 provide valuable insights into how the NG9-1-1 service is performing. Providing access to
8068 these data for such analysis will be valuable because that analysis can guide resource
8069 allocation to support continual improvement of services. Policies and agreements will need
8070 to be established to facilitate appropriate sharing of these data.

8071 **4.13 Forest Guide**

8072 The ECRF and LVF infrastructure make use of Forest Guides as defined in RFC 5582 [47]. A
8073 server that does not answer a query can refer to a Forest Guide to determine the response.

8074 **4.13.1 Functional Description**

8075 The following definitions are adapted from those in RFC 5582, used with permission of the
8076 authors:

- 8077 • Authoritative ECRF/LVF: A LoST server that can provide the authoritative answer to
8078 a particular set of queries (e.g., covering a set of civic labels or a particular region
8079 described by a geometric shape). An authoritative ECRF/LVF may redirect or forward
8080 a query to another authoritative ECRF/LVF within the tree.
- 8081 • Child: An ECRF/LVF that is authoritative for a sub-region of another authoritative
8082 ECRF/LVF. A child can in turn be a parent for another authoritative ECRF/LVF.
- 8083 • (tree node) cluster: A node cluster is a group of ECRFs that all share the same
8084 mapping information and return the same results for queries. Clusters provide
8085 redundancy and share query load. Clusters are fully meshed (i.e., they all exchange
8086 updates with each other).
- 8087 • Coverage region: The coverage region of an authoritative ECRF/LVF is the
8088 geographic region within which the ECRF/LVF is able to authoritatively answer
8089 mapping queries. Coverage regions are generally, but not necessarily, contiguous
8090 and may be represented as either a subset of a civic address or a geometric object.
- 8091 • Forest Guide (FG): A Forest Guide has knowledge of the coverage region of trees for
8092 a particular top-level service.
- 8093 • Parent: A LoST server that covers the region of all of its children. A LoST server
8094 without a parent is a root authoritative ECRF/LVF.
- 8095 • Tree: A self-contained hierarchy of authoritative mapping servers for a particular
8096 service. Each tree exports its coverage region to the Forest Guide.

8097 Given a query to an area outside its coverage area, an ECRF/LVF may have the coverage
8098 regions of other ECRF/LVFs to which it could refer a query, or it would refer to a Forest
8099 Guide. In NG9-1-1, each state is nominally a tree, with local ECRF/LVFs as the children.
8100 The top of the tree is often a state ECRF/LVF. There is a National Forest Guide that has
8101 knowledge of these trees. The National Forest Guide exchanges mappings with other
8102 National Forest Guides. A state coverage region, exported to the National Forest Guide,
8103 could be the civic state element, and a polygon representing the state boundary.

8104 **4.13.2 Interface Description**

8105 The National Forest Guide maintains a LoST interface, as described in Section 3.4, for
8106 query resolution. It also maintains a LoST-sync interface defined in RFC 6739 [79] for
8107 updating its coverage regions. The LoST-sync interface is used for both state ECRF/LVF
8108 interfaces and other National Forest Guides. The National Forest Guide only serves
8109 “urn:service:sos”, “urn:emergency:service:sos”, and “urn:emergency:service:responder”. It
8110 may be able to refer to other Forest Guides for services other than these. The National
8111 Forest Guide may interchange coverage with other National Forest Guides.

8112 A Forest Guide provides gap/overlap coverage analysis as described for ECRFs in Section
8113 4.3.5 and provides the same notification service described.

8114 The Forest Guide MUST implement the server-side of the ElementState event notification
8115 package.

8116 **4.13.3 Data Structures**

8117 The Forest Guide has one or more civic data structures and one or more GML polygons
8118 (set) representing the state coverage region. It also maintains coverage regions for other
8119 countries in a similar manner.

8120 **4.13.4 Roles and Responsibilities**

8121 The Forest Guide SHOULD be managed nationally (agency not yet identified) and MAY
8122 evolve to an entity more representative of all public safety agencies or covering more than
8123 one nation (e.g. Canada and the U.S. could share a Forest Guide). As described in RFC
8124 5582, there is no requirement that a Forest Guide be “official” or national government
8125 sanctioned. The operators of the constituent ESInets can decide whether or not to trust
8126 that any entity purporting to be a Forest Guide actually does provide the service, and so
8127 provide their coverage and mappings, and query it for out-of-area data. Although this
8128 document envisions that there will be a single authoritative Forest Guide for each country
8129 (or multiple countries), there could in fact be more than one and as long as the constituent
8130 ESInets contribute their data, it could be used. State ECRF and LVF operators SHALL
8131 arrange for their coverage regions to be provisioned in a Forest Guide. Forest Guide

8132 operators SHALL maintain well-known contact information so that other Forest Guides can
8133 arrange to exchange their coverage regions and mappings. Until a Forest Guide is
8134 available, State ECRF and LVF operators SHOULD exchange coverage and mapping data
8135 with other ESInet providers.

8136 **4.13.5 Operational Considerations**

8137 The Forest Guide idea is specifically designed so that there is no global “root” Forest Guide.
8138 This means that the National Forest Guide will have to develop policies for its own
8139 operation when identifying the authoritative Forest Guide for another country or area.
8140 Specifically, it can be expected to have to deal with disputed territory, where more than
8141 one National Forest Guide claims they are authoritative for the same area.

8142 **4.13.6 Security Considerations**

8143 Since the Forest Guide could be a bottleneck in the routing or transfer of emergency calls
8144 that are not initially presented to the appropriate ESInet, it is an attractive attack target.
8145 For this reason, there SHALL be both internal and external Forest Guides. The internal
8146 Forest Guide is accessible to ESInets and only allows queries from entities inside those
8147 ESInets. The external Forest Guide is public and allows queries from any source. When it is
8148 under stress, the internal Forest Guide MAY refuse queries from any entity for which it
8149 does not have existing entries (nominally state level ECRFs, and other Forest Guides). For
8150 this reason, queriers needing routes for emergency calls SHOULD always query their local
8151 ECRF using recursion, which will result in obtaining the correct mapping, possibly involving
8152 the internal Forest Guide as part of the query resolution process. When not under stress,
8153 the internal Forest Guide MAY answer queries from other entities, but such queries would
8154 result from misconfiguration in the querier, and management action to identify such
8155 problems may be undertaken by the Forest Guide operator. State ESInets and even large
8156 OSPs SHOULD maintain a local copy of the Forest Guide to use if they are unable to access
8157 the Forest Guide. The Forest Guide SHOULD provide an RFC 6739 LoST-sync feed for these
8158 local replicas.

8159 **4.14 DNS**

8160 All elements identified by hostnames MUST have corresponding Domain Name Service
8161 (DNS) records as specified in STD13 (RFC 1034) [74] in the global public DNS. All elements
8162 connected to the ESInet MUST have local DNS resolvers to translate hostnames they
8163 receive to IP addresses. Since the ESInet must continue to work in the face of disasters,
8164 DNS servers must be highly redundant. When a caching DNS resolver in the ESInet cannot
8165 refresh an expired cached resource record in response to a query because the authoritative
8166 DNS server is not available, it SHOULD reuse the stale cached resource record as though
8167 the cached resource record’s TTL is 1 second, as described in Section 4 of [draft-ietf-

[MM/DD/YYYY]

Page 291 of 675



8168 dnsop-serve-stale-00]. DNSSEC (RFC 4035) [118] MUST be deployed in authoritative DNS
8169 servers, especially those resolving names found in external ECRF/LVFs.
8170 A domain that has SIP elements within the domain MUST have an SRV record RFC 2782
8171 [75] for a SIP service for the domain, and any of its subdomains that may appear in a URI.
8172 Placing a LoST query always requires resolution of an Application-Unique String (AUS),
8173 which is in the form of an FQDN via U-NAPTR (RFC 4848 [154]), and U-NAPTR resolution
8174 may also be required to obtain the URI for a LIS (per RFC 5986) [155].

8175 **4.15 Service/Agency Locator**

8176 The ESInet will connect to many services and public safety agencies. A directory ("white
8177 pages" and "yellow pages") of agencies, together with key information about the service or
8178 agency, is the function of the Service/Agency Locator. The Service/Agency Locator is a
8179 distributed database. There are several mechanisms by which the Service/Agency Locator
8180 can be searched to locate a specific service or agency. One primary way to search the
8181 Service/Agency Locator is by name. The Service/Agency Locator provides a name (white
8182 page) search function, with wild cards, to find a specific service or agency. The search by
8183 name is more useful for agencies than services. The name that is searched comes from the
8184 "org" field of the Agency jCard that is returned in the Service/Agency Locator Record.
8185 Another method to search is by location and agency type.

8186 A Service/Agency Locator Service is provided in the ESInet. Every service as defined in
8187 Section 2.1.5 and every Public Safety Agency connected to the ESInet is listed in the
8188 Service/Agency Locator. The Service/Agency Locator has two components:

- 8189 a) A Service/Agency Locator Record Store (SALRS) which holds the actual data record
8190 for the service or agency;
- 8191 b) A search component, which uses the ECRF and a LoST query to find a given service
8192 or agency by type and location.

8193 A service/agency locator record is identified by a URI whose domain is an SALRS. The URI
8194 can be presented to an SALRS that will respond with the record. The ECRF returns the URI
8195 (see Section 4.15.2).

8196 Each FE in the Service/Agency Locator MUST implement the server-side of the
8197 ElementState event notification package. The Service/Agency Locator FE MUST promptly
8198 report changes in its state to its subscribed elements.

8199 The set of Service/Agency Locator FEs within an ESInet MUST implement the server-side of
8200 the ServiceState event notification package for the Service/Agency Locator. Since the
8201 Service/Agency Locator Service is typically a state-wide service it is RECOMMENDED that
8202 the state level Service/Agency Locator subscribe to ElementState for each Service/Agency

8203 Locator FE within the state and provide a single Service/Agency Locator ServiceState
8204 notifier for the entire state.

8205 **4.15.1 Service/Agency Locator Record Store**

8206 A Service/Agency Locator Record Store is a web service that, when presented with a
8207 service/agency locator URI, returns the service/agency locator record. An HTTPS GET on
8208 the URI is used to retrieve a record from the Record Store. The querier MUST use
8209 credentials traceable to the PCA to create the TLS connection, and the credential and its
8210 corresponding agency type and role may influence which information is returned.

8211 The SALRS may be operated by the agency itself, the ESInet operator may operate an
8212 SALRS for the entire ESInet, or any other party may operate an SALRS. Every service and
8213 every agency MUST have a record stored in at least one SALRS, with the URI for that
8214 record stored in the ECRF that serves the service or agency.

8215 **4.15.2 Service/Agency Locator Search by Location**

8216 The ECRF is used for a Service/Agency Locator search function. For this purpose the
8217 service URNs for all service and agency types are defined, starting with
8218 "urn:emergency:service:serviceagencylocator" and followed by a Service Name or agency
8219 type.

8220 For example, to find the service or agency locator record for the police department that
8221 serves the city of Wonderville, in Sunshine County, Iowa, a client sends a LoST FindService
8222 query to the ECRF. The query is constructed as follows:

- 8223 • a <service> element set to "urn:emergency:service:serviceagencylocator.police"
- 8224 • a <location> element constructed as follows:
 - 8225 ○ a "profile" attribute set to "civic"
 - 8226 ○ a <civicAddress> element containing:
 - 8227 ■ a <country> element set to "US"
 - 8228 ■ an <A1> element set to "IA"
 - 8229 ■ an <A2> element set to "Sunshine"
 - 8230 ■ an <A3> element set to "Wonderville"

8231 The ECRF returns a LoST findservice response. The response contains a <mapping>
8232 element that contains a URL within a <uri> element. In this example, resolving the
8233 returned URL results in the SALRS returning the service/agency locator record for the
8234 Wonderville police department. Note that if the ECRF is aware of more than one matching
8235 agency, it returns at least one <mapping> element for each agency.

8236 Service Names come from the Service Names registry (Section 10.11). The agency types
8237 are taken from the urn:emergency:service:responder registry (Section 10.5) and the

8238 subregistries defined for that registry. Note that for this function, the search for police is
8239 "urn:emergency:service:serviceagencylocator.police" and not
8240 urn:emergency:service:responder.police. The latter would return the SIP interface for the
8241 police department, where the former returns a Service/Agency Locator Record URI.

8242 **4.15.3 Service/Agency Locator Search by Name**

8243 A search for a service or agency in which the search key is a name is provided by the
8244 Service/Agency Locator Search Service. The Service is operated by the ESInet operator.
8245 The search function may return one or more Service/Agency Locator URIs, a referral to
8246 another Service/Agency Locator Search Service, or an error. The name that is searched
8247 comes from the Service Names Registry, Section 10.11, (for a service) or the first "org"
8248 element in the serviceAgencyJcard in the Service/Agency Locator Record (for an agency).

8249 HTTP method: GET

8250 Resource name .../LocatorRecordUris

8251 Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.
serviceAgencyName	MANDATORY	Name, or part of a name using wildcard notation

8252 A successful return includes a LocatorRecordURIArray consisting of:

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
locatorIds	MANDATORY	Array of LocatorRecordUri

8253 LocatorRecordUri consists of:

Name	Condition	Description
uri	MANDATORY	URI of ariLocator Record or another Service/Agency Locator
serviceAgencyName	MANDATORY	Name of Service or Agency whose URI is returned. May occur more than once
uriType	MANDATORY	Either "RecordUri" or "ReferralUri"

8254 Status Codes

8255 200 OK

8256 404 Not Found

8257 454 Unspecified Error

8258 To allow searches beyond the local ESInet, the Search Service is provisioned with other
8259 Search Services' URIs much like a Forest Guide.

8260 **Note:** A future version of this document will specify a more general way to connect the
8261 Service/Agency Locator Search Services.

8262 **4.15.4 Service/Agency Locator Record**

8263 The data returned by dereferencing a service/agency locator record URI is a JSON data
8264 structure containing the following elements:

Name	Condition	Use
recordId	MANDATORY	Id of this record at this S/AL
serviceAgencyId	MANDATORY	ServiceId or AgencyId of the Service or Agency
serviceAgencyName	MANDATORY	Official name of Service or Agency
serviceAgencyJcard	MANDATORY	Service operator or Agency Contact information. The name of the service or agency is found in the first 'org' field of the jCard.
serviceAgencyTypes	MANDATORY	Array of Service or Agency Type (psap, police, fire, ...)
emergencySipInterfaceUri	CONDITIONAL See Note 1	Interface where 9-1-1 SIP calls are accepted (Note 2)
adminLineUri	CONDITIONAL See Note 3	sip or tel: URI containing 10 digit admin line #, see Section 4.2.1.1.
loggingServiceUriArr	OPTIONAL See Note 4	Service or Agency Logging Service interface, see Section 4.12.1
eidoInterfaceUri	OPTIONAL See Note 5	EIDO Interface URI, See Section 4.12.1
mdsFeatureInterfaceUri	OPTIONAL	MappingDataService Web Feature Service interface
mdsImageInterfaceUri	OPTIONAL	MappingDataService Web Map Service interface
svcStateUri	CONDITIONAL	Service State Subscription URI for a service, such as the PSAP service.
dscRptSvc	OPTIONAL See Note 6	Discrepancy Report Service URI, see Section 3.7

Name	Condition	Use
headJcard	OPTIONAL	jCard of top agency or service operator official
onDutySuperJcard	OPTIONAL	jCard of supervisor on duty now

- 8265 Note 1: For all URIs, if the service or agency provides SIP service for handling emergency
8266 calls, the URI MUST be provided in the record. For example, if the agency accepts
8267 emergency calls transferred to it, it MUST provide the emergencySipInterface URI.
- 8268 Note 2: This URI MUST be provided and MUST be the same URI obtained from the SRV
8269 record for the SIP service for the domain of the service or agency. If there is any
8270 discrepancy, the SRV record SHOULD be used. This URI is also the same URI obtained
8271 directly from the ECRF for the appropriate service URN.
- 8272 Note 3: Not all agencies will have an admin line that accepts emergency calls. Not relevant
8273 for services.
- 8274 Note 4: Although unusual, not all agencies have a Logging Service.
- 8275 Note 5: Although unusual, not all agencies have an EIDO interface. Not relevant for
8276 services.
- 8277 Note 6: Although unusual, not all agencies or services have a Discrepancy Reporting
8278 Service.

8279 **4.15.5 Service/Agency Locator Inter-ESInet Index**

8280 A Service/Agency Locator may be aware of other Service/Agency Locators. It can ask those
8281 external Locators the names for which it has records, so that it can provide an appropriate
8282 referral when it gets a query for a name for which it does not provide records. This index
8283 can also contain records for names that the responding Locator has discovered using this
8284 mechanism.

8285 The number of agencies listed in a nationwide index could number 100,000-400,000
8286 agencies. As the response to this query can be quite large, "limit" and "start" parameters
8287 are available. The server treats all the names it knows (names for which it has records and
8288 names it has learned from other Locators) as a single list with the name, the URI of the
8289 Locator that has the record (which may be its own URI), and a simple index, which starts
8290 at one. The client specifies the maximum number of names it will accept in the response,
8291 and the starting index, which is one to retrieve records from the beginning. The response is
8292 a series of arrays of names prefaced by the URI of the Locator that has the record for that
8293 name. The index of the last name provided is also returned. The client can increment the
8294 last index by 1 and use that as the starting index for a subsequent call to the service. A
8295 status code is provided for the end of the list. The server MAY supply less than the number
8296 of names requested by the client in its response, but it MUST NOT supply more. The server

8297 may restrict this service to other Service/Agency Locators, which would be denoted in the
8298 PCA-issued credential.

8299 Discovering other Service/Agency Locators to use this function can be accomplished by
8300 provisioning but can be entirely automated by using the Search by Location function in
8301 Section 4.15.2. To do so, the Service/Agency Locator itself is a "Service", so the ECRF can
8302 be searched for the Service/Agency Locator for a location. In addition, Section 3.4.1
8303 requires the ECRF to return the entire service boundary for the Service/Agency Locator
8304 when queried by an entity with a credential traceable to the PCA. A Service/Agency Locator
8305 can then create a list of other Service/Agency Locators by querying by location for a
8306 Service/Agency Locator, say for a point in the middle of a state, and getting the service
8307 boundary of that Locator. It might cover the state, or it might cover a part of the state. If
8308 the latter, another search for a point in the state but outside the boundary of the initial
8309 Locator will get the URL of another Locator, and its service boundary, and repeating this
8310 will get all the Locators in the state. This sequence can be repeated for all states. This
8311 discovery function need only be done perhaps once a year as the boundaries do not
8312 change often, and when the name retrieval is executed, the service area of the Locator
8313 queried could be verified to see if it is the same as it was when the discovery sequence
8314 was completed. It is RECOMMENDED that a state level Service/Agency Locator be created
8315 which runs this procedure, and if there is a local or regional Service/Agency Locator, that it
8316 refer out of area queries to the state Service/Agency Locator which could provide referrals
8317 for any other Locators in the state or in any other state.

8318 HTTP method: GET

8319 Resource name .../NameSets

8320 Parameters:

Name	Condition	Description
limit	OPTIONAL	Maximum number of results to return
start	OPTIONAL	First item in the page of results, as an ordinal 1-based integer.

8321 A successful response returns a NameSetArray

Name	Condition	Description
count	MANDATORY	Number of items in the array
totalCount	MANDATORY	Total number of items found
nameSet	MANDATORY	Array of NameSet

8322 NameSet consists of:

Name	Condition	Description
locatorUri	MANDATORY	URI of Service/Agency Locator
names	MANDATORY	Array of Service/Agency Locator Names

8323 Status Codes

8324 200 OK

8325 404 Not Found

8326 441 Index beyond available names

8327 454 Unspecified Error

8328 **4.16 Policy Store**

8329 **4.16.1 Functional Description**

8330 A Policy Store holds policies created by an agency and used by a functional element such
8331 as an ESRP. The Policy Store is a simple repository; it does not manipulate the policy.

8332 **4.16.2 Interface Description**

8333 A Policy Store implements the policy storage and retrieval functions defined in Section
8334 3.3.1. Policy Store replicas can be maintained by having one Policy Store retrieve policies
8335 from another Policy Store and subsequently accept requests to retrieve such policies.
8336 Replicas normally do not allow a Policy Store operation for a policy that they replicate.
8337 There is always one (possibly redundant) authoritative Policy Store for a given policy.

8338 **4.16.3 Roles and Responsibilities**

8339 Any agency may operate a Policy Store. While it is permissible for an element to contain a
8340 Policy Store that it uses, it normally is not authoritative, but rather a replica of the policy.
8341 The element must have a mechanism for retrieving the policy from the authoritative source
8342 rather than using the internally stored replica, if provisioned to do so.

8343 **4.17 Time Server**

8344 The ESInet MUST provide an NTP service for time of day information. The service may
8345 have a hardware clock, or may be synchronized to another NTP time service provided that
8346 there are sufficient backups so that if the ESInet is isolated from its time source, it can
8347 provide local time. Time accuracy MUST be within 1 ms of true time. Agencies MAY have
8348 their own time server, which MAY have a hardware clock if it is more accurate than syncing
8349 the server to the ESInet time server.

8350 **4.18 Originating networks and Devices**

8351 A device, network, or service provider presenting calls to an ESInet is expected to support
8352 the following interfaces. The manner in which the originating network, device, or service
8353 arranges its emergency calling services to meet this standard is beyond the scope of this
8354 document.

8355 **4.18.1 SIP Call Interface**

8356 The originating network is expected to present calls to the ESInet meeting the ESInet SIP
8357 interface specified in Section 3.1. All calls will be signaled with SIP, MUST contain a
8358 Geolocation header field, except if they are calls to an administrative number, and MUST
8359 be routed by the ECRF, or an equivalent function that produces the same result, using the
8360 location contained in, or referenced by the Geolocation header field.

8361 **4.18.2 Location by Reference**

8362 Originating networks that are also access networks are expected to also provide a Location
8363 Information Server function (i.e., location dereference, and location validation if applicable)
8364 meeting the requirements of Section 4.10, if they supply location by reference.

8365 **4.18.3 Additional Data Repository**

8366 Originating networks and devices presenting calls to ESInets are expected to provide an
8367 Additional Data Repository interface meeting the requirements of Section 4.11 unless they
8368 always send Additional Data by value.

8369 **4.19 Mapping Data Service (MDS)**

8370 When answering calls out of area, the answering PSAP needs to be able to display an
8371 appropriate map covering the area in which the caller is located, just as if the call was
8372 received from an in-area caller. Today, if a call is answered locally, or even in a
8373 neighboring PSAP, the data needed to construct a map is available locally. However, if a
8374 call was answered in a totally different PSAP, one which does not have a mutual aid
8375 agreement, for example, the answering PSAP likely would not have the GIS data from the
8376 serving PSAP to construct a map. The Mapping Data Service (MDS) provides this capability.
8377 In addition, it is often desirable for all elements within a PSAP that need to display a map
8378 to have the same display as other elements which display maps, and differences between
8379 implementations of multiple elements are often significant, which makes training and use
8380 complicated. The MDS MAY be used by all elements within a PSAP to show consistent
8381 displays, but it is not a requirement of this standard that they do so.

8382 All PSAPs MUST have an MDS available to hold their data. The MDS MAY be shared. The
8383 MDS MUST be provisioned with GIS data from the layers that are provisioned to the ECRF

[MM/DD/YYYY]

Page 299 of 675



as well as layers defined in the NG9-1-1 GIS Data Model [184] that are not included in Appendix B. The service can return a set of GIS features from a specified set of layers within a lat/long bounding box using the Web Feature Service (WFS) [93], or it can return an image file rendered from a similar set of features with a similar input specification plus a "viewport"⁵⁰ specified by the number of pixels in X and Y using the Web Map Service (WMS) [186]. The MDS supports both interfaces, and clients may choose which one to use. Note that if the WFS interface is used, the client receives a set of features and it determines what the map looks like. If WMS is used, the MDS determines what the map looks like.

The querier may specify which layers it wishes to receive in the return feature set or image. For this purpose, a registry listing every layer that could be supported by the MDS is defined in Section 10.32. A given GIS system may not have every layer defined in the registry and thus the return feature set or images may be a subset of the layers requested.

The MDS for a given location is discovered with the Service Locator function. It is queried with one of two Web Service interfaces: a Web Feature Service (WFS) interface for features and Web Map Service (WMS) for images as defined below.

The MDS MUST offer a Web Feature Service Version 2.0.2 [93]. The WFS MAY support:

- Insert, Update, or Delete operations
- Transaction/lock capability
- Stored queries
- Filters (other than BBOX)

The WFS MUST support GML 3 output format. Other formats MAY be supported.

The MDS MUST offer a Web Map Service Version 1.3.0 [186]. The WMS MUST support the EPSG:4326 Coordinate Reference System (CRS) [187] and MAY support others for each layer it provides. The WMS MUST support a PNG output file format and MAY support others. The WMS MUST support at least 15 layers and MaxWidth and MaxHeight of at least 2048. The WMS must be capable of supporting every layer defined by the NENA Standard for GIS Data Model, NENA-STA-006.1-2018 [184], although the WMS may not be provisioned for every layer in every area it supports and thus MAY not be able to respond to a request for a layer for which it has no data. It MAY support other layers. The layer name MUST be the layer name as defined in the NENA Standard for NG9-1-1 GIS Data Model [184].

⁵⁰ The visible area on a screen where an image is rendered. Usually specified as the X and Y pixel location of two opposite corners, or the X and Y pixel location of one corner and a height and width, the viewport is the destination of a rendering operation such as rendering a part of a map onto a display.

8416 To maintain a local copy of the MDS, the PSAP could obtain the SI feed to its data. It could
8417 also obtain SI feeds from the data provider of any neighboring MDS.

8418 No common style definition is provided in this edition. A future edition may provide a
8419 common style definition to improve uniform display of WMS data.

8420 **4.20 Outbound Call Interface Function (OCIF)**

8421 The Outbound Call Interface Function is part of the NGCS and responsible for handling calls
8422 originating from i3-PSAPs over their serving ESInet/NGCS. The OCIF is used to process
8423 callbacks as well as other outgoing calls that transit the ESInet (e.g., official calls from one
8424 Public Safety agency to another, perhaps on a different ESInet), including admin calls
8425 promoted to emergency calls. The OCIF is on the border of the ESInet. It allows traffic
8426 outbound to another PSAP hosted on the same ESInet. It also allows traffic outbound from
8427 the serving ESInet to interconnected networks⁵¹. The OCIF MUST NOT allow any calls or
8428 other SIP operations inbound from any source to entities inside the ESInet. An OCIF MAY
8429 include a Session Border Controller as part of its functionality.

8430 The OCIF operates as a SIP proxy server (or B2BUA in some circumstances), routing
8431 callbacks to an interconnected network, which will ultimately forward the call toward the
8432 caller's device, possibly via one or more other networks. The NGCS provider MUST have an
8433 IP-based Network-to-Network Interface (IP-NNI) with one or more interconnected network
8434 providers to facilitate callbacks routed via the OCIF. Note that other outgoing calls initiated
8435 by a PSAP, such as those destined for another agency, may also transit the ESInet. Such
8436 calls will also be processed by the OCIF. In addition, outbound ESInet calls destined to the
8437 PSTN MUST go through the OCIF, which will interwork SIP to SS7 through a standard PSTN
8438 Gateway⁵². Alternatively, OCIF PSTN access COULD be provided by an interconnected
8439 network provider. In such case, the SIP to SS7 interworking will be provided by the
8440 interconnected network provider.

8441 The OCIF MUST support all media types listed in this standard. All callbacks MUST be
8442 marked with the value "psap-callback" in the Priority header field as documented in RFC
8443 7090 [141].

51 Interconnected networks include directly connected originating networks, transit networks, and other ESInets.

52 Technical details of the PSTN Gateway function and its legacy interface to the PSTN are outside the scope of this document.

8444 The ESRP MAY be used to route callbacks and other outgoing calls from a PSAP toward the
8445 OCIF. If included in the call path, the ESRP SHALL route the outgoing call to the OCIF. The
8446 OCIF SHALL forward the call to the appropriate interconnected network.

8447 SIP INVITE messages for callbacks destined to be routed through an OCIF MUST contain:

- 8448 1. A Request-URI line containing the callback URI;
- 8449 2. A To header field populated with the callback URI. Usually the value is the content of
8450 the P-A-I (preferred, if present) or From header field of the original emergency call;

8451 **Note:** The callback URI MUST contain a dialable telephone number either expressed as
8452 a national 10-digit NANP number or as an international number following ITU-T
8453 Recommendation E.164 and, if expressed as a sip URI, the domain part SHALL
8454 represent the home network of the target. If the original emergency call was from a
8455 non-service initialized handset, the callback number of the form "911 plus the last 7
8456 digits of the ESN or IMEI expressed as a decimal" is not dialable and therefore
8457 MUST NOT be used for callback.

- 8458 3. A From header field containing `sip:TN@<psapdomain>;user=phone`, which SHOULD
8459 be the same value as in the P-A-I header field;

8460 **Note:** The OCIF MUST support receipt of outgoing calls from PSAPs marked for
8461 presentation restriction of caller ID expressed by the presence of a Privacy header
8462 field (RFC 3323 [207], expanded by RFC 3325 [16] and RFC 7044 [35]) and the
8463 From header field value populated with "Anonymous"
8464 `sip:anonymous@anonymous.invalid`;

- 8465 4. A Route header field populated with a routing URI that should contain the "lr"
8466 parameter to avoid Request-URI rewriting (the INVITE from the PSAP MAY contain
8467 the outgoing ESRP, or, if ESRPs are not used to route callbacks in the ESInet
8468 originating the callback, the OCIF URI. An INVITE from an ESRP to the OCIF SHALL
8469 contain the OCIF URI. The INVITE from the OCIF to the interconnected network
8470 SHALL contain the well-known URI associated with that network);
- 8471 5. A SIP Priority header field with "psap-callback" as the value;
- 8472 6. A Resource-Priority header field with "esnet.0" as the value;
- 8473 7. A P-Asserted-Identity header field containing `sip:TN@<psapdomain>;user=phone`,
8474 where the TN is associated with the PSAP originating the call, and can be asserted
8475 by an Secure Telephone Identity Authentication Service (STI-AS) function;
- 8476 8. A second P-Asserted-Identity header field containing the identity of the agent
8477 originating the call expressed as `sip: "agent name" <agentID@agencyID>`;

8478 **Note:** The Display Name part is OPTIONAL;

[MM/DD/YYYY]

Page 302 of 675



8479 9. An SDP offer containing all media supported at the PSAP. The SDP SHOULD include
8480 offers matching the negotiated SDP from the original emergency call, placing the
8481 SDP that was used as the top-most value in the list;

8482 The OCIF processing a callback INVITE constructed as above will interact with the STI-AS
8483 FE to assert the telephone identity of the caller. Once the assertion and signing process is
8484 completed, the OCIF will receive the INVITE back with an added SIP Identity header field
8485 constructed per RFC 8224 [60], using the NGCS provider's credentials as the signing
8486 authority for the PSAP telephone identity.

8487 **Note:** The INVITE message received back from the STI-AS MUST be constructed in such a
8488 way that the OCIF will recognize it as a "spiral" as defined in RFC 3261 [10], if the OCIF
8489 has loop detection enabled.

8490 SIP INVITE messages for other outgoing calls that transit the ESInet through an OCIF
8491 MUST contain:

- 8492 1. A Request-URI line containing the target URI;
8493 2. A To header field populated with the target URI, as determined by the initiating
8494 PSAP;

8495 **Note:** The target URI MUST contain a dialable telephone number either expressed as a
8496 national 10-digit NANP number or as an international number following ITU-T
8497 Recommendation E.164, or a sip URI that is routable within the ESInet, where the
8498 domain part represents the home network of the target.

- 8499 3. A From header field containing sip:TN@<psapdomain>;user=phone, which SHOULD
8500 be the same as in the P-A-I header field;

8501 **Note:** The OCIF MUST support receipt of outgoing calls from i3-PSAPs marked for
8502 presentation restriction of caller ID, expressed by the presence of a Privacy header
8503 field (RFC 3323 [207], expanded by RFC 3325 [16] and RFC 7044 [35]) and the
8504 From header field value populated with "Anonymous"
8505 sip:anonymous@anonymous.invalid;

- 8506 4. A Route header field populated with a routing URI that should contain the "lr"
8507 parameter to avoid Request-URI rewriting (the INVITE from the PSAP MUST contain
8508 the outgoing ESRP. The INVITE from the ESRP to the OCIF SHALL contain the OCIF
8509 URI. If the INVITE from the OCIF is to an interconnected network, it MAY contain
8510 the well-known URI associated with that network);

- 8511 5. A Resource-Priority header field populated with an appropriate value based on
8512 section 3.1.7 (e.g., "esnet.0" or "esnet.2") as determined by the originating PSAP;

- 8513 6. A P-Asserted-Identity header field containing `sip:TN@<psapdomain>;user=phone`,
8514 where the TN is associated with the PSAP originating the call and can be asserted by
8515 an STI-AS function;
8516 7. A second P-Asserted-Identity header field containing the identity of the agent
8517 originating the call expressed as `sip:"agent name"<agentID@agencyID>`;
8518 **Note:** the Display Name part is OPTIONAL
8519 8. An SDP offer containing all media supported at the PSAP;
8520 The OCIF processing an outgoing INVITE constructed as above will interact with the
8521 STI-AS FE to assert the telephone identity of the caller. Once the assertion and signing
8522 process is completed, the OCIF will receive the INVITE back with an added SIP Identity
8523 header field constructed per RFC 8224 [60], using the NGCS provider's credentials as the
8524 signing authority for the PSAP telephone identity.
8525 **Note:** The INVITE message received back from the STI-AS MUST be constructed in such a
8526 way that the OCIF will recognize it as a "spiral" as defined in RFC 3261 [10], if the OCIF
8527 has loop detection enabled.
8528 The OCIF service interfaces are SIP/RTP based and MUST conform to sections 3.1 and
8529 3.1.9. The generic SIP interface from the OCIF to an interconnected network MUST
8530 conform to the definition of the SIP interface as defined in Section 3.1, except:
8531 1. The Request-URI line MUST NOT contain an "sos" service URN;
8532 2. The Geolocation and Geolocation-Routing header fields MUST NOT be used;
8533 3. The P-Asserted-Identity header field MUST be present and populated with a value
8534 that can be asserted through an STI-AS function;
8535 4. P-type headers other than P-A-I are OPTIONAL;
8536 5. No purpose for the Call-Info header field is yet defined;
8537 6. Header fields listed in Section 3.1.6 MAY be used.
8538 The OCIF MAY, based on local policy, add a P-Charge-Info header field (RFC 8496 [208])
8539 and/or a P-Charging-Vector header field (RFC 7315 [209]) on the outgoing INVITE.
8540 The OCIF has a SIP interface to the STI-AS FE (see section 4.21.3) for the purpose of
8541 asserting and digitally signing the telephone identity (i.e., the telephone number) of PSAP-
8542 originated outbound calls. The OCIF invokes the STI-AS FE for any call presented to it after
8543 call processing has completed, that is, after the destination interconnected network has
8544 been determined.
- 8545 **4.21 Secure Telephone Identity (STI)**
8546 The Secure Telephone Identity (STI) Authentication Service is an NGCS functional element
8547 that provides caller identity assertion for callbacks and other PSAP-originated outbound

[MM/DD/YYYY]

Page 304 of 675



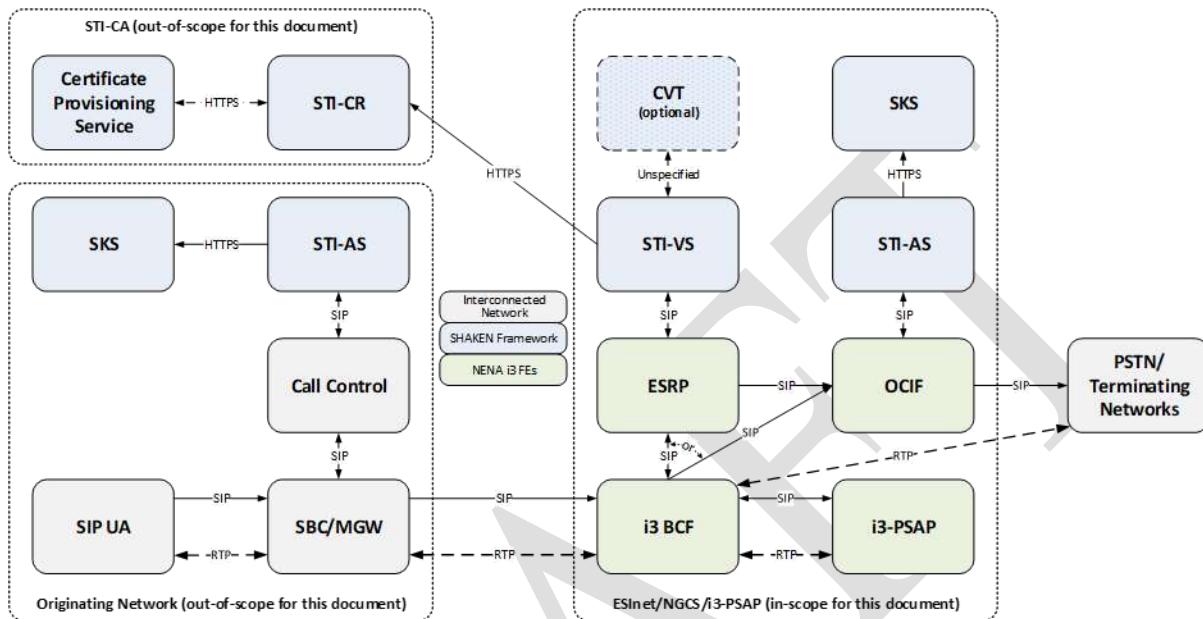
calls. The STI Verification Service is an NGCS functional element that provides verification services applicable to emergency calls destined for i3 PSAPs. Both the Secure Telephone Identity Authentication Service (STI-AS) and the Secure Telephone Identity Verification Service (STI-VS) FEs are defined by the SHAKEN framework as specified in ATIS-1000074-E (errata) [210]. The STI-AS and STI-VS FEs adhere to ATIS-1000074-E (errata) unless otherwise specified herein.

The SHAKEN reference architecture specified in ATIS-1000074-E (errata) also includes the Call Validation Treatment (CVT) and Secure Key Store (SKS) elements.

For emergency calls, the STI-VS FE provides the results of the verification process to downstream entities to help detect potential telephone scams using spoofed telephone numbers such as SWATting, prank calls and illegitimate robocalling. For PSAP-originated outbound calls, including callbacks, the STI-AS FE asserts and cryptographically signs the telephone identity of the caller, allowing PSAP-originated calls to be validated by the networks these calls transit through (if they support such capabilities), and for the home network performing the verification to present the called party with an indication of the validity of the calling telephone number (if it supports such capabilities). Calls with a validated telephone identity have a higher chance of completing at the called party, which is an important feature for emergency callbacks.

8566 The STI-AS and STI-VS FEs interconnect with NGCS as per the following diagram.

8567



8568

Figure 21 - NGCS-STI Interconnection Architecture

8570 The STI-VS FE supports caller identity validation for emergency 9-1-1 calls presented to the
8571 ESInet/NGCS (forward path) and the STI-AS FE supports i3 PSAP-originated caller identity
8572 assertion for outbound calls transiting through the ESInet/NGCS (reverse path), such as
8573 emergency callback calls. The STI-VS FE interacts with the ESRP for inbound emergency
8574 calls and the STI-AS FE interacts with the OCIF for outbound calls originated from i3-PSAPs
8575 and transiting the ESInet.

8576 **Note:** This document does not impose any requirements on Originating Networks to
8577 support STIR and SHAKEN. It defines the procedures an NGCS SHALL apply to 9-1-1
8578 emergency calls that are presented with SHAKEN-compliant signaling in order to provide
8579 caller identity verification services to i3 PSAPs, as well as caller identity assertion services
8580 for calls originating from i3 PSAPs over the ESInet/NGCS and presented to interconnected
8581 networks for verification, if supported by such networks.

8582 The STI-VS FE and the STI-AS FE MUST implement a logging interface as per Section 4.12.

8583 **Note:** All transactions and every message sent and received via the service interfaces
8584 MUST be sent to the Logging Service.

8585 Each STI server MUST implement the server-side of the ElementState event notification
8586 package, including its sub-components.

[MM/DD/YYYY]

Page 306 of 675

8587 The STI-VS FE and the STI-AS FE MUST implement the server-side of the ServiceState
8588 event notification package, including its sub-components.

8589 **Note:** The concept of Secure Telephone Identity is nascent. As such, it is expected that
8590 the referenced standards will evolve. A future version of this document will ensure
8591 alignment with the evolution of these standards, when appropriate.

8592 **4.21.1 STI Verification for Emergency 9-1-1 Calls**

8593 The STI-VS FE is invoked by the ESRP before call processing has completed; that is, before
8594 applying Origination Policies.

8595 For emergency 9-1-1 calls presented to the ESInet/NGCS with an Identity header field
8596 populated as per RFC 8224 [60], the procedures defined in ATIS-1000074-E (errata) for
8597 the STI-VS SHALL be applied with the following clarifications.

- 8598 • If the To header received by the STI-VS in the incoming INVITE message contains a
8599 URI that can be interpreted as "911" or an sos service urn (e.g., urn:service:sos),
8600 the content of the To header in the received INVITE does not match the "dest" claim
8601 in the PASSporT, and the "dest" claim in the PASSporT is something other than a
8602 URI that can be interpreted as "911" or an sos service URN, the "dest" claim
8603 verification SHALL be considered failed;
- 8604 • If the To header received by the STI-VS in the incoming INVITE message contains a
8605 URI that can be interpreted as "911" or an sos service urn (e.g., urn:service:sos),
8606 the content of the To header in the received INVITE does not match the "dest" claim
8607 in the PASSporT, and the "dest" claim in the PASSporT contains a URI that can be
8608 interpreted as "911" or an sos service URN, the "dest" claim verification SHALL be
8609 considered passed;
- 8610 • If the Request-URI and the To header field contain a URI that can be interpreted to
8611 be "911", the "dest" claim verification procedure SHALL be considered passed if a
8612 match is found;
- 8613 • If the Request-URI is a service URN (e.g., urn:service:sos)⁵³ and the To header field
8614 contains a URI that can be interpreted to be "911", the "dest" claim verification
8615 procedure SHALL be considered passed;
- 8616 • If the Request-URI and the To header field value contain a service URN (e.g.,
8617 urn:service:sos)⁵⁴, the "dest" claim verification procedure SHALL be performed and
8618 considered passed if a match is found;

53 Additional work outside of NENA is in progress to support this scenario

54 Additional work outside of NENA is in progress to support this scenario

- 8619 • Emergency 9-1-1 calls MUST always be progressed forward regardless of the
8620 success or failure of the verification process. If the verification process fails, the STI-
8621 VS FE MUST include the error response code and a reason phrase in a Reason
8622 header (RFC 3326 [18]) field added to the next response (provisional or final) back
8623 to the Originating Network. The STI-VS FE MAY issue a Discrepancy Report to the
8624 Originating Network as per section 3.7.14;
8625 • Emergency calls that include a Resource-Priority header field populated with a value
8626 from the “esnet” namespace SHOULD be passed to the CVT⁵⁵, if this component is
8627 available from the NGCS provider.

8628 Upon having completed its verification steps, the STI-VS SHOULD invoke the CVT, if
8629 available. The processing performed by the CVT and the interface used to convey the
8630 results of that processing are left to implementations.

8631 For the calling number, the STI-VS FE MUST add the “verstat” parameter to the P-
8632 Asserted-Identity header field or From header field to convey the results of the verification
8633 and forwards the call to the ESRP on the same queue the call originally arrived on. The
8634 ESRP then processes the call as per its normal procedures i.e., applying Origination
8635 Policies, ECRF query, etc.

8636 **4.21.2 STI Authentication for PSAP-Originated Calls.**

8637 The STI-AS FE is invoked by the OCIF after call processing has completed, that is, after the
8638 interconnected network has been determined.

8639 The STI-AS functions as described in ATIS-1000074-E (errata) [210], and the output is a
8640 cryptographically signed Personal Assertion Token (PASSporT) as defined in RFC 8225
8641 [203], inserted in an Identity header field as per RFC 8224 [60] in the outgoing SIP INVITE
8642 message.

8643 **4.21.3 Call Validation Treatment**

8644 The Call Validation Treatment (CVT) is an optional, value-add FE providing call spam
8645 analytics and possibly other mitigation techniques. It interacts with the STI-VS and returns
8646 a response that influences what should be signaled to the called party for a legitimate or
8647 illegitimate call.

8648 ATIS-1000074-E (errata) [210] provides a high-level view of the CVT FE. However, its
8649 interfaces and detailed specifications are purposely not defined and left to the vendor
8650 community to specify. It is included here for alignment with the ATIS standard.

55 Additional work outside of NENA is in progress to support this scenario.

8651 **4.21.4 STI Secure Key Store**

8652 The STI Secure Key Store (STI-SKS) FE provides a highly secure storage for private keys to
8653 be used for cryptographically signing SIP INVITE messages presented to the STI-AS FE. It
8654 interacts with, or is part of, the STI-AS FE.

8655 ATIS-1000074-E (errata) [210] provides a high-level view of the STI-SKS FE, with further
8656 details related to the management of STI certificate/key management provided in ATIS-
8657 1000080-E [211]. The NGCS STI-SKS SHALL store keys in a FIPS-PUB-140-3 [67] level 3 or
8658 higher key store. Certificates for signing keys SHALL be signed directly by the root key.

8659 **Note:** It is an objective that the NGCS' root signing keys will be traceable to the PCA, and
8660 the PCA's certificate will be cross signed by the ATIS STI Certificate Authority.

8661 **4.22 Incident Data eXchange (IDX)**

8662 The Incident Data eXchange (IDX) functional element collects Emergency Incident Data
8663 Objects (EIDOs). The IDX receives requests for EIDOs and puts the information together. A
8664 detailed description of IDX functionality/interfaces will be part of a future version of this
8665 document.

8666 **5 Security**

8667 This section contains information about specific considerations for this Standard. For other
8668 security considerations, see NENA 75-001 [231].

8669 **5.1 Identity**

8670 Each agency and each agent in an agency are issued credentials that allow them to be
8671 identified to all services in the ESInet. An agency identifier is a globally unique FQDN (such
8672 as "erie.psap.ny.us"), which appears in the SubjectAltName of an X.509 [144] certificate
8673 issued to the agency. The agency assigns identities to an agent. The identity for an agent
8674 is a string containing a userpart which is unique to the agent within the agency, an "@",
8675 and the FQDN of the agency. For example: "nancy@erie.psap.ny.us". This string appears in
8676 the SubjectAltName of an X.509 certificate issued to the agent. See Identifiers in Section
8677 2.1.

8678 For PSAPs and 9-1-1 Authorities, the root Certificate Authority for agent and agency
8679 certificates is the PSAP Credentialing Agency (PCA). The certificate can be issued directly
8680 by the PCA, or the PCA can issue a certificate to an agency that, in turn, issues certificates
8681 to other agencies or agents. It is recommended that a state PCA be created for each state,
8682 with the national PCA signing the state PCA certificate, and the state PCA signing 9-1-1
8683 Authority and PSAP certificates. 9-1-1 Authorities or PSAPs may sign the certificate of their
8684 agents.

[MM/DD/YYYY]

Page 309 of 675



8685 Operating a CA requires the creation of, and strict adherence to, a Certificate Policy and
8686 Practice Statement (CP/CPS) [59]. A CP/CPS includes strict specifications for vetting: who
8687 gets a certificate, under what conditions they get a certificate, and what proof of identity is
8688 needed before a certificate can be issued. If an agency cannot reasonably control its
8689 certificate issuing mechanisms it SHOULD contract to an entity that can provide strong
8690 controls and strict adherence to a suitable CP/CPS. NENA foresees that other agencies such
8691 as police, fire, and EMS agencies will need a similar Public Key Infrastructure (PKI), and it
8692 may be that, for example, a county level agency provides the Certificate Authority for all
8693 agents in the county.

8694 Great care MUST be taken to protect private keys. Key storage options are defined in FIPS-
8695 140-2 [67] agency keys MUST be protected with at least LEVEL 2, and LEVEL 3 is highly
8696 recommended. CA keys for agency CAs MUST meet LEVEL 3 requirements. State and
8697 National CA keys MUST be stored in a LEVEL 4 device.

8698 The identities, and the credentials, MUST be presented to gain access to ALL services and
8699 data in the ESInet.

8700 **5.2 PSAP Credentialing Agency**

8701 The PCA CP/CPS MUST be in conformance with the minimum standards included in this
8702 document. Any agency or agent may obtain a certificate from the PCA through the
8703 appropriate CA for that jurisdiction. Prior to the PCA being available in a given jurisdiction,
8704 NG9-1-1 implementations SHOULD accept credentials issued by any certificate authority
8705 listed in the current Mozilla Certificate Store (<https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/>).

8707 **5.3 Roles**

8708 When authenticating within the ESInet, an agent or agency assumes one or more roles.
8709 The roles which an agent or agency may assume are limited by policy of the immediately
8710 superior agency. The Role is contained in the X.509 certificate of the agency or agent.

8711 Agency Roles defined within this specification are:

- 8712 • PSAP per NENA ADM-000 Master Glossary: "... responsible for receiving 9-1-1 calls
8713 and processing those calls according to a specific operational policy."
- 8714 • Dispatch per ANS1.107.1.2015 "... alerting and directing the response of public
8715 safety responders to the desired location".
- 8716 • 9-1-1 Authority – per NENA ADM-000 Master Glossary: "... governmental entity
8717 responsible for 9-1-1 service operations.
- 8718 • ESInet Service Provider – The entity responsible for the operation of an Emergency
8719 Services IP Network.

- 8720 • ESRP Service Provider – The entity responsible for the operation of an Emergency
- 8721 Service Routing Proxy
- 8722 • ECRF/LVF Service Provider – The entity responsible for the operation of an
- 8723 Emergency Call Routing Function/Location Validation Function.
- 8724 • LIS Service Provider – The entity responsible for the operation of a Location
- 8725 Information Server.
- 8726 • Any responder agency listed in the “urn:emergency:service:responder” Registry (see
- 8727 Section 10.5).
- 8728 • Agency Role modifier are scopes that can be applied to the above agency roles to
- 8729 further clarify the extent of the authority:
 - 8730 ○ National
 - 8731 ○ State
 - 8732 ○ Regional
 - 8733 ○ Local

8734 A registry for Agency Roles is defined. See Section 10.27. While ESInet implementations
8735 may define other roles for agencies, it is RECOMMENDED that the policies of the ESInet
8736 provide 100% functionality without additional roles so that availability of resources is
8737 maximized when disaster situations occur and other ESInets and agencies are providing
8738 services to the PSAPs. In the same vein, all ESInets MUST have agencies that assume all of
8739 the above roles.

8740 Agent Roles defined in this specification are:

- 8741 • Dispatching Role – per ANSI.107.1.2015 “... alerting and directing the response of
- 8742 public safety responders to the desired location”.
- 8743 • Call Taking Role – per ANSI.107.1.2015 “... processes incoming calls through the
- 8744 analyzing, prioritizing, and disseminating of information to aid in the safety of the
- 8745 public and responders”.
- 8746 • GIS Analysis Role – assembles and maintains geospatial and addressing information.
- 8747 • IP Network Administration Role – monitors, manages, and controls network
- 8748 elements and services (e.g., switches, routers, gateways, firewalls, and network
- 8749 services such as DNS and DHCP); plans for and responds to service outages and
- 8750 other problems.
- 8751 • Database Administration Role – installs, configures, manages, monitors, and controls
- 8752 access to databases.
- 8753 • IT Systems Administration Role – installs, configures, supports, and maintains
- 8754 system hardware, operating systems, application elements and services; plans for
- 8755 and responds to service outages and other problems.
- 8756 • Application Administration Role – installs, configures, supports, and maintains
- 8757 applications; plans for and responds to service outages and other problems.

- 8758 • Security Administration Role – creates, assigns, configures, maintains, and supports user authentication and authorization elements and services; monitors for possible security violations and vulnerabilities, and ensures that vulnerabilities are corrected.
- 8759 • Records Production Role – searches for, retrieves, and reproduces records and recordings for internal and external uses, including FOIA requests, subpoenas, and media requests.
- 8760 • Data Analysis Role – researches and analyzes specific kinds of data to identify trends, anomalies, and conditions important to supporting emergency services.
- 8761 • Quality Assurance Evaluation Role – per ANSI.1.107.1.2015 "... reviews telecommunicator work performance and documents an evaluation of the level of compliance with Agency directives and standards".

8762 Role Modifiers (may be added to further specify the above roles):

- 8763 • Management Role
- 8764 • Supervision Role
- 8765 • Trainer Role
- 8766 • Trainee Role
- 8767 • Assistant Manager
- 8768 • Shift Supervisor (to include Dispatch, Call Taking or a combination of both)
- 8769 • Dispatcher
- 8770 • Call taker
- 8771 • GIS Specialist
- 8772 • GIS Supervisor
- 8773 • Maintenance Supervisor
- 8774 • Maintenance Technician
- 8775 • Temporary Technician
- 8776 • ESInet Network Operator
- 8777 • ESInet Network Operations Supervisor
- 8778 • 9-1-1 Authority Director
- 8779 • 9-1-1 Authority Agent
- 8780 • Database Administrator
- 8781 • IT Systems Analyst
- 8782 • Records Production Specialist

8783 Specific definitions of these roles will be provided in a NENA Information Document to be referenced in a future version of this document. A registry of Agent Roles is defined. See Section 10.28.

8793 **5.4 Authentication**

8794 Authentication of Agents accessing elements described in this document MUST be
8795 implemented with a universal Single Sign On (SSO) paradigm. The mechanism used is
8796 OASIS SAML (Security Assertion Markup Language). There are two entities: an Identity
8797 Provider (IDP) which authenticates users and supplies the other party with a "token" that
8798 can be used in subsequent operations to refer to an authorized user, and a Relying party
8799 which uses the token. SAML is used by a Relying Party to ask if a user should be permitted
8800 to perform an operation. Agents in PSAPs and Responder Agencies, as well as other service
8801 agencies with agents use the SSO mechanism for all operations requiring agent
8802 authorization. In this document, the only mechanism defined that uses these tokens is the
8803 Authorization and Data Rights Management mechanism, but any application or service that
8804 uses Agents SHOULD use this mechanism for any authentication and authorization
8805 decisions for Agents. For establishment of TLS sessions between agents and elements, the
8806 SSO mechanism is used to authenticate the agent, which is then used to unlock the private
8807 key for that agent, and the key is used (together with its accompanying X.509 certificate)
8808 to establish the TLS session.

8809 For applications that depend upon interactions with Agents, several profiles of the Security
8810 Assertion Markup Language Version 2 [58] as amended by errata shall be used. SAMLv2, is
8811 an XML-based framework for describing and exchanging security information.

8812 SAMLv2 consists of a suite of core specifications, which outline schema and protocols [58],
8813 transport bindings [127], and a set of concrete profiles [128], which carefully orchestrate
8814 bindings and message patterns for SAML processors to discover SAML authorities and
8815 relying parties, as well as to request, produce, send, and receive SAML assertions. Also
8816 specified are the publication and discovery mechanisms for entity metadata [129]
8817 necessary for bootstrapping interactions between parties.

8818 For HTTP-bound NG9-1-1 web applications, the following existing SAMLv2 profiles MUST be
8819 supported by both asserting parties (i.e., IDP) and relying parties (i.e., RP), as specified in
8820 [128]:

- 8821 • Web Browser SSO Profile
- 8822 • Identity Provider Discovery Profile
- 8823 • Single Logout Profile.

8824 In addition, the following profiles MAY be supported:

- 8825 • Enhanced Client or Proxy (ECP) Profile
- 8826 • Artifact Resolution Profile.

8827 The Web Browser SSO Profile outlines the exchanges for requesting and producing SAMLv2
8828 assertions, in the presence of a web browser-based user-agent, which is used as the

8829 intermediary transport agent for these request, via orchestrated HTTP 302 redirects. For
8830 systems that use a client application to authenticate a user, the X500 profile of [128] is
8831 used.

8832 The Identity Provider Discovery Profile provides a mechanism for enabling the discovery of
8833 authentication authorities by means of a shared HTTP cookie, which carries an
8834 enumeration of IDPs to which the client is capable of authenticating. It is RECOMMENDED
8835 that this be the primary means for IDP discovery for an actor. Providers are identified by a
8836 URI as defined above.

8837 Most SIP and HTTPS sessions covered by this document are server to server. Some involve
8838 a client which is an agent (and thus not a server), but all agents, agencies and elements
8839 have credentials with certificates traceable to the PCA which can be used with mutual
8840 authentication methods. Mutual Authentication MUST be used for TLS and SIP session
8841 establishment using a certificate traceable to the PCA.

8842 **Note:** The mechanism used to implement the SSO requirement may change in version 4 of
8843 this document. OpenID is under consideration as a mechanism.

8844 5.5 Trusting Asserting and Relying parties

8845 In order for entities within the NENA infrastructure to be strongly identified in this
8846 federated authentication architecture, and for the proper run-time provisioning of new
8847 entities within the infrastructure, SAML metadata XML instances, as defined by [129], of
8848 each entity SHOULD be aggregated into a single XML instance using the
8849 <EntitiesDescriptor> container. This aggregated metadata document MUST be signed (via
8850 XML Signature) by an identified administrative body, using a well-known signing certificate.
8851 Thus, any entity (and the encryption and signing keys) contained within the
8852 <EntityDescriptor> element is identified as an authorized party to the infrastructure.

8853 Within this framework, each identity provider MUST insist on two-factor authentication of
8854 agents. The factors defined are:

- 8855 • Passwords, which must conform to local password policy;
- 8856 • Tokens (RSA SecurID);
- 8857 • Smart Cards conforming to ISO/IEC-7816 (1-15) [157];
- 8858 • Biometrics, including fingerprints, palm prints, retina scans, facial recognition, and
8859 voice recognition.

8860 It is RECOMMENDED that all authentication services enroll agents with as many factors as
8861 practical and allow any specific authentication to use any two. At present, there are no
8862 widely accepted standards for biometric information. Consequently, biometric
8863 authentication would only work when the authentication server and enrollment server use
8864 the same brand of scanner. Furthermore, if network access to the authentication data is

[MM/DD/YYYY]

Page 314 of 675



8865 lost, biometric authentication may not work. All agencies SHOULD have backup
8866 mechanisms (such as smart cards) available for local authentication when network access
8867 is unavailable.

8868 Protocol operations use RSA-2048 (see RFC 8017 [158]) with the credentials rooted in the
8869 PCA, typically over TLS. All elements in the ESInet MUST accept RSA-2048 with a certificate
8870 rooted in the PCA. They MAY accept alternate authentication cryptosystems as long as they
8871 are at least as strong as RSA-2048. RSA-2048 MUST be supported by all implementations.

8872 All protocol exchanges across the ESInet SHOULD be authenticated.

8873 **5.6 Authorization and Data Rights Management**

8874 Authorization and Data Rights Management in NG9-1-1 is based on XACML 2.0 [61]. Each
8875 XACML policy defines a "target", which describes what the policy applies to (by referring to
8876 attributes of users, roles, operations, objects, dates, and more), and one or more "rules" to
8877 permit or deny access. Access is defined to mean some combination of:

- 8878 • Read – the ability to retrieve a data object
- 8879 • Update – the ability to modify an existing data object
- 8880 • Create – the ability to create a new data object
- 8881 • Delete – the ability to remove an existing data object
- 8882 • Execute – the ability to execute one or more functions from a service

8883 Rules may "permit" or "deny" access.

8884 XACML policies are stored in a Policy Store. The XACML "Policy Decision Point" can be
8885 inside the element or agency that has the "Policy Enforcement Point" or may be external to
8886 it. Policies have names. The names come from a registry (10.14) or from the Service
8887 Names Registry (10.11).

8888 Provisioning data is owned by the agency operating an element, or the agency contracting
8889 with the agency operating the element, and thus is subject to data rights management.

8890 In policy rules:

- 8891 • Subject attributes can include the id (as an agentId), agency (as an agencyId), role
8892 (from the Agent or Agency role registries, Sections 10.27 and 10.28), and
8893 agencyType (from the agency locator record). The attributes agencyId, agency, role,
8894 and agencyType are string types.
- 8895 • Resources can be data structures or interfaces. Interfaces are named by the element
8896 Id and an interface keyword from a registry defined in Section 10.30 separated by
8897 an ampersand. Data items are named by the json object name from the OpenAPI
8898 interface description that defines them and the element tag (if access is controlled
8899 by element) separated by a period. For example, "LoST@ecrf.state.pa.us" and

8900 "civicAddr.A3". If no element name is specified, the access to the entire data
8901 structure is controlled by the rule.
8902 • Actions are "Read", "Create", "Update", "Delete", and "Execute".
8903 • A default rule must be included in every policy rule set.

8904 The XACML document is a JWS [171] (see Section 5.10) that MUST be signed by the owner
8905 of the Policy and MUST include the certificate and signing chain by value or by reference.

8906 **Note:** Occasionally data becomes orphaned and must come under new ownership to
8907 provide updates. A mechanism to re-home orphaned data will be provided in a future
8908 version of this document.

8909 **5.7 Integrity Protection**

8910 All protocol operations MUST be integrity-protected with TLS, using SHA-256 [62] or
8911 stronger. SHA-256 MUST be supported by all implementations. See [213] for details related
8912 to SRTP support for SHA-256.

8913 **5.8 Privacy**

8914 All protocol operations MUST be privacy protected via TLS, preferably using Advanced
8915 Encryption Standard (AES) [63] with a minimum key length of 256 bits (AES-256). Shorter
8916 key length MUST NOT be used. Systems currently using Data Encryption Standard (DES) or
8917 triple-DES MUST be upgraded to at least AES-256. Alternate encryption algorithms are
8918 acceptable as long as they are at least as strong as AES.

8919 Stored data which contains confidential information MUST be stored encrypted, using
8920 AES-256 or an equivalently strong algorithm. Access to encryption keys MUST be defined
8921 by a management policy that is strictly adhered to. Keys MUST NOT be stored in clear text.
8922 Access to keys MUST be secured by at least a pass phrase, and a two-factor authentication
8923 system for key access is RECOMMENDED. Guidelines for implementing and maintaining
8924 stored data securely can be found in [110]. Alternate privacy protection algorithms are
8925 acceptable as long as they are at least as strong as AES as long as both sides can
8926 implement it. AES-256 MUST be supported by all implementations.

8927 **5.9 Algorithm Upgrades**

8928 Cryptology choices are constantly being re-evaluated due to ongoing threat analysis,
8929 algorithm weakness research and other factors. Implementers should be aware that the
8930 mandatory algorithm choices (RSA-1024, SHA-256, and AES-256) to be supported in all
8931 implementations as described in this section may need to be upgraded as new threats
8932 emerge. At present, only a future version of this document could change the mandatory
8933 algorithm requirements.

[MM/DD/YYYY]

Page 316 of 675



8934 **5.10 JSON Web Signatures**

8935 This document, and i3 in general, extensively uses JSON objects. These JSON objects often
8936 contain information that needs to be protected against alteration and repudiation. As
8937 specified in various parts of this document, the JSON Web Signature (JWS) [171]
8938 mechanism is used to provide this protection. Within this document, a JWS MUST use the
8939 Flat JSON serialization format (not JWS Compact Serialization and not General JWS JSON
8940 Serialization Syntax), and only the Edwards-curve Digital Signature Algorithm (ECDSA) with
8941 Curve448 (algorithm "EdDSA") [227] [228] signature method is used.

8942 Each Web Service that has entrypoints in which a JWS is used MUST include the
8943 "requiredAlgorithms" parameter in the "serviceInfo" parameter of the object returned by its
8944 Versions endpoint. The "requiredAlgorithms" parameter specifies the JWS signing
8945 algorithms [221] permitted by the Web Service's currently in force policy. Implementations
8946 MUST support (be capable of generating and using) algorithm "EdDSA" and MUST NOT use
8947 other algorithms except that implementations of the Logging Service and clients of the
8948 Logging Service MUST support (be capable of generating and using) unsigned (algorithm
8949 "none"). A Logging Service MAY include "none"; a policy store MUST NOT include "none".
8950 If a Web Service request receives an "Unacceptable Algorithm" error, the client MUST make
8951 a new request on the Versions entry point and retry the request with a JWS that uses a
8952 signing algorithm acceptable to the Web Service.

8953 **Note:** Use of other algorithms, especially in situations where third parties may verify a
8954 signature, will be considered in a future version of this document.

8955 LogEvents are allowed to be unsigned because of their high volume and the potential for
8956 performance impacts; the policy currently in force of the agency operating the Logging
8957 Service determines if LogEvents are to be signed or unsigned. For signed LogEvents, the
8958 policy in force at the entity creating the LogEvent chooses between the size burden of each
8959 LogEvent containing the X.509 certificate of the signer (with all intermediate certificates)
8960 versus the additional network transactions the Logging Service or entity accessing the
8961 LogEvents needs to perform to retrieve the certificate (and chain) by reference, as
8962 described below. (Although this choice potentially impacts the Logging Service, the choice
8963 is up to the policy of the agency operating the entity creating the LogEvent).

8964 Implementations that access JWSs MUST support certificates (and chains) both by
8965 reference and by value; implementations that generate JWSs MAY use either.

8966 When this document indicates that a set of Web Service interface parameters is a JWS
8967 (e.g., for LogEvents), the set of parameters is conveyed in the web service request as a
8968 string consisting of a JWS. The JWS is formed by applying the JWS algorithm to the set of
8969 parameters per the JWS standard [171].

[MM/DD/YYYY]

Page 317 of 675



- 8970 • The JWS Protected Header MUST contain exactly one “alg” field. The “alg” field
8971 MUST have a value acceptable to the Web Service.
8972 • An unsigned (unprotected) JWS is indicated by an “alg” field set to the value “none”.
8973 • For signed LogEvents, and all other uses of JWS requiring signatures (e.g., policy
8974 documents), the JWS Protected Header MUST have its “alg” field set to a value
8975 acceptable to the Web Service that MUST NOT be “none” and MUST specify the
8976 signing entity’s X.509 certificate and all intermediate certificates up to one signed by
8977 the trusted root⁵⁶. The certificate is provided either by reference or by value. A
8978 certificate provided by value is contained in an “x5c” field. A certificate is provided
8979 by reference using the “x5u” and “x5t#256” fields. When the “x5u” field is present,
8980 it MUST contain a URL that is stable (resolvable) for a minimum of 10 years. The
8981 JWS Protected Header MAY contain other fields.

8982 Including a certificate (with chain) in each LogEvent increases the size of the event (in
8983 some cases by a multiple of the event size) but avoids the additional network requests
8984 necessary to retrieve the certificate chain using the “x5u” field.

8985 When the “x5u” field is used, the “x5t#256” field MUST also be used, to allow an entity to
8986 more easily detect when a certificate chain needs to be retrieved.

8987 The JWS is passed as the actual parameter of the entry point.

8988 **6 Gateways**

8989 While NG9-1-1 is defined to utilize an end-to-end IP architecture, there will continue to be
8990 wireline and wireless (circuit-switched) originating networks and legacy PSAPs deployed
8991 after emergency service networks and a significant number of PSAPs have evolved to
8992 support the i3 Solution. Since any i3 PSAP will need to be able to receive emergency calls
8993 that originate on these legacy networks, and legacy PSAPs will need to process voice
8994 emergency call originations that traverse ESInets, it is clear that gateways will be a
8995 required part of the i3 Solution architecture. The Legacy Network Gateway (LNG) is an i3
8996 functional element that supports the interconnection of legacy originating networks and the
8997 ESInet. The Legacy PSAP Gateway (LPG) is a functional element that supports the
8998 interconnection of the ESInet with legacy PSAPs. Each of these gateways is comprised of a
8999 set of functional components. The placement of the gateways in the i3 Solution
9000 architecture, and the functional components that make up the Legacy Network Gateway
9001 and the Legacy PSAP Gateway, are illustrated in Figure 6-1. The following subsections

56 The trusted root is the PCA for all entities within an ESInet, but in some cases (such as when a Logging Service is asked to log events that originated outside an ESInet) there may be a different trusted root.

9002 provide a detailed description of the functional components and interfaces that MUST be
9003 supported by a Legacy Network Gateway and a Legacy PSAP Gateway.

9004 **Note:** Another component, a Legacy Selective Router Gateway (LSRG), is used as part of
9005 transition to i3. The LSRG is described in a separate document [114].

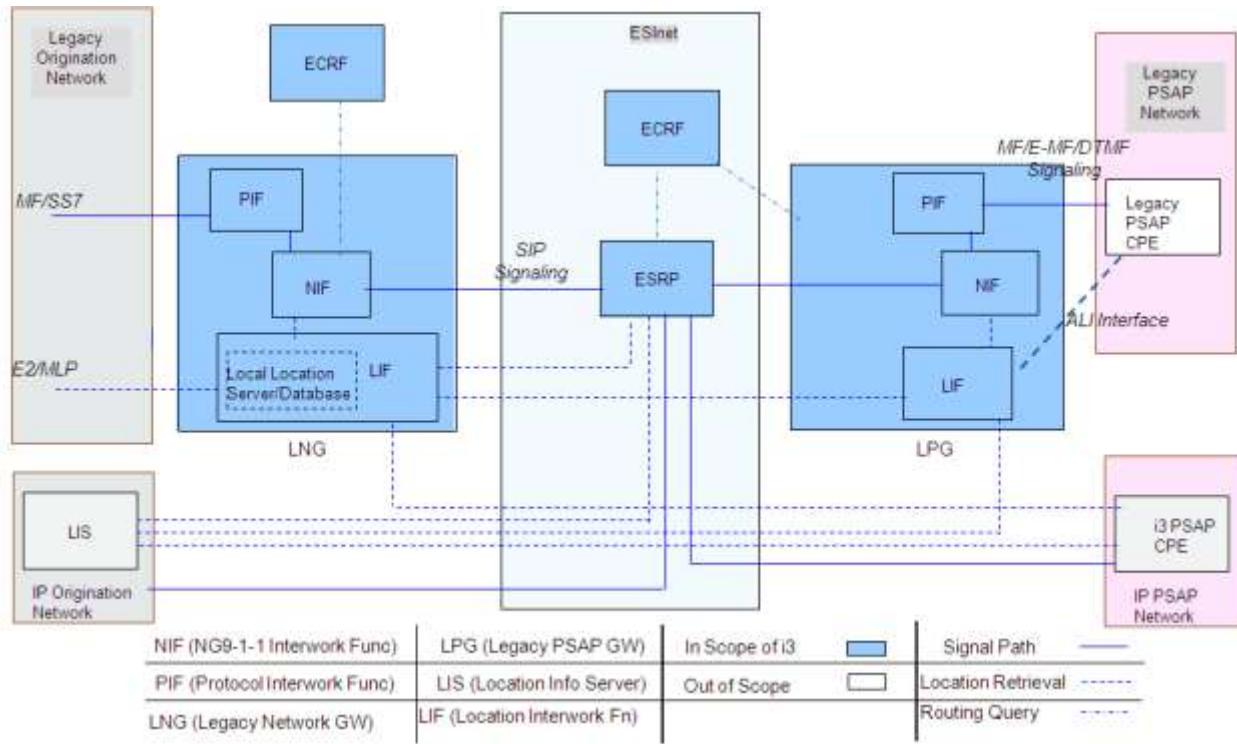


Figure 6-1 i3 Gateways – Functional Architecture

9006

9007

9008

9009 **6.1 Legacy Network Gateway (LNG)**

9010 A Legacy Network Gateway is a signaling and media interconnection point between callers
9011 in legacy wireline/wireless originating networks and the i3 architecture. The Legacy
9012 Network Gateway logically resides between the originating network and the ESInet and
9013 allows i3 PSAPs to receive emergency calls from legacy originating networks. Calls
9014 originating in legacy wireline or wireless networks must undergo signaling interworking to
9015 convert the incoming Multi-Frequency (MF) or Signaling System Number 7 (SS7) signaling
9016 to the IP-based signaling supported by the ESInet. Thus, the Legacy Network Gateway
9017 supports a physical SS7 or MF interface on the side of the originating network, and an IP
9018 interface which produces SIP signaling towards the ESInet and MUST provide the protocol
9019 interworking functionality from the SS7 or MF signaling that it receives from the legacy
9020 originating network to the SIP signaling used in the ESInet.

9021 The Legacy Network Gateway is also responsible for routing emergency calls to the
9022 appropriate ESRP in the ESInet. To support this routing, the Legacy Network Gateway
9023 MUST apply specific interwork functionality to legacy emergency calls that will allow the
9024 information provided in the call setup signaling by the wireline switch or Mobile Switching
9025 Center (MSC) (e.g., calling number/ANI, ESRK, cell site/sector represented by an ESRD) to
9026 be used as input to the retrieval of location information from an associated location
9027 server/database. The Legacy Network Gateway uses this location information to query an
9028 ECRF to obtain routing information in the form of a URI. The Legacy Network Gateway
9029 MUST then forward the call/session request to an ESRP in the ESInet, using the URI
9030 provided by the ECRF, and include callback and location information in the outgoing
9031 signaling.

9032 The Legacy Network Gateway functional element contains three functional components, as
9033 illustrated in Figure 6-1.⁵⁷ These functional components are described below:

- 9034 1. (MF/SS7 to SIP) Protocol Interwork Function (PIF): This functional component
9035 performs a standard interworking function that converts the incoming MF signaling
9036 or SS7 protocol from the legacy network to the SIP protocol expected by the i3
9037 ESInet and also converts the incoming TDM voice to the RTP data required by the i3
9038 ESInet. If the incoming call is a TTY call, the PIF will be responsible for interworking
9039 TTY to real-time text per RFC 5194 [84]. It is assumed that the PIF functional
9040 component does not require specialized hardware and can therefore be
9041 implemented using commercially available hardware. (See Section 6.1.1 for further
9042 details.)
- 9043 2. NG9-1-1-specific Interwork Function (NIF): This functional component provides
9044 NG9-1-1-specific processing of the incoming call signaling, which includes
9045 identification of the key(s) (e.g., calling number/ANI, ESRK, ESRD) that will be used
9046 as input to location retrieval. (See below for further information regarding the
9047 Location Interwork Function [LIF] functional component of the Legacy Network
9048 Gateway.) Having received the location information from the LIF, the NIF functional
9049 component provides the means by which the address of the target ESRP is identified
9050 (i.e., via a query to the ECRF), and the route to that ESRP is selected. This
9051 functional component also includes the ability to select a default route if necessary.
9052 Having identified the route to the ESRP, the NIF is also responsible for forwarding

57 Note that the functional decomposition of the Legacy Network Gateway described in this section is provided to assist the reader in understanding the functions and external interfaces that a Legacy Network Gateway must support. Actual implementations may distribute the functionality required of the Legacy Network Gateway differently among functional components, as long as all of the functions and external interfaces described herein are supported.

9053 the request to the ESRP and including location and callback information in the
9054 outgoing SIP signaling. The NIF is also responsible for taking any non-location call
9055 information provided by the LIF and generating a data structure that contains
9056 Additional Data about the call, along with a pointer/reference to that data structure.
9057 (See Section 6.1.2 for further details.)

- 9058 3. Location Interwork Function (LIF): This functional component is responsible for
9059 taking the appropriate key(s) from the incoming signaling (e.g., calling number/ANI,
9060 ESRK, ESRD), provided to it by the NIF, and using it (them) to retrieve location
9061 information via an associated location server/database⁵⁸. The location information is
9062 provided to the NIF for use in determining the route for the emergency call, and for
9063 populating the outgoing SIP INVITE message. Other non-location information
9064 associated with the call that is known or obtained by the LIF will be passed to the
9065 NIF for population in an AdditionalData data structure. (See Section 6.1.3 for further
9066 details.)

9067 When the LNG is provided by the 9-1-1 authority, or the NGCS operator, the LNG must
9068 implement the server-side of the ElementState event notification package.

9069 The following subsections describe each of the functional components of the Legacy
9070 Network Gateway in detail.

9071 **Note:** The LNG must log all significant events. Log record formats for this purpose are
9072 provided in Section 4.12.3 of this document.

9073 **6.1.1 Protocol Interwork Function (PIF)**

9074 To receive emergency calls from legacy originating networks, the Legacy Network Gateway
9075 is expected to support MF and SS7 trunking arrangements. Flexibility is required to
9076 accommodate different implementations for each type of interface.

9077 **6.1.1.1 MF Trunk Interface**

9078 If legacy wireline or wireless emergency calls are routed via MF trunks from the wireline
9079 end office or wireless MSC to the Legacy Network Gateway, the PIF component of the
9080 Legacy Network Gateway SHALL be capable of receiving and processing the following MF
9081 signaling:

58 Note that, in the case of certain legacy wireless emergency call originations, the location server/database will need to query an element in the legacy wireless network (i.e., an MPC/GMLC) to obtain caller location associated with the emergency call.

- 9082 • The PIF component of the Legacy Network Gateway SHALL be capable of
9083 recognizing a trunk seizure and returning a wink back to the wireline switch or MSC.
9084 • Upon receiving an MF digit string containing the dialed digits "911" (i.e., KP + 911 +
9085 ST), the PIF component SHALL return an ANI request signal to the wireline trunk or
9086 MSC.
9087 • The PIF component of the Legacy Network Gateway SHALL be capable of receiving
9088 and processing the appropriate ANI sequence. If CAMA-type signaling is used on the
9089 MF trunk from a wireline end office to the Legacy Network Gateway, the PIF
9090 component of the Legacy Network Gateway SHALL be capable of receiving and
9091 processing an ANI sequence that consists of "I + 7-digit ANI".
9092 • If Feature Group D operator-type signaling is used on the MF trunk from a wireline
9093 end office to the PIF component of the Legacy Network Gateway, the PIF
9094 component SHALL be capable of receiving and processing an ANI sequence
9095 consisting of "II + 7/10 digit ANI".
9096 • If the Legacy Network Gateway receives an emergency call that originates in a
9097 wireless network and is routed over an MF trunk group from an MSC, the PIF
9098 component of the Legacy Network Gateway SHALL be capable of receiving and
9099 processing Feature Group D signaling as described below:
9100 ○ If an emergency call originates in a wireless network and is routed from an
9101 MSC to the Legacy Network Gateway over an MF trunk group, and an ESRD is
9102 outpulsed with the ANI, the PIF component of the Legacy Network Gateway
9103 SHALL be capable of receiving and processing "II+7/10 digit+10 digit"
9104 Feature Group D-type signaling, where ANI is outpulsed as the first 7/10 digit
9105 number, and ESRD is outpulsed as the second 10 digit number (i.e., the
9106 called party number).
9107 ○ If an emergency call originates in a Commercial Mobile Radio Service (CMRS)-
9108 type wireless network and is routed from an MSC to the Legacy Network
9109 Gateway over an MF trunk group, and the wireless network uses the Wireline
9110 Compatibility Mode approach (i.e., only the ESRK is signaled), the PIF
9111 component of the Legacy Network Gateway SHALL be capable of receiving
9112 and processing an ESRK following the "II" (i.e., as ANI), and the digits
9113 "9-1-1", "1-1", or "1" as the called number.
9114 • Upon receiving a 200 OK message from the NIF component, the PIF component
9115 SHALL generate an answer signal to the wireline switch or MSC.
9116 • The PIF component of the Legacy Network Gateway SHALL be capable of receiving
9117 and processing an on-hook indication from a wireline switch or MSC and shall
9118 generate a SIP BYE message toward the NIF, as described in Section 6.1.1.5.

9119 **6.1.1.2 SS7 Interface**

9120 When a wireline end office or MSC determines that an SS7 Initial Address Message (IAM)
9121 associated with a 9-1-1 call is to be generated, it will also need to generate and pass some
9122 Message Transfer Part (MTP)-level information, along with the Integrated Services Digital
9123 Network User Part (ISUP) information, to the Legacy Network Gateway.

9124 **6.1.1.2.1 SS7 Message Transfer Part (MTP) Signaling for 9-1-1 Call Setup**

9125 The wireline end office/MSC will be responsible for generating information that will be
9126 populated in the MTP Signaling Information Field (SIF) and the Service Information Octet
9127 (SIO) portions of the IAM sent to the Legacy Network Gateway.

9128 The SIO contains the service indicator that identifies the MTP user involved in the
9129 message. In the case of a call setup message generated by a wireline end office or MSC,
9130 the service indicator will identify the ISDN User Part as the MTP user. The subservice field
9131 will indicate that the message is a national network message and will identify the MTP
9132 message priority. In the case of IAMs related to 9-1-1 calls, the message priority will have
9133 the value "1" (where priority 3 is the highest priority assigned to SS7 messages)⁵⁹.
9134 Therefore, the PIF component of the Legacy Network Gateway SHALL be capable of
9135 receiving and processing an IAM that contains MTP information that includes a Service
9136 Information Octet (SIO) that contains the following information:

- 9137 • The service indicator SHALL identify the ISDN User Part as the MTP user.
- 9138 • The subservice field SHALL indicate that the message is a national network message
9139 and that the message priority has a value of "1".

9140 The SIF contains a routing label, consisting of the Originating and Destination Point Codes,
9141 as well as the Signaling Link Selection value for the message, a Circuit Identification Code
9142 associated with the trunk selected for the call, a Message Type Code identifying the
9143 message as an Initial Address Message (IAM), and the content of the IAM itself. The PIF
9144 component of the Legacy Network Gateway SHALL be capable of receiving and processing
9145 an IAM that contains MTP information that includes a Signaling Information Field (SIF)
9146 containing the following information:

- 9147 • A routing label that contains the point code of the wireline end office or MSC in the
9148 Originating Point Code field, the point code of the Legacy Network Gateway in the
9149 Destination Point Code field, and an SLS code assigned by the wireline end
9150 office/MSC.

59 Note that the MTP message priority does not determine which messages are processed first when received at a node but is used instead to determine which messages should be discarded if the SS7 network experiences congestion.

- 9151 • A Circuit Identification Code assigned by the wireline end office/MSC and associated
9152 with the trunk selected for the call.
9153 • A Message Type code identifying the message as an IAM.
9154 • The content of the IAM itself.

9155 Further details related to MTP message structure can be found in GR-246-CORE [143],
9156 *Telcordia Technologies Specification of Signaling System Number 7*, Chapter T1.110.1,
9157 Section 5.1 and Chapter T1.111.3, Section 2.

9158 **6.1.1.2.2 SS7 ISUP Signaling for 9-1-1 Call Setup**

9159 This subsection describes requirements on the Legacy Network Gateway for processing
9160 ISUP signaling related to the receipt of emergency calls originated by legacy wireline and
9161 wireless customers over an SS7-controlled trunk. It is assumed that the trunk group from
9162 the wireline end office or MSC to the Legacy Network Gateway is a dedicated trunk group
9163 per carrier.

9164 If the incoming trunk to the Legacy Network Gateway is an SS7-controlled dedicated trunk
9165 selected by a wireline end office or wireless MSC, the PIF component of the Legacy
9166 Network Gateway SHALL be capable of receiving and processing an ISUP IAM containing
9167 parameters populated as described in GR-2956-CORE [159], *CCS/SS7 Generic*
9168 *Requirements in Support of E9-1-1 Service*, Sections 5.2.1.2.1, R2956-77 and 5.2.1.4.1,
9169 R2956-82, respectively.

9170 The PIF component of the Legacy Network Gateway SHALL also be capable of receiving
9171 and processing an ISUP Release (REL) message from a wireline end office or MSC,
9172 formatted as described in Table A-5 of GR-317-CORE [160], and generating a Release
9173 Complete Message (RLC) formatted as described in Table A-6 of GR-317-CORE in response.
9174 The PIF component of the Legacy Network Gateway SHALL also generate a SIP BYE
9175 message toward the NIF, as described in Section 6.1.1.5.

9176 The PIF component of the Legacy Network Gateway SHALL be capable of receiving and
9177 processing supervisory ISUP messages sent by wireline end offices and MSCs (e.g.,
9178 Blocking, Blocking Acknowledgement). The PIF component SHALL follow the procedures
9179 described in Section 3.1.4 of GR-317-CORE for processing these messages.

9180 **6.1.1.3 Early Media**

9181 In order to provide the equivalent of “trunk-side recording”, an LNG is expected to provide
9182 Early Media to downstream elements whenever it is possible to do so (for example, with an
9183 MF trunk origination). Any LNG that is acting as a SIPREC (RFC 5766) [119] SRC (Session
9184 Recording Client) SHALL provide Early Media (RFC 3960) [30] to the SRS (Session
9185 Recording Server).

[MM/DD/YYYY]

Page 324 of 675



9186 **6.1.1.4 Handling of Media Associated with TTY Calls**

9187 If the Legacy Network Gateway receives an incoming TTY call, the PIF component will be
9188 responsible for recognizing the Baudot tones in incoming media and replacing them with
9189 RFC 4103 [85] real-time text. Likewise, the PIF component will be responsible for
9190 generating Baudot tones in outgoing media (i.e., toward the caller) if real-time text is
9191 received in RTP packets, as described below.

9192 The Legacy Network Gateway SHALL handle a TTY emergency origination by establishing
9193 an audio session with the PSAP and subsequently requesting, or processing an incoming
9194 request for, the addition of an RFC 4103 text media session as described below.

9195 If the emergency call is delivered to the PSAP as a “silent” call, the Legacy Network
9196 Gateway MUST be capable of receiving and processing a re-INVITE from an i3 PSAP or
9197 Legacy PSAP Gateway that requests the addition of RFC 4103 text media to the existing
9198 emergency session.

9199 If the PIF component detects Baudot tones from the caller after an audio session is
9200 established, and an RFC 4103 text media session has not already been established (via a
9201 re-INVITE from an i3 PSAP or Legacy PSAP Gateway), the PIF component SHALL generate
9202 a SIP re-INVITE message that includes an offer in the SDP describing a media format
9203 associated with real-time text (as specified in RFC 4103) and send the SIP re-INVITE
9204 message to the NIF component. The PIF component will buffer any real-time text that is
9205 converted from the received Baudot tones until such time as the real-time text media
9206 session is established (i.e., a 200 OK message is received from the NIF component in
9207 response to the re-INVITE) and the real-time text can be passed forward. (See Section
9208 6.1.1.5 for further details.)

9209 If the PIF component detects Baudot tones from the caller before an audio session is
9210 established, the PIF component SHALL wait for the audio session to be established, and if a
9211 text session has not already been established, the PIF SHALL generate a SIP re-INVITE
9212 message that includes an offer in the SDP describing a media format associated with real-
9213 time text (as specified in RFC 4103) and send the SIP re-INVITE message to the NIF
9214 component. The PIF component will buffer any real-time text that is converted from the
9215 received Baudot tones until such time as the real-time text media session is established
9216 (i.e., a 200 OK message is received from the NIF component in response to the re-INVITE)
9217 and the real-time text can be passed forward. (See Section 6.1.1.5 for further details.)

9218 If the PIF component receives (i.e., from a legacy PSAP/LPG) simultaneous RFC 4103 real-
9219 time text and audio media that may include Baudot tones or other sounds, the PIF
9220 component MUST notch the audio frequencies used for Baudot tones from the received
9221 audio media and then insert the Baudot tones transcoded from the received RFC 4103 text
9222 to minimize the distortion of the Baudot tones delivered to the caller. When transcoding

9223 from RFC 4103 text to Baudot tones, the LNG SHALL support the special character
9224 mappings described in Section 6.2.1.4

9225 **6.1.1.5 Internal Interface to the NIF Component**

9226 The PIF component of the Legacy Network Gateway MUST have the capability to use
9227 standard interworking procedures, as defined in ATIS-1000679.2015 [130], to generate a
9228 SIP INVITE message based on incoming SS7 signaling and pass that INVITE message to
9229 the NIF component of the Legacy Network Gateway. The PIF component MUST also
9230 support mappings from MF signaling sequences to the appropriate fields in the outgoing
9231 SIP INVITE message, as described below.

9232 The initial SIP INVITE message generated by the PIF SHALL consist of the following
9233 information:

- A Request-URI that contains the information signaled in the SS7 Called Party Number parameter (per ATIS-1000679.2015) or as the MF called number.
- A To header field that contains the information signaled in the SS7 Called Party Number parameter (per ATIS-1000679.2015) or as the MF called number.
- A From header field that contains the information signaled in an SS7 Generic Digits Parameter (GDP), if present.

If a GDP is not received in incoming signaling, the From header field will be populated with the information signaled in the SS7 Calling Party Number parameter (if present).

- A P-Asserted-Identity (P-A-I) header field that is populated with the information contained in the SS7 Calling Party Number parameter (per ATIS-1000679.2015). In addition, the P-A-I header field will also contain the content of the SS7 Calling Party Category (CPC) parameter and the Originating Line Information (OLI) parameter, if present in the received SS7 Initial Address Message (IAM) (per ATIS-1000679.2015).
- A P-Charge-Info header field that is populated with the information that was contained in the SS7 Charge Number parameter (per ATIS-1000679.2015) or was signaled as the MF ANI.
- A Contact header field that contains the trunk group parameters that identify the ingress trunk group to the Legacy Network Gateway, as defined in RFC 4904 [161].
- A Via header field that is populated with the Element Identifier (see Section 2.1.3) for the Legacy Network Gateway.
- An SDP offer that includes the G.711 codec.

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and processing a SIP Trying (100) message passed to it by the NIF component, acknowledging receipt of the INVITE that was previously generated by the PIF component.

9260 The PIF component of the Legacy Network Gateway SHALL also be capable of receiving
9261 and processing a 180 Ringing message that contains either a "text" media feature tag or a
9262 "urn:emergency:media-feature.tty-interworking" media feature tag. (A 183 Session
9263 Progress message with a "urn:emergency:media-feature.tty-interworking" media feature
9264 tag will be received by the PIF component if the destination PSAP is an i3 PSAP.) If the
9265 incoming trunk group to the Legacy Network Gateway is an SS7 trunk group, then upon
9266 receiving the 180 Ringing message, the PIF component of the Legacy Network Gateway
9267 SHALL generate an ISUP Address Complete Message (ACM) formatted as described in
9268 Section 7.2.1.1 of ATIS-1000679.2015 [130] and Section 3.1.1.5 of GR-317-CORE, *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, with the following clarification: It is expected that bits DC of the Backward Call Indicator parameter SHOULD be set to "01" indicating "subscriber free", bits HG of the Backward Call Indicator parameter SHOULD be set to "00" indicating "no end-to-end method available", bit I SHALL be set to "1" indicating "interworking encountered", bit K SHALL be set to "0" indicating "ISDN User Part not used all the way", and bit M SHALL be set to "0" indicating "terminating access non-ISDN".
9275

9276 The PIF component of the Legacy Network Gateway SHALL be capable of receiving and
9277 processing a 183 Session Progress message that contains a "text" media feature tag. (This
9278 message will be received by the PIF component if the destination PSAP is a legacy PSAP.)
9279 If the incoming trunk group to the Legacy Network Gateway is an SS7 trunk group, then
9280 upon receiving the 183 Session Progress message, the PIF component of the Legacy
9281 Network Gateway SHALL generate an ISUP Address Complete Message (ACM) formatted as
9282 described in Section 7.2.1.1 of ATIS-1000679.2015 [130] and Section 3.1.1.5 of
9283 GR-317-CORE, LSSGR: Switching System Generic Requirements for Call Control Using the
9284 Integrated Services Digital Network User Part (ISDNUP), with the following clarification: It
9285 is expected that bits DC of the Backward Call Indicator parameter SHOULD be set to "00"
9286 indicating "no indication", bits HG of the Backward Call Indicator parameter SHOULD be set
9287 to "00" indicating "no end-to-end method available", bit I SHALL be set to "1" indicating
9288 "interworking encountered", bit K SHALL be set to "0" indicating "ISDN User Part not used
9289 all the way", and bit M SHALL be set to "0" indicating "terminating access non-ISDN". The
9290 Optional Backward Call Indicators parameter SHALL also be included in the ACM, with the
9291 "inband information indicator" (Bit A) set to "1" indicating "inband information or an
9292 appropriate pattern is now available".
9293

The PIF component of the Legacy Network Gateway SHALL be capable of receiving and
9294 processing a 200 OK message, indicating that the call has been answered. If the incoming
9295 trunk to the Legacy Network Gateway is an SS7 trunk, then upon receiving the 200 OK
9296 message, the PIF SHALL generate an ISUP Answer Message (ANM) formatted as described
9297 in Section 3.1.1.6 of GR-17-CORE. If ANM is the first backward message sent by the
9298 Legacy Network Gateway (i.e., no ACM is sent previously due to the 200 OK being the first

[MM/DD/YYYY]

Page 327 of 675



9299 SIP message received), the Legacy Network Gateway SHALL follow the procedures
9300 specified in Section 7.5.1 of ATIS-1000679.2015. Specifically, the Called Party's Status
9301 indicator (Bit DC) of the Backward Call Indicators parameter SHALL be set to "no
9302 indication," bit I SHALL be set to "1" indicating "interworking encountered," bit K SHALL be
9303 set to "0" indicating "ISDN User Part not used all the way," and bit M SHALL be set to "0"
9304 indicating "terminating access non-ISDN."

9305 If the incoming trunk to the Legacy Network Gateway is an MF trunk, then upon receiving
9306 the 200 OK message, the PIF SHALL generate an answer signal to the wireline switch or
9307 MSC.

9308 As described in Section 6.1.1.4, if the PIF component subsequently detects Baudot tones
9309 associated with a TTY origination, and a real-time text media session has not already been
9310 established for the emergency call (due to receipt of a re-INVITE generated by an i3 PSAP
9311 or Legacy PSAP Gateway or egress LSRG), the PIF component SHALL generate a SIP re-
9312 INVITE message that includes an SDP offer associated with real-time text, and send it to
9313 the NIF component. The re-INVITE message SHALL reference the existing dialog so that
9314 the i3 PSAP (or Legacy PSAP Gateway, or egress LSRG, in the case of a legacy PSAP)
9315 knows that it is requesting modification of an existing session instead of establishing a new
9316 session. The re-INVITE message SHALL include the same information as the original SIP
9317 INVITE message generated by the PIF component, with the exception that the SDP offer
9318 will include a media format associated with real-time text, as described in RFC 4103 [85].

9319 The PIF component SHALL wait to receive a 200 OK message from the NIF component
9320 indicating that the offer of real-time text has been accepted before sending the text media
9321 forward. The PIF component SHALL respond to the 200 OK by returning an ACK message.

9322 The PIF component MUST be capable of receiving and processing re-INVITE messages
9323 from the NIF component associated with emergency calls that are presented to the PSAP
9324 as a "silent" call. The received re-INVITE message will include an offer of a media format
9325 associated with real-time text (as described in RFC 4103 [85]). This re-INVITE message will
9326 include the following information:

- 9327 • A Request-URI that contains the URI and trunk group parameters delivered to the
9328 NIF component in the Contact header field of the initial INVITE message.
- 9329 • A To header field that contains the information signaled in the From header field of
9330 the original INVITE message (i.e., the information signaled in an SS7 GDP, if
9331 present, or the information signaled in the SS7 Calling Party Number parameter).
- 9332 • A From header field that contains the digits "911" expressed as a URI (delivered to
9333 the NIF component in the To header field of the original INVITE message).
- 9334 • A Contact header field that contains the information signaled to the NIF in the
9335 Request-URI of the original INVITE message (i.e., the digits contained in the SS7

9336 Called Party Number parameter (e.g., “911” expressed as a URI) and either a ‘text’
9337 media feature tag or a “urn:emergency:media-feature.tty-interworking” media
9338 feature tag.

9339 • A Via header field that is populated with a URI associated with the i3 PSAP or
9340 Legacy PSAP Gateway or egress LSRG.

9341 • An SDP offer that includes a media format associated with real-time text, as
9342 described in RFC 4103 [85].

9343 Upon receiving the re-INVITE message from the NIF component, the PIF SHALL respond
9344 with a 200 OK message, indicating that it accepts the SDP offer associated with real-time
9345 text. It SHALL be capable of receiving an ACK from the NIF component in response.

9346 The PIF component of the Legacy Network Gateway SHALL be capable of receiving and
9347 processing a SIP BYE message and acknowledging the BYE by returning a 200 OK message
9348 to the NIF. If the incoming trunk to the Legacy Network Gateway is an SS7 trunk, then
9349 upon receipt of the BYE message, the PIF SHALL generate an ISUP REL message, and be
9350 capable of receiving and processing an ISUP RLC sent in response. If the incoming trunk to
9351 the Legacy Network Gateway is an MF trunk, then upon receipt of the BYE message, the
9352 PIF SHALL generate an on-hook signal to the wireline switch or MSC.

9353 The PIF SHALL also be capable of generating a BYE message and sending it to the NIF if
9354 an ISUP REL is received from the wireline switch or MSC or an on-hook signal is received
9355 over an MF trunk from the wireline switch or MSC and SHALL be capable of receiving and
9356 processing a 200 OK message from the NIF sent in acknowledgement.

9357 In support of emergency call transfer procedures, the PIF component of a Legacy Network
9358 Gateway SHALL be capable of receiving and processing an INVITE method containing a
9359 conference URI, isfocus, and a Replaces header field that references the leg between the
9360 Legacy Network Gateway and the Primary (transfer-from) PSAP, from the NIF component.
9361 (See Section 6.1.2.2 for further discussion.) The PIF component SHALL respond to this SIP
9362 INVITE by returning a 200 OK, and SHALL receive an ACK from the NIF component in
9363 response to the 200 OK. The PIF component SHALL generate a BYE message to terminate
9364 the session with the Primary PSAP and send it to the NIF component. At this point, the
9365 Legacy Network Gateway switches the media from the session with the transfer-from PSAP
9366 to the session with the bridge.

9367 The PIF component of the Legacy Network Gateway SHALL be capable of receiving and
9368 processing a 200 OK message from NIF component in response to the BYE message. At
9369 this point the session between the Legacy Network Gateway and the transfer-from PSAP is
9370 terminated.

9371 If the ESInet supports the transfer models described in Sections 4.7.1.1 or 4.7.1.2, the PIF
9372 component of the Legacy Network Gateway SHALL be capable of receiving and processing

9373 a SIP INVITE from the NIF component that contains a Replaces header that requests that
9374 the connection to the bridge be replaced with a connection to the transfer-to PSAP. The
9375 PIF component SHALL respond to this SIP INVITE by returning a 200 OK and SHALL
9376 receive an ACK from the NIF component in response to the 200 OK. The PIF component
9377 SHALL generate a BYE message to terminate the session with the bridge and send it to the
9378 NIF component. At this point, the Legacy Network Gateway switches the media from the
9379 session with the bridge to the session with the transfer-to PSAP. The PIF component of the
9380 Legacy Network Gateway SHALL be capable of receiving and processing a 200 OK message
9381 from NIF component in response to the BYE message. At this point the session between
9382 the Legacy Network Gateway and the conference bridge is terminated.

9383 Note that if the PIF does not support INVITE/Replaces, the NIF MAY complete processing
9384 of INVITE/Replaces instead of the PIF.

9385 If the PIF component receives other SIP messages from the NIF component, it SHALL
9386 process them per RFC 3261 [10].

9387 **6.1.2 NG9-1-1-specific Interwork Function (NIF)**

9388 **6.1.2.1 NIF Handling of INVITE from PIF**

9389 The NIF component of the Legacy Network Gateway functional element is expected to
9390 provide special processing of the information received in the incoming INVITE message
9391 from the PIF component to facilitate call delivery to an i3 ESInet. The NIF SHALL
9392 determine, based on the incoming trunk group and/or the incoming signaling, whether the
9393 call is a wireline or wireless emergency call. If the call is received over an MF trunk group,
9394 the NIF SHALL make this determination based on the incoming trunk group parameters
9395 included in the Contact header field of the INVITE message from the PIF. If the call is
9396 received over an SS7 trunk group, the NIF SHALL make this determination based on the
9397 coding of the cpc and oli parameters in the P-A-I header field of the INVITE message from
9398 the PIF and/or the ingress trunk group parameters in the Contact header field of the
9399 INVITE message from the PIF. Based on this determination, the NIF SHALL extract the
9400 appropriate information (i.e., calling party number, charge number, and/or ESRD) from the
9401 incoming signaling to be used as the location key and SHALL pass it to the Location
9402 Interwork Function (LIF) for use in obtaining caller location information. (See Section 6.1.3
9403 for further discussion of LIF functionality and interfaces.)

9404 If the NIF determines that the incoming call is a legacy wireline emergency call, and only
9405 one number is received in incoming signaling as the Calling Party Number (CPN)/ANI (i.e.,
9406 the URI in the From, P-A-I, and P-Charge-Info header fields of the INVITE message
9407 received from the PIF contains the same CPN/ANI), the NIF SHALL pass this number to the

9408 LIF to use in retrieving the location for the call⁶⁰. If the NIF determines that the incoming
9409 call is a legacy wireline emergency call and two different numbers are received in incoming
9410 signaling (i.e., the INVITE message from the PIF contains a URI associated with the Charge
9411 Number in the P-Charge-Info header field and a different URI associated with the CPN in
9412 the P-A-I header field) the NIF MUST support a configuration option to tell it which number
9413 to send to the LIF as input to location retrieval.

9414 If the NIF determines (based on the oli parameter in the P-A-I header field or the trunk
9415 group information in the Contact header field) that the incoming call is a legacy wireless
9416 emergency call, and both a callback number (i.e., Mobile Directory Number [MDN]) and an
9417 ESRD are received in incoming signaling, the NIF SHALL send both numbers to the LIF
9418 since both are required to uniquely identify the call. The NIF will determine, based on
9419 configured information associated with the trunk group identified in the trunk group
9420 parameters within the Contact header field of the received INVITE, where to extract the
9421 callback information and ESRD from. The ESRD MAY be populated in the Request-URI/To
9422 header fields or in the From header field. The MDN MAY be populated in the From header
9423 field or the P-A-I header field.

9424 (See Section 6.1.3 for further discussion of what the LIF does with this information.)

9425 **6.1.2.1.1 NIF Handling of Location Information from the LIF**

9426 Once the NIF receives location information from the LIF in geodetic or civic format, the NIF
9427 MUST be capable of generating a routing request to an ECRF. The NIF SHALL generate a
9428 LoST query, which includes the location information provided by the LIF and an appropriate
9429 service URN (i.e., "urn:service:sos"), following the procedures described in Section 3.4. If
9430 the NIF does not receive a routing location from the LIF component within a pre-specified
9431 period of time, the NIF component SHALL use a default location (based on the incoming
9432 trunk group information provided in the Contact header field of the INVITE message from
9433 the PIF component) to query the ECRF.

9434 Upon receiving the response from the ECRF, the NIF SHALL determine the outgoing route
9435 for the call using the URI of the target ESRP received in the LoST response. If the NIF
9436 component of the Legacy Network Gateway does not receive a response to a LoST query
9437 within a provisioned time period, or receives an error indication from the ECRF, it SHALL
9438 log the event and route the call based on a provisioned default ESRP URI.

60 Note that this processing will also apply to wireless Wireline Compatibility Mode calls, since these are marked as wireline in incoming signaling and contain a single 10-digit number, the ESRK, which is signaled as the SS7 CPN or MF ANI.

9439 In addition to determining the outgoing route, the NIF may generate a data structure that
9440 contains Additional Data about the call. The data structure SHALL contain the mandatory
9441 information identified in Section 3.1 of NENA 71-001 [73], as well as any other non-location
9442 information associated with the call that is provided to the NIF by the LIF, formatted
9443 according to RFC 7852 [107]. The NIF may include this Additional Data (or a subset of it)
9444 "by-value" in the body of the outgoing SIP message it sends to the ESRP, and/or it may
9445 generate a pointer/reference to that data structure. The pointer SHALL contain the URI of
9446 the ADR in which the Additional Data information is stored. The URI generated by the NIF
9447 SHOULD include the callback number. If there is only static information and no per-call
9448 information, the NIF MAY include a reference URI to a static ADR that may be maintained
9449 at the NIF or elsewhere if maintained by the 9-1-1 Authority. If the NIF generates a
9450 pointer/reference to an Additional Data structure (or passes Additional Data by value), it
9451 SHALL include the reference URI (which may be a CID) in the Call-Info header field of the
9452 INVITE message sent to the ESRP, with a purpose parameter beginning with
9453 "EmergencyCallData", a dot and the block name of the Additional Data structure. If the NIF
9454 passes Additional Data by reference, and the reference refers to the LNG, the NIF
9455 component of the LNG MUST maintain an ADR interface, utilizing the HTTPS GET method
9456 described in IETF RFC 7230 [162], to support dereference requests for Additional Data.

9457 **6.1.2.2 SIP Interface to the ESInet**

9458 The NIF is expected to behave as a B2BUA and generate a SIP INVITE message to be sent
9459 to the ESRP. This initial INVITE message SHALL contain information received in the initial
9460 INVITE message from the PIF component, as well as location and possibly callback
9461 information received from the LIF component. The initial INVITE message MAY also contain
9462 reference URIs associated with any Additional Data structures generated by the NIF, if any
9463 are generated.

9464 If a default location was used to query the ECRF, the SIP INVITE message generated by
9465 the NIF component SHALL include a PIDF-LO document in the body that contains the
9466 default location with a <method> element set to the value "Default", and the <provided-
9467 by> element set to the identity of Legacy Network Gateway provider that inserted it, and a
9468 Geolocation header field populated with a "cid" URI pointing to it.

9469 The INVITE message generated by the NIF component of the Legacy Network Gateway
9470 SHALL contain the following information:

- 9471
 - A Request-URI that contains a service URN in the "sos" tree (i.e., "urn:service:sos")
 - A To header field that contains the digits "911"
 - A From header field that contains the callback number (or Originating TN for legacy
9474 wireline emergency call originations) received by the NIF component in incoming

- 9475 signaling from the PIF component, or retrieved by the LIF component, as
9476 appropriate for the type of emergency call origination.
- 9477 o If the "Service Delivered by Provider to End User" provided by the LIF
9478 component is equal to "POTS," the NIF component SHALL populate the From
9479 header field based on the Calling Party Number received in the From and
9480 P-A-I header fields of the incoming INVITE message from the PIF component.
- 9481 o If the "Service Delivered by Provider to End User" provided by the LIF
9482 component is equal to "wireless", then the NIF component SHALL populate
9483 the From header field as follows:
- 9484 ▪ If the From header field and the P-A-I header field of the incoming
9485 INVITE message from the PIF component are not the same (i.e., a
9486 GDP was received in the incoming signaling from the MSC), the NIF
9487 component SHALL use the value provided in the P-A-I header field of
9488 the INVITE message from the PIF component to populate the From
9489 header field of the outgoing INVITE message.
- 9490 ▪ If the From header field and the P-A-I header field of the incoming
9491 INVITE message from the PIF component are the same (i.e., no GDP
9492 was present in the incoming signaling from the MSC), the NIF
9493 component SHALL use the callback number provided by the LIF
9494 component to populate the From header field of the outgoing INVITE
9495 message. If the LIF component does not provide a callback number to
9496 the NIF component within a pre-specified period of time, the NIF
9497 component SHALL populate the From header field with the value
9498 received in the incoming INVITE message from the PIF component.
- 9499 o If the call was originated by a non-initialized mobile caller (i.e., the callback
9500 number is of the form 911+ "last 7 digits of the ESN or IMEI expressed as a
9501 decimal") the From header field SHALL contain a value of "Anonymous."
- 9502 • A P-Asserted-Identity (P-A-I) header field that contains the callback number
9503 retrieved by the LIF component or received in incoming signaling from the PIF
9504 component, as appropriate for the type of emergency call origination. Note that the
9505 P-A-I sent by the NIF component to the ESRP will not contain cpc or oli parameters.
- 9506 o If the "Service Delivered by Provider to End User" provided by the LIF
9507 component is equal to "POTS," the NIF component SHALL populate the P-A-I
9508 with the SS7 Calling Party Number information received in the P-A-I header
9509 field of the incoming INVITE message from the PIF component.
- 9510 o If the "Service Delivered by Provider to End User" provided by the LIF
9511 component is equal to "wireless", then the NIF component SHALL populate
9512 the P-A-I header field as follows:

[MM/DD/YYYY]

Page 333 of 675



- 9513 ▪ If the From header field and the P-A-I header field of the incoming
9514 INVITE message from the PIF component are not the same (i.e., a
9515 GDP was received in the incoming signaling from the MSC), the NIF
9516 component SHALL use the SS7 Calling Party Number value provided in
9517 the P-A-I header field of the INVITE message from the PIF component
9518 to populate the P-A-I header field of the outgoing INVITE message.
9519 ▪ If the From header field and the P-A-I header field of the incoming
9520 INVITE message from the PIF component are the same (i.e., no GDP
9521 was present in the incoming signaling from the MSC), the NIF
9522 component SHALL use the callback number provided by the LIF
9523 component to populate the P-A-I header field of the outgoing INVITE
9524 message. If the LIF component does not provide a callback number to
9525 the NIF component within a pre-specified period of time, the NIF
9526 component SHALL omit the P-A-I header field from the outgoing
9527 INVITE message.
9528 ○ If a non-initialized mobile caller originated the call, the P-A-I header field
9529 SHALL be omitted.
9530 • A P-Charge-Info header field, if one was received in the INVITE message from the
9531 PIF component. This field will contain the information received by the Legacy
9532 Network Gateway in an SS7 Charge Number parameter or signaled as an MF ANI.
9533 • A Via header field that is populated with the Element Identifier (see Section 2.1.3)
9534 for the Legacy Network Gateway
9535 • A Route header field that contains the ESRP URI obtained from the ECRF (this URI
9536 should be augmented with the "lr" parameter in the Route header field to avoid
9537 Request-URI rewriting)
9538 • A Contact header field that contains a SIP URI that is associated with the Legacy
9539 Network Gateway, along with a "urn:emergency:media-feature.tty-interworking"
9540 media feature tag.
9541 • A Supported header field that contains the "geolocation-sip" option tag
9542 • A Geolocation header field that either:
9543 ○ Points to the message body (using a "Content Identifier" URI, as defined in
9544 RFC 2392 [132]) where a PIDF-LO containing the location value retrieved by
9545 the LIF is coded (see Section 6.1.3 and RFC 6442 [8])⁶¹, or;
9546 ○ Contains a location-by-reference URI⁶².

61 This method SHALL be used for wireline emergency calls or default-routed calls.

62 This method SHALL be used for wireless Phase 1 and Phase 2 calls to allow the queries for routing location as well as for initial and updated caller location.

- 9547 • A Geolocation-Routing header field set to "yes"
9548 • An SDP offer as received from the PIF component.
9549 • If, during the processing of the emergency call, the NIF component of the Legacy
9550 Network Gateway creates an Additional Data data structure and stores it, the NIF
9551 component of the Legacy Network Gateway SHALL include one or more⁶³ Call-Info
9552 header fields with a purpose parameter beginning with "EmergencyCallData", a dot
9553 and the block name of the Additional Data structure; a value set to the URI
9554 associated with the ADR that contains the Additional Data data structure which,
9555 when dereferenced, yields the Additional Data data structure.
9556 • If, during the processing of the emergency call, the NIF component of the Legacy
9557 Network Gateway creates one or more AdditionalData structures and sends them
9558 forward by value in the outgoing INVITE message, the NIF component of the Legacy
9559 Network Gateway:
9560 ○ SHALL populate each data structure as a body part of the INVITE message
9561 with a MIME type of "Application/EmergencyCallData", a dot and the block
9562 name of Additonal Data.
9563 ○ For each Additional Data structure, SHALL include a Call-Info header field
9564 with a purpose parameter set to "EmergencyCallData.", a dot and the block
9565 name of the Additional Data, and a value set to the cid: URI that points to the
9566 body part containing the Additional Data.
9567 ○ Each Additional Data structure is contained in one body part and referenced
9568 by one Call-Info header field that identifies the block type and the CID.
9569 • A P-Preferred-Identity header field populated with 911 + "last 7 digits of the ESN or
9570 IMEI expressed as a decimal" if the call was originated by a non-initialized mobile
9571 caller.

9572 After sending the SIP INVITE to the ESInet, the NIF SHALL return a SIP Trying (100)
9573 message to the PIF.

9574 The NIF component SHALL be capable of receiving and processing a 180 Ringing message
9575 or a 183 Session Progress message that includes a Contact header field with either a "text"
9576 media feature tag or a "urn:emergency:media-feature.tty-interworking" media feature tag
9577 from the ESInet in response to the SIP INVITE. If the NIF component receives a 180
9578 Ringing message, it SHALL send a 180 Ringing message to the PIF component. If the NIF

63 The NIF MUST add at least ProviderInfo and ServiceInfo and MAY add SubscriberInfo blocks as described in Section 4.11. These MAY be referenced in one Call-Info header field with multiple URIs or multiple Call-Info header fields with one or more URIs.

9579 component receives a 183 Session Progress message, it SHALL send a 183 Session
9580 Progress message to the PIF component.

9581 The NIF component SHALL also be capable of receiving and processing a 200 OK message
9582 from the ESInet. If the NIF component receives a 200 OK message from the ESInet, it
9583 SHALL send it to the PIF component. The NIF component SHALL be capable of receiving
9584 and processing an ACK message from the PIF component in response to the 200 OK
9585 message. The NIF component SHALL subsequently send an ACK message to the ESInet.

9586 If callback information is not available at the time that the initial INVITE message is sent by
9587 the NIF component to the ESRP, but is subsequently provided by the LIF component, the
9588 NIF component SHALL generate a re-INVITE message to communicate this information to
9589 the PSAP. The re-INVITE message SHALL reference the existing dialog so that the i3 PSAP
9590 (or Legacy PSAP Gateway or egress LSRG, in the case of a legacy PSAP) knows that it is to
9591 modify an existing session instead of establishing a new session. The re-INVITE message
9592 SHALL include the following information:

- 9593 • A Request-URI that contains the information provided in the Contact header field of
9594 the 200 OK message that was returned in response to the original INVITE message;
- 9595 • A To header field that contains the same information as the original INVITE
9596 message (i.e., the digits "911");
- 9597 • A From header field that contains the same information as in the original INVITE
9598 message (i.e., the From header field will be populated with the value received in the
9599 incoming INVITE message from the PIF component, which is the ESRK);
- 9600 • A P-Asserted-Identity (P-A-I) header field that contains the callback number
9601 retrieved by the LIF component;
- 9602 • A Via header field that is populated with the Element Identifier (see Section 2.1.3)
9603 for the Legacy Network Gateway;
- 9604 • A Route header field that contains the same information as in the original INVITE
9605 (i.e., the ESRP URI obtained from the ECRF, which should be augmented with the
9606 "lr" parameter to avoid Request-URI rewriting);
- 9607 • A Contact header field that contains the same information as in the original INVITE
9608 message (i.e., a SIP URI associated with the Legacy Network Gateway along with a
9609 "urn:emergency:media-feature.tty-interworking" media feature tag).

9610 Likewise, if the NIF component receives a re-INVITE message from the PIF component
9611 (because the PIF component has detected Baudot tones after the initial session was
9612 established), the NIF component SHALL send a re-INVITE message toward the PSAP
9613 requesting the establishment of a real-time text media session. The re-INVITE message
9614 SHALL include the following information:

- 9615 • A Request-URI that contains the information provided in the Contact header field of
9616 the 200 OK message that was returned in response to the original INVITE message;

[MM/DD/YYYY]

Page 336 of 675



- 9617 • A To header field that contains the same information as the original INVITE
9618 message (i.e., the digits "911");
9619 • A From header field that contains the same information as in the original INVITE
9620 message;
9621 • A P-Asserted-Identity (P-A-I) header field that contains the callback number included
9622 in the previous INVITE message;
9623 • A Via header field that is populated with the Element Identifier (see Section 2.1.3)
9624 for the Legacy Network Gateway;
9625 • A Route header field that contains the same information as in the original INVITE
9626 (i.e., the ESRP URI obtained from the ECRF, which should be augmented with the
9627 "lr" parameter to avoid Request-URI rewriting);
9628 • A Contact header field that contains the same information as in the original INVITE
9629 message (i.e., a SIP URI associated with the Legacy Network Gateway along with a
9630 along with a "urn:emergency:media-feature.tty-interworking" media feature tag);
9631 • An SDP offer that includes a media format associated with real-time text, as
9632 described in RFC 4103 [85].

9633 The i3 PSAP/Legacy PSAP Gateway/egress LSRG SHALL return a 200 OK to indicate that it
9634 accepts the change, and the Legacy Network Gateway SHALL respond to the 200 OK by
9635 returning an ACK message.

9636 The NIF component MUST also be capable of receiving and processing a re-INVITE
9637 message sent by an i3 PSAP or Legacy PSAP Gateway or LSRG. This will occur if a "silent"
9638 call is received by the PSAP, and the PSAP attempts to establish communication using
9639 TTY/RTT (as specified in the SOP that specifies the handling of silent calls). The re-INVITE
9640 generated by the i3 PSAP/Legacy PSAP Gateway/LSRG SHALL request the addition of RFC
9641 4103 text media to the emergency session already established with the Legacy Network
9642 Gateway. (See Section 6.2.2.4 for details related to the content of this re-INVITE message
9643 when generated by a Legacy PSAP Gateway/LSRG.) Upon receiving the re-INVITE from the
9644 i3 PSAP/Legacy PSAP Gateway, the NIF component SHALL send a re-INVITE message to
9645 the PIF component, as described in Section 6.1.1.5. The PIF component SHALL return a 200
9646 OK indicating that it accepts the change, and the NIF component SHALL respond to the
9647 200 OK by returning an ACK message. The NIF component SHALL also send a 200 OK
9648 message to the i3 PSAP/Legacy PSAP Gateway/LSRG, and the i3 PSAP/Legacy PSAP
9649 Gateway/LSRG SHALL return an ACK.

9650 The NIF component SHALL be capable of receiving and processing a BYE message from
9651 the ESInet. If the NIF component receives a BYE message from the ESInet, it SHALL pass
9652 it to the PIF component. The NIF component SHALL be capable of receiving and processing
9653 a 200 OK message from the PIF component in response to the BYE message and SHALL
9654 subsequently send a 200 OK message to the ESInet.

[MM/DD/YYYY]

Page 337 of 675



9655 If the NIF component receives other SIP messages from the ESInet, it SHALL validate them
9656 and if necessary, apply the appropriate error handling per RFC 3261 [10]. If the messages
9657 pass the validity checks, the NIF component SHALL pass them to the PIF component.

9658 The NIF component SHALL be capable of receiving and processing a BYE message from
9659 the PIF component. If the NIF component receives a BYE message from the PIF
9660 component, it SHALL send a BYE message to the ESInet. Upon receiving a 200 OK
9661 message from the ESInet in response to the BYE message, the NIF component SHALL
9662 return a 200 OK message to the PIF component.

9663 In support of emergency call transfer procedures, the NIF component of a Legacy Network
9664 Gateway SHALL be capable of receiving and processing an INVITE method containing a
9665 conference URI, isfocus, and a Replaces header field that references the leg between the
9666 Legacy Network Gateway and the transfer-from PSAP, from a conference bridge in the
9667 ESInet. The NIF component SHALL pass the INVITE with Replaces to the PIF component.
9668 Upon receiving a 200 OK from the PIF component, the NIF component SHALL send an ACK
9669 to the PIF component and SHALL send a 200 OK to the conference bridge. The conference
9670 bridge will respond by returning an ACK to the NIF component.

9671 At this point, a session is established between the Legacy Network Gateway and the
9672 conference bridge. Note that the media session between the Legacy Network Gateway and
9673 the transfer-from PSAP still exists at this time. Note also that the media between the caller
9674 and the Legacy Network Gateway is undisturbed.

9675 The Legacy Network Gateway SHALL terminate the session with the transfer-from PSAP by
9676 sending a BYE message from the PIF component to the NIF component and on to the
9677 transfer-from i3 PSAP or LPG or LSRG, following the signaling path established by the
9678 INVITE request associated with the original emergency session. At this point, the Legacy
9679 Network Gateway switches the media from the session with the transfer-from PSAP to the
9680 session with the bridge.

9681 The NIF component of the Legacy Network Gateway SHALL be capable of receiving and
9682 processing a 200 OK message from the transfer-from i3 PSAP/LPG/LSRG in response to the
9683 BYE message. Upon receiving a 200 OK from the transfer-from i3 PSAP/LPG/LSRG, the NIF
9684 component SHALL forward the 200 OK message to the PIF component. At this point the
9685 session between the Legacy Network Gateway and the transfer-from PSAP is terminated.

9686 If the ESInet supports the transfer models described in Sections 4.7.1.1 or 4.7.1.2, the NIF
9687 component of the Legacy Network Gateway SHALL also be capable of receiving and
9688 processing a SIP INVITE from the transfer-to PSAP that contains a Replaces header that
9689 requests that the connection from the Legacy Network Gateway to the bridge be replaced
9690 with a connection to the transfer-to PSAP. The NIF component SHALL pass the INVITE with
9691 Replaces to the PIF component. Upon receiving a 200 OK from the PIF component, the NIF

9692 component SHALL send an ACK to the PIF component and SHALL send a 200 OK to the
9693 transfer-to PSAP. The transfer-to PSAP will respond by returning an ACK to the NIF
9694 component.

9695 At this point, a session is established between the Legacy Network Gateway and the
9696 transfer-to PSAP. Note that the media session between the Legacy Network Gateway and
9697 the conference bridge still exists at this time. Note also that the media between the caller
9698 and the Legacy Network Gateway is undisturbed.

9699 The Legacy Network Gateway SHALL terminate the session with the conference bridge by
9700 sending a BYE message from the PIF component to the conference bridge, following the
9701 signaling path established by the INVITE with Replaces previously received from the
9702 conference bridge. At this point, the Legacy Network Gateway switches the media from the
9703 session with the conference bridge to the session with the transfer-to PSAP.

9704 Note that if the PIF does not support INVITE/Replaces, the NIF MAY complete processing
9705 of INVITE/Replaces instead of the PIF.

9706 **6.1.2.3 Handling of Media Associated with TTY Emergency Originations**

9707 As described in Section 6.1.1.4, the PIF component of the Legacy Network Gateway is responsible
9708 for interworking between Baudot tones and RFC 4103 text. To support this interworking,
9709 the NIF component MUST be capable of processing re-INVITE messages either received
9710 from the PIF component or from the PSAP or Legacy PSAP Gateway or egress LSRG via the
9711 ESInet (i.e., for “silent” calls) that contain an SDP offer for RFC 4103 real-time text. (See
9712 Section 6.1.1.5 for further discussion of the content of these re-INVITE messages.)

9713 In addition, the NIF component SHALL be responsible for supporting the “turn-taking”
9714 conventions expected in TTY communications. When a TTY caller is sending characters,
9715 (i.e., it is the TTY caller’s “turn”), the Baudot tones are converted to RFC 4103 characters
9716 and forwarded by the NIF to the ESInet. The NIF buffers any RFC 4103 characters it
9717 receives from the ESInet. When a “_GA”⁶⁴ (where the underscore indicates a space
9718 character) is received from the caller via the PIF, the NIF component will set an inter-
9719 character timer of 1500 ms. If a space or line delimiter is received, or the 1500 ms timer
9720 expires without any other character being received, the NIF will recognize that a change in
9721 turn is in effect. The NIF SHALL perform one of the following procedures, depending on the

64 It is a convention with TTY to use the characters “GA” for “Go Ahead” at the end of the typed message when one user wants to give a turn to the other user. The following should also be interpreted as end of message values to address scenarios where there is a lost shift character: “+‐” and “<BELL>” (where the bell-character is U+0007 when converted to RFC 4103 text). See Emergency Access Advisory Committee (EAAC) Report on procedures for calls between TTY users and NG9-1-1 PSAPs [175] for further details.

capabilities of the far end, as indicated by the value of the media feature tag returned by the far end in response to the SIP INVITE generated by the NIF. If, instead, a character other than space or line delimiter is received from the TTY user before the 1500 ms timer expires, then the NIF component will recognize that the " GA" was the beginning of a regular word, and reception of text from the TTY user will continue with no change of turn.

If a change of turn is in effect, and the media feature tag returned in a response to the initial SIP INVITE message generated by the NIF component has the value "text", the NIF SHALL substitute a line delimiter (e.g., CRLF) for the GA and forwards the line delimiter to the ESInet. The NIF SHALL then send any buffered characters received from the ESInet to the caller via the PIF and SHALL continue forwarding characters received from the ESInet in real time to the TTY caller using the mechanism described below.

If a change of turn is in effect, and the media feature tag received by the NIF component in a response to the initial SIP INVITE message has the value "urn:emergency:media-feature.tty-interworking", the NIF component SHALL pass the string of text characters (including the "GA") toward the PSAP, unchanged. As above, the NIF SHALL then send any buffered characters received from the ESInet to the caller via the PIF and SHALL continue forwarding characters received from the ESInet in real time to the TTY caller using the mechanism described below.

The NIF component MUST be capable of sending text characters toward a TTY caller, received from the ESInet toward a TTY caller. When the ESInet is sending text characters toward a TTY caller, the NIF will use the presence of a pre-defined pause between characters, or the presence of a " GA" or a line delimiter, to simulate a request by the PSAP to change the turn. Upon detecting a request to change the turn, the NIF component will add a "_GA" to the end of the text characters that are to be sent toward the caller, if "_GA" is not already present in the received text characters, as follows.

To support the interworking of RFC 4103 real-time text to Baudot tones performed by the PIF component of the Legacy Network Gateway, the NIF component SHALL initiate a provisonable inter-character timer, with a default value of 7 seconds, upon receipt of the first RFC 4103 text character from the ESInet. This timer SHALL be restarted with a value of 7 seconds every time a character is transmitted towards the TTY caller. If the characters "_GA" are detected, the inter-character timer shall be reduced to 1500 ms and if the NIF component receives no further text before the 1500 ms timer expires, the NIF component SHALL pass the text characters to the PIF component, unchanged. At this point, the turn will be changed and the NIF component will begin buffering any subsequent text from the ESInet. If additional text (other than a space or line delimiter) is received before the 1500 ms expires, the NIF component SHALL set the inter-character timer at 7 seconds and again continue forwarding characters toward the TTY caller and wait for a "_GA" or line delimiter.

9759 If a line delimiter is detected before the 7-second timer expires, the NIF component SHALL
9760 replace the line delimiter with a space and SHALL reset the inter-character timer to 1500
9761 ms. If the inter-character timer expires without a “_GA” being detected, the NIF
9762 component SHALL append the characters “_GA” to the incoming RFC 4103 text and pass
9763 the text characters with the “_GA” appended to the PIF component for conversion to
9764 Baudot tones. At this point, a change of turn is performed, and the NIF component starts
9765 buffering characters received from the ESInet. If the NIF component receives a “_GA”
9766 before the 1500 ms timer expires, the NIF component SHALL follow the procedure
9767 described above for receipt of a “_GA”. Once the inter-character timer has been initiated to
9768 1500 ms, the receipt of space characters or line delimiters SHALL NOT cause the timer to
9769 be reset, rather the same procedure shall be followed as when the 1500 ms timer has
9770 expired.

9771 The intention of the above procedure is to change turn and send “_GA” to the TTY caller
9772 when the PSAP sends a line delimiter or “_GA”, possibly followed by spaces or line
9773 delimiters, but not immediately followed by text. A change of turn will also be made and
9774 “_GA” sent to the TTY caller when the PSAP is idle for an extended period of time,
9775 assuming that the PSAP makes no specific action to change turn. (A PSAP idle time of 7
9776 seconds is specified in the Emergency Access Advisory Committee (EAAC) Report on
9777 procedures for the TTY as a text terminal in legacy 9-1-1 PSAPs without IP connection
9778 [175].) The NIF component will replace line delimiters used for text formatting (e.g., by i3
9779 PSAPs) with a space because most TTYs have a limited display of only one or two lines.
9780 Such line delimiters SHALL NOT cause the NIF component to change turn. In addition,
9781 words beginning with “GA” should also not cause a change of turn. It is assumed that in
9782 such cases the next character in the word will be sent within the 1500 ms.

9783 **6.1.3 Location Interwork Function (LIF)**

9784 At the request of the NIF, the LIF SHALL invoke location retrieval functionality to obtain the
9785 location information that will be used as the basis for call routing and that will be delivered
9786 to the PSAP. Specifically, the LIF SHALL query an associated location server/database.

- 9787 • If the call is a wireline emergency call, the associated database will contain location
9788 information in the form of a location value. This location value MAY be used for both
9789 routing and dispatch purposes.
- 9790 • If the call is a Phase I wireless emergency call for which static caller location
9791 information is stored locally (i.e., no query is launched to the MPC/GMLC), the
9792 associated database will obtain a routing location by accessing pre-provisioned data
9793 that maps the ESRD to a routing location chosen so that it will route to the primary
9794 PSAP that is to receive the call, and MAY use the locally stored information as the
9795 caller’s location for the call.

- 9796 • If the call is a wireless Phase II emergency call (or a Phase I wireless emergency call
9797 using this implementation), the associated database will access pre-provisioned data
9798 that maps the location key (i.e., ESRK or ESRD) provided with the call to a routing
9799 location chosen so that it will route to the target PSAP associated with the
9800 ESRK/ESRD, and will query an MPC/GMLC for caller location information.
- 9801 The data in the internal location server/database are provisioned using proprietary
9802 mechanisms/interfaces, e.g., using the existing provisioning flows, systems, and interfaces
9803 that are used for provisioning legacy ALI databases today.
- 9804 The LIF may receive one or two numbers/keys⁶⁵ from the NIF to be used for location
9805 retrieval/acquisition. Upon receiving the key(s), the LIF SHALL consult “steering” data to
9806 determine whether another system must be queried to obtain location information for
9807 dispatch purposes.
- 9808 • If a single key is received from the NIF associated with a legacy wireline origination,
9809 it will not be present in the steering data. The LIF SHALL utilize internally defined
9810 procedures/protocols to retrieve static location information which SHALL be used for
9811 both routing and dispatch purposes from an associated location server/database.
- 9812 • If the NIF provides two keys to the LIF and they are not present in the steering data
9813 (i.e., the keys include an ESRD that is associated with a Phase I wireless origination
9814 in which no MPC/GMLC query is to be launched), the LIF SHALL obtain routing
9815 location for the call by accessing pre-provisioned data in an associated database that
9816 maps the ESRD to a routing location chosen so that it will route to the target PSAP
9817 associated with the ESRD. Caller location will be retrieved from static location
9818 information accessed via internally defined procedures/protocols.
- 9819 • If the key(s) include an ESRK or ESRD that is contained in the steering data, the LIF
9820 SHALL access pre-provisioned data in an associated database that maps the location
9821 key (i.e., ESRK or ESRD) to a routing location chosen so that it will route to the
9822 target PSAP associated with the ESRK/ESRD, and will generate an E2 ESPOSREQ
9823 message, as specified in J-STD-036-C-2 [50] or Mobile Location Protocol (MLP)
9824 query, as specified in Mobile Location Protocol 3.2 (RFC 7540) [197] (as appropriate
9825 for the MPC/GMLC whose address is included in the steering data) and direct it to
9826 the MPC/GMLC identified in the steering data to obtain the caller’s location.
- 9827 If the call is from a legacy wireline originating network, it is expected that the LIF will map
9828 the CPN/ANI to a location value (in the form of a civic address) and other non-location call-

⁶⁵ Note that in some networks, the callback number, when presented to the NIF, could be more than 10 digits when the caller number is international. Many networks truncate such numbers to 10 digits. The LNG MUST NOT truncate if the originating network can present more than 10 digits.

related information (Refer to Appendix A for details on mapping between legacy and NG9-1-1 data). The location value and any non-location information will be returned to the NIF where it is used to build the corresponding Additional Data blocks.

If the call originated in a legacy wireless network using Wireline Compatibility Mode, the LIF SHALL interrogate its steering data with the ESRK. The steering data SHALL contain the address of the MPC/GMLC in the legacy wireless network that should be queried for initial/updated caller location. The LIF component SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRK to routing location chosen so that it will route to the target PSAP associated with the ESRK. The LIF component will also generate an E2 or MLP query for caller location, containing the ESRK, to the MPC/GMLC and MUST be capable of processing an E2/MLP response. The LIF component SHALL immediately return the routing location to the NIF component, along with an indication that the "Service Delivered by Provider to End User" is "wireless", and a SIP or HELD location reference that contains the ESRK and the URI of the Legacy Network Gateway. Upon receiving the caller location returned by the MPC/GMLC (which is initially expected to convey information about the location of the cell site/sector), the LIF component SHALL store the caller location and pass any non-location information received in the MPC/GMLC response, including the callback number, to the NIF component.

If the call originated in a legacy wireless network that supports the signaling of callback number and ESRD, the LIF component SHALL consult its steering data using the ESRD. The steering data includes the address of the MPC/GMLC in the legacy wireless network that should be queried for initial/updated caller location.

- If the legacy wireless network is only Phase-I-capable, the LIF may not find steering data that corresponds to the ESRD and will instead retrieve from its local database a static location value that is associated with the cell site/sector to be used as the caller location. The LIF SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRDs to routing location chosen so that it will route to the target PSAP associated with the ESRD. The LIF SHALL then pass the routing location, along with an indication that the "Service Delivered by Provider to End User" is "wireless", and originating network contact information (i.e., the "Data Provider Contact URI") to the NIF component. The LIF SHALL also pass a SIP or HELD location reference to the NIF that uniquely identifies the location information and the Legacy Network Gateway. The LIF will associate the location reference with the routing and caller location.
- If the LIF component finds steering data corresponding to the ESRD, it SHALL obtain the routing location for the call by consulting an associated database that contains static mappings of ESRD-to-routing-location chosen such that it will route to the target PSAP associated with the ESRD. The LIF component SHALL also generate an

9867 E2/MLP query for caller location, containing the callback number and ESRD, to the
9868 MPC/GMLC and MUST be capable of processing an E2/MLP response. The LIF
9869 component SHALL immediately return the routing location to the NIF component,
9870 along with an indication that the "Service Delivered by Provider to End User" is
9871 "wireless". The LIF SHALL also pass a SIP or HELD location reference to the NIF that
9872 uniquely identifies the location record and the Legacy Network Gateway. Upon
9873 receiving the caller location returned by the MPC/GMLC (which is initially expected to
9874 convey information about the location of the cell site/sector), the LIF component
9875 shall retain the caller location and associate it with the location reference. The LIF
9876 component will also pass any non-location information received in the E2/MLP
9877 response to the NIF component.

9878 Since the Legacy Network Gateway may provide a location reference (e.g., associated with
9879 a legacy wireless emergency call origination) in the INVITE that it sends to the ESRP, the
9880 LIF MUST also support the dereferencing of location references by external elements (e.g.,
9881 ESRPs, PSAPs). The interface used by a LIF for dereferencing is the same as the interface
9882 used by a LIS for dereferencing, as described in Section 3.2. Specifically, the LIF MUST
9883 support SIP and/or HELD dereferencing protocols and MUST be capable of applying the
9884 appropriate one based on the format of the location reference provided as output from the
9885 location retrieval process.

9886 **6.1.3.1 Interworking to Support Location Dereferencing**

9887 **6.1.3.1.1 Interworking Between HELD and E2**

9888 The following tables illustrate the interworking between HELD and E2 to support location
9889 dereferencing.

9890 **Table 6-1 HELD locationRequest to E2 ESPOSREQ Mapping**

HELD locationRequest→	ESPOSREQ→	Notes
locationURI	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
locationType	-	May include the optional "exact" attribute and indicates "civic" and/or "geodetic"

HELD locationRequest→	ESPOSREQ→	Notes
responseTime	Position Request Type	The HELD responseTime parameter indicates the purpose for which the location is being requested (i.e., "emergencyRouting" or "emergencyDispatch") and the amount of time the requesting entity is willing to wait for a response. Only HELD locationRequests with a responseTime of "emergencyDispatch" will be mapped to an E2 ESPOSREQ message, with a Position Request Type value set to "UPDATED or LAST KNOWN". If the wait time value in the responseTime attribute is set to 0 ms, the LNG SHALL return the most accurate location it has locally (e.g., Phase I or Phase II).
-	Package Type = Query With Permission	
-	Transaction ID	Assigned by the Legacy Network Gateway
-	Component Sequence	
-	Component Type = INVOKE (last)	
-	Component ID	Assigned by the Legacy Network Gateway
-	Operation Code = Emergency Services Position Request	
-	Parameter Set	
-	ESME Identification	Identifies the requesting entity
-	Emergency Services Routing Key	Populated with ESRK, if received by Legacy Network Gateway in incoming signaling from the MSC

[MM/DD/YYYY]

Page 345 of 675



HELD locationRequest→	ESPOSREQ→	Notes
-	Callback Number - Request	Populated with callback number if received by Legacy Network Gateway in incoming signaling from the MSC
-	Emergency Services Routing Digits - Request	Populated with ESRD if received by Legacy Network Gateway in incoming signaling from the MSC

9891

9892

Table 6-2 E2 esposreq to HELD locationResponse Mapping

esposreq→	HELD locationResponse →	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If the locationRequest contains a responseTime parameter value of "emergencyRouting," this parameter will be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Package Type = Response	-	
Transaction ID	-	
Component Sequence	-	
Component Type = Return Result (last)	-	
Component ID	-	
Parameter Set	-	
Position Result	-	Indicates whether returned position is initial, updated, last known, not available

esposreq→	HELD locationResponse →	Notes
Position Information: - Generalized Time - Geographic Position - Position Source	presence	<p>Indicates time of position determination</p> <p>One or the other of Position Information – Geographic Position or Location Description may be populated, and when present, MUST be populated with geodetic location and civic address, respectively. Both may be populated if both are available at the MPC.</p> <p>Geographic Position would map to geodetic location formatted as a PIDF-LO</p> <p>Method of location determination; Position Source maps to 'Method' parameter within PIDF-LO</p>
Callback Number - Response	-	Populated with MDN/MSISDN that identifies the caller
Emergency Services Routing Digits - Response	-	Populated with the ESRD associated with the cell site/sector from which the emergency call originated
Mobile Identification Number	-	Optional
IMSI	-	Optional
Mobile Call Status	-	Optional
Company ID	-	Carries unique identifier for the Wireless Service Provider

esposreq→	HELD locationResponse →	Notes
Location Description	presence	If present, the Location Description parameter will be used to populate a civic location in the PIDF-LO. The non-location information in this parameter will also be used by the LNG to create an Additional Data structure. See Appendix A for mappings of data elements received in Location Description Parameter to the PIDF-LO or Additional Data structure.

9893 **6.1.3.1.2 Interworking Between HELD and MLP**

9894 The following tables illustrate the interworking between HELD and MLP to support location
9895 dereferencing.

9896 **Table 6-3 HELD locationRequest to MLP ELIR Mapping**

HELD locationRequest→	MLP ELIR→	Notes
locationURI	-	Reflects the value provided in the Geolocation header field of the INVITE message sent by the LNG
locationType	-	May include the optional "exact" attribute and indicates "civic" and/or "geodetic"
responseTime	Loc_Type	The HELD responseTime parameter indicates the purpose for which the location is being requested (i.e., "emergencyRouting" or "emergencyDispatch") and the amount of time the requesting entity is willing to wait for a response. Only HELD locationRequests with a responseTime of "emergencyDispatch" will be mapped to an MLP ELIR message, in which case the Loc_Type in the ELIR will be set to "CURRENT". If the wait time value in the responseTime attribute is set to 0 ms,

HELD locationRequest→	MLP ELIR→	Notes
-		the LNG SHALL return the most accurate location it has locally (e.g., Phase I or Phase II).
-	Header: - hdr ver=" 3.2.0" - client o id o pwd o serviceid	The <i>id</i> and <i>pwd</i> contain the username and password assigned by the WSP to the ILEC and is common to all ALIs within the redundant configuration. The <i>serviceid</i> may OPTIONALLY be used by the ILEC to identify the individual ALI making the request.
-	MSID = callback number	Two different types of MSID are possible: MSISDN or MDN; type used in ELIR will be appropriate for the ESRD
-	ESRD	
-	eqop - resp_timer ¹	Indicates the maximum time the MPC/GMLC has before it must respond to the request.
-	GEO_INFO	Defines the reference coordinate system (i.e., WGS 84)

9897 ¹A value of 30 seconds is used in Canadian networks today.

9898

9899

Table 6-4 MLP ELIA to HELD locationResponse Mapping

MLP ELIA→	HELD locationResponse	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If the locationRequest contains a responseTime parameter value of "emergencyRouting," this parameter will be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Result	-	Indicates whether or not an error occurred, and if so, what type of error

MLP ELIA→	HELD locationResponse	Notes
EME_POS		
- MSID	-	From the ELIR message
- ESRD	-	From the ELIR message
- pd (Position Data)	presence	
o time		Indicates time of position determination
o shape		The shape returned in the ELIA message will be set to "Circular Area" with x and y coordinates and radius expressed in meters
o lev_conf ²		The percentage of confidence of the returned location
pos_method ³		This geo-location will be formatted as a PIDF-LO for population in the HELD locationResponse if the HELD locationRequest contains a responseTime parameter value of "emergencyDispatch"
		Method of location determination; If present, pos_method maps to 'Method' parameter within PIDF-LO

9900 ²A value of 90% is used in Canadian networks today.

9901 ³This is an EME_POS attribute and is not provided in Canadian networks today.

9902 **6.1.3.1.3 Interworking Between SIP Presence and E2**

9903 Using SIP Presence with location by reference is discussed in Section 4.10. The following
9904 tables illustrate the interworking between SIP Presence and E2 to support location
9905 dereferencing.

9906

Table 6-5 SIP Presence SUBSCRIBE to E2 ESPOSREQ Mapping

SIP Subscribe→	ESPOSREQ→	Notes
location URI (in Request-URI and To:)	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
Filter (in body)	-	MAY include rate filters and/or location filters
-	Position Request Type	Indicates whether initial or updated location is being requested; Initial NOTIFY contains the initial location, subsequent NOTIFYs contain updated location.
-	Package Type = Query With Permission	
-	Transaction ID	Assigned by the Legacy Network Gateway
-	Component Sequence	
-	Component Type = INVOKE (last)	
-	Component ID	Assigned by the Legacy Network Gateway
-	Operation Code = Emergency Services Position Request	
-	Parameter Set	
-	ESME Identification	Identifies the requesting entity
-	Emergency Services Routing Key	Populated with ESRK, if received by Legacy Network Gateway in incoming signaling from the MSC
-	Callback Number - Request	Populated with callback number if received by Legacy Network Gateway in incoming signaling from the MSC
-	Emergency Services Routing Digits - Request	Populated with ESRD if received by Legacy Network Gateway in incoming signaling from the MSC

9907

[MM/DD/YYYY]

Page 351 of 675



9908

Table 6-6 E2 ESPOSREQ to SIP Presence NOTIFY Mapping

esposreq→	SIP NOTIFY→	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; Initial NOTIFY will contain ESRK/ESRD, formatted as a PIDF-LO
Package Type = Response	-	
Transaction ID	-	
Component Sequence	-	
Component Type = Return Result (last)	-	
Component ID	-	
Parameter Set	-	
Position Result	-	Indicates whether returned position is initial, updated, last known, not available
Position Information: - Generalized Time - Geographic Position 1. - Position Source	presence	Indicates time of position determination One or the other of Position Information – Geographic Position or Location Description may be populated, and when present , MUST be populated with geodetic location and civic address, respectively. Both may be populated if both are available at the MPC. Geographic Position would map to geodetic location formatted as a PIDF-LO Method of location determination: Position Source maps to 'Method' parameter within PIDF-LO
Callback Number - Response	-	Populated with MDN/MSISDN that identifies the caller
Emergency Services Routing Digits - Response	-	Populated with the ESRD associated with the cell site/sector from which the emergency call originated

[MM/DD/YYYY]

Page 352 of 675



esposreq→	SIP NOTIFY→	Notes
Mobile Identification Number	-	Optional
IMSI	-	Optional
Mobile Call Status	-	Optional
Company ID	-	Carries unique identifier for the Wireless Service Provider
Location Description	presence	If present, the Location Description parameter SHALL be used to populate a civic location in the PIDF-LO. The non-location information in this parameter SHALL also be used by the LNG to create an Additional Data structure. See Appendix A for mappings of data elements received in Location Description Parameter to the PIDF-LO or Additional Data structure.

9909 **6.1.3.1.4 Interworking Between SIP Presence and MLP**

9910 The following tables illustrate the interworking between SIP Presence and MLP to support
9911 location dereferencing.

9912 **Table 6-7 SIP Presence SUBSCRIBE to MLP ELIR Mapping**

SIP SUBSCRIBE→	MLP ELIR→	Notes
location URI (in Request-URI and To:)	-	Reflects value provided in the Geolocation header field of the INVITE message sent by the LNG
Filter (in body)	-	May include rate filters and/or location filters
-	Loc_Type	The SUBSCRIBE is mapped to an MLP ELIR message with Loc_Type set to "CURRENT"; Initial NOTIFY contains the most accurate location the LIF has locally at the time of subscription (i.e., Phase I or Phase II), the next NOTIFY contains the updated location.

SIP SUBSCRIBE→	MLP ELIR→	Notes
-	Header: - hdr ver=" 3.2.0" - client o id o pwd o serviceid	The <i>id</i> and <i>pwd</i> contain the username and password assigned by the WSP to the ILEC and is common to all ALIs within the redundant configuration. The <i>serviceid</i> MAY optionally be used by the ILEC to identify the individual ALI making the request.
-	MSID = callback number	Two different types of MSID are possible: MSISDN or MDN; type used in ELIR will be appropriate for the ESRD
-	ESRD	
-	eqop - resp_timer ¹	Indicates the maximum time the MPC/GMLC has before it must respond to the request.
-	GEO_INFO	Defines the reference coordinate system (i.e., WGS 84)

9913

¹A value of 30 seconds is used in Canadian networks today.

9914

Table 6-8 MLP ELIA to SIP Presence NOTIFY Mapping

MLP ELIA→	SIP NOTIFY→	Notes
-	presence	Contains civic and/or geodetic location populated in a PIDF-LO; If this is the first NOTIFY, this parameter SHALL be populated with the location mapped from the ESRK/ESRD, formatted as a PIDF-LO
Result	-	Indicates whether or not an error occurred, and if so, what type of error

MLP ELIA→	SIP NOTIFY→	Notes
EME_POS		
- MSID	-	From the ELIR message
- ESRD	-	From the ELIR message
- pd (Position Data)	presence	
o Time		Indicates time of position determination
o Shape		The shape returned in the ELIA message will be set to "Circular Area" with x and y coordinates and radius expressed in meters
o lev_conf ²		The percentage of confidence of the returned location
pos_method ³		This geo-location SHALL be formatted as a PIDF-LO for population in the NOTIFY if this is not the first one.
		Method of location determination; If present, pos_method maps to 'Method' parameter within PIDF-LO

9915 ²A value of 90% is used in Canadian networks today.

9916 ³This is an EME_POS attribute and is not provided in Canadian networks today.

9917 **6.1.3.2 Call Flow Example**

9918 Figure 6-2 illustrates a call flow in which a legacy wireless emergency call origination is
 9919 routed via a Legacy Network Gateway to an ESRP in an i3 ESInet. This call flow assumes
 9920 that the MSC delivers the call to the Legacy Network Gateway with an ESRK only. It also
 9921 assumes that there is only one ESRP in the call path, and that HELD is used as the
 9922 dereferencing protocol.

9923

[MM/DD/YYYY]

Page 355 of 675



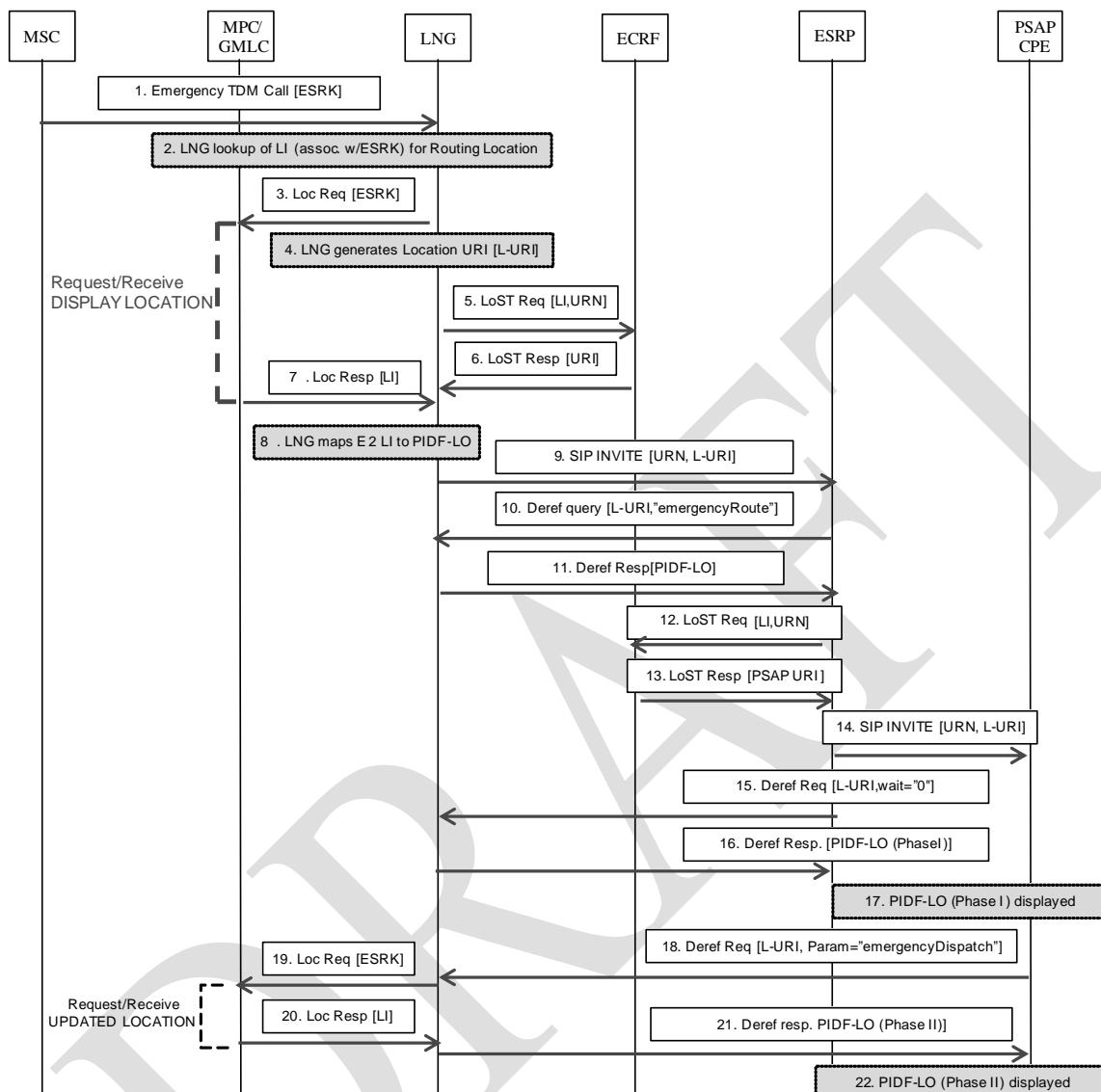


Figure 6-2 Example Call Flow

- 9924 1. A legacy wireless emergency call origination is signaled from the MSC to the Legacy Network Gateway with an ESRK.
- 9925 2. The Legacy Network Gateway maps the ESRK to a Routing Location (i.e., Location Information [LI]) that is chosen so that it will route to the PSAP that is associated with that ESRK.
- 9926 3. The Legacy Network Gateway initiates a Location Request (e.g., an E2 ESPOSREQ) to the MPC/GMLC that contains the ESRK.

- 9933 4. The Legacy Network Gateway generates a location reference in the form of a HELD
9934 location URI. (Note that this can happen prior to Step 3.)
9935 5. The Legacy Network Gateway sends a routing request to the ECRF that contains a
9936 service URN and the Routing Location (i.e., LI from Step 2).
9937 6. The Legacy Network Gateway receives a routing response from the ECRF that
9938 contains the next hop ESRP URI.
9939 7. Sometime after Step 3, the Legacy Network Gateway receives Phase I Location
9940 Information (Phase I LI) from the MPC/GMLC.
9941 8. The Legacy Network Gateway maps the LI received from the MPC/GMLC to a
9942 PIDF-LO based on a mapping rule set (e.g., by accessing the MSAG Conversion
9943 Service [MCS]).
9944 9. The Legacy Network Gateway forwards the SIP INVITE message to the ESRP (via a
9945 BCF which is not pictured). The INVITE message includes the location URI (from
9946 Step 4) in the Geolocation header field.
9947 10. The ESRP sends a HELD dereference request to the Legacy Network Gateway. The
9948 HELD locationRequest includes the location URI and a responseTime parameter set
9949 to "emergencyRouting".
9950 11. The Legacy Network Gateway returns the Routing Location to the ESRP formatted as
9951 a PIDF-LO.
9952 12. The ESRP sends a routing request to the ECRF that contains a Service URN and the
9953 Routing Location.
9954 13. The ESRP receives a routing response from the ECRF that contains a PSAP URI.
9955 14. The ESRP forwards the SIP INVITE to the PSAP CPE. The INVITE contains the
9956 location URI from Step 4.
9957 15. The PSAP CPE sends a HELD dereference request to the Legacy Network Gateway.
9958 The HELD locationRequest includes the location URI, and a responseTime parameter
9959 indicating a wait time of "0 ms". This tells the Legacy Network Gateway that it
9960 should return whatever location is currently available (i.e., the Phase I location
9961 received in Step 7).
9962 16. The Legacy Network Gateway returns Phase I location information to the PSAP CPE,
9963 formatted as a PIDF-LO (from Step 8).
9964 17. The Phase I location information is displayed at the PSAP CPE.
9965 18. After waiting 30 seconds, the PSAP CPE sends an additional HELD dereference
9966 request to the Legacy Network Gateway. The HELD locationRequest includes the
9967 location URI, and a responseTime parameter set to "emergencyDispatch."
9968 19. The Legacy Network Gateway sends a Location Request (i.e., E2 ESPOSREQ) to the
9969 MPC/GMLC, requesting updated/last known location. The Location Request includes
9970 the ESRK that was provided in call setup signaling from the MSC.
9971 20. The MPC/GMLC returns updated/last known location (i.e., in an esposreq message).

[MM/DD/YYYY]

Page 357 of 675



- 9972 21. The Legacy Network Gateway returns the updated/last known Phase II location
9973 information to the PSAP, formatted as a PIDF-LO, in a HELD locationResponse
9974 message.
9975 22. The Phase II location information is displayed at the PSAP CPE.

9976 **6.2 Legacy PSAP Gateway (LPG)**

9977 The Legacy PSAP Gateway is a signaling and media interconnection point between an
9978 ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse
9979 an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of
9980 emergency calls between legacy PSAPs and i3 PSAPs. The Legacy PSAP Gateway supports
9981 an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced
9982 MF interface (comparable to the interface between a traditional Selective Router (SR) and a
9983 legacy PSAP, described in NENA 03-002 [163]) on the other. The Legacy PSAP Gateway
9984 also includes an ALI interface (as defined in NENA-STA-027 [164] or NENA 04-005 [165])
9985 that can accept an ALI query from the legacy PSAP. The legacy PSAP controller supplies an
9986 appropriate ALI query key (i.e., “ANI”) for the call. When queried with this key, the Legacy
9987 PSAP Gateway responds with the location. If the emergency call routed via the ESInet
9988 contains a location by value, the Legacy PSAP Gateway responds with that value, formatted
9989 appropriately for the receiving PSAP. If the ESInet provides a location by reference, the ALI
9990 query to the Legacy PSAP Gateway results in a dereference operation from the gateway to
9991 the LIS or Legacy Network Gateway. The results of the dereference operation are returned
9992 to the Legacy PSAP Gateway, and subsequently passed from the Legacy PSAP Gateway to
9993 the legacy PSAP. The ALI response generated by the Legacy PSAP Gateway will also
9994 contain additional information that may be obtained from a variety of sources. See Section
9995 6.2.2 for further discussion.

9996 The Legacy PSAP Gateway functional element contains three functional components, as
9997 illustrated in Figure 6-1⁶⁶:

- 9998 1. (SIP-MF/E-MF/DTMF) Protocol Interwork Function (PIF). This functional component
9999 interworks the SIP protocol to traditional MF, Enhanced MF, or ISDN, or other

66 Note that the functional decomposition of the Legacy PSAP Gateway described in this section is provided to assist the reader in understanding the functions and external interfaces that a Legacy PSAP Gateway must support. Actual implementations MAY distribute the functionality required of the Legacy PSAP Gateway differently among functional components, as long as all of the functions and external interfaces described herein are supported.

10000 protocols, as appropriate for the interconnected PSAP⁶⁷. If the PIF component
10001 determines that the call is to be delivered to the PSAP as a TTY call, the PIF
10002 component will be responsible for interworking real-time text and TTY per RFC 5194
10003 [84]. The PIF component MUST also be capable of interworking text messages
10004 received in an MSRP session with TTY. It is assumed that the PIF functional
10005 component does not require specialized hardware, and can therefore be
10006 implemented using commercially available hardware. (See Section 6.2.1 for further
10007 details.)

10008 2. NG9-1-1-specific Interwork Function (NIF). This functional component provides
10009 NG9-1-1-specific processing of the call signaling, which includes special handling of
10010 attached location, selection of trunk groups, and callback number mapping, etc. The
10011 NIF associates one form of identifier with another, which includes mapping any
10012 combination of identifiers, such as 10-digit NANP numbers, non-NANP identifiers
10013 (pANIs), E.164 (International 11-15 digit) identifiers, and SIP URIs. For example,
10014 when a call is received with location and a SIP URI and it is destined for a legacy
10015 PSAP, the NIF maps the attached location and callback identifier information to a
10016 pANI that is then delivered to the PSAP with the call and used by the PSAP as a key
10017 for subsequent location and callback information retrieval. In addition, the NIF
10018 includes functionality to support transfer requests and, optionally, requests for the
10019 invocation of alternate routing (e.g., in cases of PSAP evacuation). This functional
10020 component should be viewed as a Back-to-Back User Agent (B2BUA) in front of the
10021 PIF. (See Section 6.2.2 for further details.)

10022 3. Location Interwork Function (LIF). This functional component supports standard ALI
10023 query/response interface protocols, as well as the interworking of NG9-1-1 relevant
10024 data elements to a standardized ALI format for population in ALI response
10025 messages. (See Section 6.2.3 for further details.)

10026 The LPG MUST implement the server-side of the ElementState event notification package.
10027 The following subsections describe each of these functional components of the Legacy
10028 PSAP Gateway in detail.

10029 **Note:** The LPG MUST log all significant events. Log record formats for this purpose are
10030 provided in Section 4.12.3 of this document.

⁶⁷ Note that only interworking between SIP and traditional MF, E-MF, and DTMF signaling are addressed in this specification. Interworking with ISDN and other protocols that may be used by legacy PSAPs is outside the scope of this specification.

10031 **6.2.1 Protocol Interwork Function (PIF)**

10032 The PIF component of the Legacy PSAP Gateway will be responsible for interworking the
10033 SIP signaling received from the NIF component with the traditional or Enhanced MF
10034 signaling sent over the interface to the destination PSAP. The PIF will also be responsible
10035 for accepting Dual Tone Multi-Frequency (DTMF) signaling (e.g., associated with transfer
10036 requests) from the legacy PSAP and sending it to the NIF component in RTP packets, per
10037 RFC 4733 [142].

10038 The PIF component of the Legacy PSAP Gateway MUST be capable of accepting a SIP
10039 INVITE message generated by the NIF component (see Section 6.2.2.3).

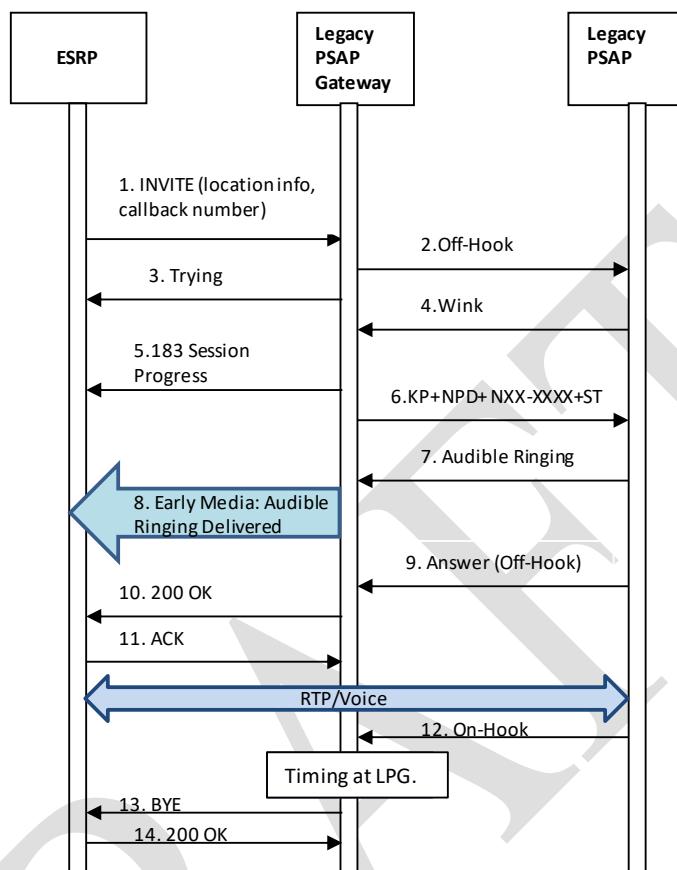
10040 Upon receiving the INVITE method, the PIF component of the Legacy PSAP Gateway
10041 SHALL identify the destination PSAP based on the information in the Request-URI and
10042 select an outgoing trunk to that PSAP based on the outgoing trunk group information in the
10043 Request-URI. Based on the information received in incoming signaling from the NIF
10044 component, the PIF component SHALL generate either traditional MF (i.e., 8-digit CAMA) or
10045 Enhanced MF (E-MF) call signaling. In both cases, the MF signaling sequences used in
10046 delivering emergency calls to legacy PSAPs include a “Special Handling” indication along
10047 with the ANI⁶⁸. (See Section 6.2.2.2 for further information.) Legacy PSAPs that support
10048 E-MF interfaces MAY support the delivery of a 10-digit key or pANI that serves as a
10049 reference to the caller’s location information in addition to a 10-digit callback number and
10050 “Special Handling” indication. The traditional MF and E-MF signaling interfaces that may be
10051 supported by a legacy PSAP are described below.

10052 **6.2.1.1 Traditional MF Interface**

10053 If a traditional MF interface is supported by the legacy PSAP, the signaling interworking
10054 provided by the Legacy PSAP Gateway will be as depicted below:

10055

68 The “ANI” may contain the caller’s callback information or a query key (i.e., a pANI).



10056

10057

Figure 6-3 Call Delivery With Traditional MF Interface to PSAP

10058 The emergency call delivery flow illustrated above begins when the ESRP determines that a
10059 call is to be delivered to a particular PSAP, and that the route to that PSAP is via the
10060 Legacy PSAP Gateway. Note that if this call was being delivered to the Legacy PSAP
10061 Gateway by a network that has implemented the Route All Calls Via a Conference Aware
10062 UA model, the ESRP in this call flow would be replaced by an ESRP/Conference Aware UA.
10063 This flow illustrates disconnect being initiated by the PSAP.

- 10064 1. The ESRP constructs a SIP INVITE and sends it to the Legacy PSAP Gateway. The
10065 SIP INVITE is populated as described in RFC 3261 [10], with the clarifications
10066 provided in Sections 3.1 and 6.2.2.
- 10067 2. When the NIF component of the Legacy PSAP Gateway receives the INVITE
10068 message, it follows the procedures described in RFC 3261 [10] for processing the
10069 INVITE, with the following clarifications. The NIF component of the Legacy PSAP
10070 Gateway uses the content of the INVITE to determine that the call is an emergency
10071 call, and to determine the information that will be signaled to the PSAP CPE to
10072 support such functions as display of ANI and queries for ALI information (i.e., the

- 10073 Numbering Plan Digit [NPD]⁶⁹ and ANI digits to be signaled via MF to the legacy PSAP).
- 10075 If the INVITE contains both callback information and location information, the NIF component SHALL be provisioned to determine, on a per-PSAP basis, whether the information signaled as the ANI will be associated with the callback information or the location information.
- 10079 It is desirable that a callback number be delivered to the PSAP as the "ANI" for emergency calls that traverse an i3 ESInet, whenever possible. This will give the PSAP the ability to call back the emergency caller even if attempts to access ALI information are unsuccessful.
- 10083 If, based on provisioning, the PSAP should receive callback information, the ANI will usually be based on the callback number/address included in the P-A-I (if available) or the From header field of the incoming INVITE message.
- 10086 If the P-A-I or the From header field contains callback information that is in the form of a 10-digit NANP number, and the NPA portion of that number is appropriate for the target PSAP (i.e., can be associated with an appropriate NPD value), the NIF SHALL identify an NPD associated with the NPA and SHALL signal the NPD-NXX-XXXX in the From header field of the INVITE message sent to the PIF component. The PIF component SHALL then prepare to signal that NPD along with the NXX-XXXX portion of the callback number received in the incoming INVITE message in the ANI sequence.
- 10094 If the P-A-I or the From header field in the INVITE message received by the NIF contains callback information that is either not in the form of a 10-digit NANP number, or is in the form of a 10-digit NANP number, but the NPA portion of that number is not appropriate for the target PSAP, the NIF SHALL identify an NPD associated with an NPA that is appropriate for the target PSAP, and SHALL generate locally a 7-digit pANI that consists of the following:
- 10100 • An NXX of "511"
- 10101 • An XXXX consisting of a sequential number from 0000 to 9999 with wrap around⁷⁰.

⁶⁹ See Section 6.2.2.2 for further discussion of NPD digits.

⁷⁰ Because the pANI is only sent by the Legacy PSAP Gateway to the legacy PSAP, and is not sent onward to any other entity, there is no significance beyond the gateway and the legacy PSAP.

- 10103 The NIF SHALL signal the pANI in the From header field of the INVITE message it
10104 sends to the PIF.
- 10105 If, based on provisioning, the PSAP should only receive a location key, the NIF
10106 SHALL signal that information to the PIF in a From header field that consists of an
10107 NPD associated with an NPA that is appropriate for the target PSAP and a 7-digit
10108 pANI of the form 511-XXXX.
- 10109 The PIF component of the Legacy Network Gateway creates connectivity (i.e., seizes
10110 an MF trunk) to the PSAP CPE for the emergency call.
- 10111 3. After sending the INVITE message to the PIF component, the NIF component sends
10112 a SIP 100 Trying message to the ESRP. The PIF also sends a SIP 100 Trying
10113 message to the NIF component (not shown).
- 10114 4. The PSAP CPE responds with a "wink" indicating that it is ready to receive further
10115 signaling related to the emergency call.
- 10116 If the PSAP fails to respond with a wink within four (4) seconds⁷¹, the Legacy PSAP
10117 Gateway SHALL treat the call attempt as a failure, mark the PSAP trunk, and alert
10118 management personnel to the situation. If this is a first failure on the call, the
10119 Legacy PSAP Gateway SHALL make a second attempt on another PSAP trunk circuit
10120 or re-attempt on the same circuit after a sufficient guard time period to allow the
10121 PSAP trunk to idle itself in preparation for a subsequent call attempt. If the call
10122 failure is on a second attempt, the Legacy PSAP Gateway SHALL deem the call a
10123 failure, and return a SIP 500 Server Internal Error message to the NIF component,
10124 indicating that it was unable to present the call to the legacy PSAP. The NIF
10125 component SHALL signal the SIP 500 Server Internal Error message back to the
10126 ESRP. (See Section 6.2.4.1 for further information on call setup timing at the Legacy
10127 PSAP Gateway.)
- 10128 5. The PIF component signals a SIP 183 Session Progress back to the NIF (not shown),
10129 and the NIF signals a SIP 183 Session Progress message back to the ESRP,
10130 indicating that connectivity should be established in the backward direction to
10131 support call progress signaling (i.e., early media/audible ringing) provided by PSAP
10132 CPE. The Contact header field in the SIP 183 Session Progress message sent by the
10133 NIF to the ESRP shall include a "text" media feature tag.
- 10134 6. The PIF signals an MF digit string consisting of a Key Pulse (KP) signal followed by
10135 the NPD and seven NXX-XXXX digits derived in Step 2. The MF signaling sequence

⁷¹ The 4-second timer is specified in ATIS-0600414.1998(R2007), *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling*. [188]

- 10136 ends with the Start (ST) signal. (See GR-350-CORE [189] or NENA-STA-027 [164]
10137 for further discussion of signaling sequences associated with traditional MF
10138 interfaces.)
10139 7. Upon receiving complete ANI information, the PSAP signals the attendant and
10140 returns audible ringing to the calling party.
10141 8. Early media/audible ringing is delivered via the ESRP to the calling UA.
10142 9. The PSAP call taker answers the call and the off-hook signal is conveyed to the PIF.
10143 10. The PIF component sends a SIP 200 OK message to the NIF component (not
10144 shown) and the NIF component sends a SIP 200 OK message to the ESRP.
10145 11. The ESRP forwards the SIP ACK generated by the calling UA to the NIF component
10146 of the Legacy PSAP Gateway to confirm acceptance of the answer indication. The
10147 NIF component forwards the SIP ACK to the PIF component (not shown).
10148 *The media streams are established. The caller and the PSAP call taker can now
10149 communicate.*
10150 12. In this example flow, the PSAP initiates the release of the call by sending an on-
10151 hook signal to the Legacy PSAP Gateway.
10152 The Legacy PSAP Gateway MUST determine if the on-hook condition is a true
10153 disconnect (i.e., the on-hook condition persists for >1100ms), or a hook flash
10154 (500ms +/- 250ms). Therefore, in this example, where the PSAP disconnects first,
10155 there will be a timing interval between the on-hook signal from the PSAP, and the
10156 SIP BYE message being sent (in Step 13). It is RECOMMENDED that this interval be
10157 a minimum of 1100ms. See Section 6.2.4.2 for further information about call
10158 disconnect timing.
10159 13. In response to receiving the on-hook signal from the legacy PSAP CPE, the PIF
10160 component sends a SIP BYE message to the NIF (not shown) and the NIF
10161 component sends a BYE message to the ESRP.
10162 14. The ESRP forwards the 200 OK message generated by the calling UA, confirming the
10163 call termination.

10164 **6.2.1.2 Enhanced MF (E-MF) Interface**

10165 As described in Section 6.2.2.3, the use of E-MF signaling on an interface to a legacy PSAP
10166 will be selectable on a trunk group basis by the Legacy PSAP Gateway. A legacy PSAP that
10167 supports an E-MF interface may be capable of receiving one or two MF signaling
10168 sequences. If a PSAP supports the delivery of only one 10-digit number, and only the
10169 callback number, referred to in E-MF as the Calling Station Number, is available, the PIF
10170 component of the Legacy PSAP Gateway SHALL signal the following:

10171 **KP + II + NPA NXX XXXX ST',**

[MM/DD/YYYY]

Page 364 of 675



10172 where NPA NXX XXXX is the Calling Station Number obtained from the From header field of
10173 the incoming INVITE message sent by the NIF and the ST' denotes the omission of the
10174 second 10-digit number sequence. The value to be signaled forward in the II digits will be
10175 obtained from the oli parameter in the From header field of the INVITE message from the
10176 NIF. (See Section 6.2.2.2 for further discussion of encoding of the II digits.) Today, this
10177 scenario is typically associated with the delivery of wireline emergency calls to legacy
10178 PSAPs.

10179 When the PSAP supports delivery of two 10-digit numbers via the E-MF interface, the PIF
10180 component of the Legacy PSAP Gateway shall signal the following:

KP + II + NPA NXX XXXX ST KP NPA NXX XXXX ST

10182 where the first NPA NXX XXXX is the callback/Calling Station Number received in the P-A-I
10183 header field of the INVITE from the NIF and the second NPA NXX XXXX contains a location
10184 key/reference formatted as a 10-digit NANP number obtained from the From header field
10185 of the INVITE message from the NIF. The value to be signaled forward in the II digits will
10186 be obtained from the oli parameter in the P-A-I header field of the INVITE message from
10187 the NIF. (See Section 6.2.2.2 for further discussion of the encoding of the II digits.)⁷²
10188 Today, this scenario is typically associated with the delivery of wireless emergency calls to
10189 legacy PSAPs.

10190 With respect to emergency call originations routed via a legacy Emergency Services
10191 Network, if a PSAP is capable of receiving only one 10-digit number, and both the callback
10192 number/Calling Station Number and location reference are available at the SR, the SR is
10193 provisioned to determine, on a per-PSAP basis, whether to signal the Calling Station
10194 Number or the location reference. For VoIP emergency call originations routed via an
10195 ESInet/NGCS, if the PSAP is only capable of receiving one 10-digit number, and both
10196 callback information and location information are received by the Legacy PSAP Gateway in
10197 the incoming INVITE, the NIF component of the Legacy PSAP Gateway SHALL determine,
10198 on a per-PSAP basis, whether to signal the callback information or location information to
10199 the legacy PSAP. In either case the PIF component of the Legacy PSAP Gateway shall
10200 signal the following:

KP + II + NPA NXX XXXX + ST'

10202 where NPA NXX XXXX is the one 10-digit number specified by the PSAP and provided in the
10203 From header field of the incoming INVITE message from the NIF. The II value to signal

⁷² See GR-2953-CORE [190] or NENA 03-002 [163] for further discussion of MF signaling sequences associated with E-MF interfaces.

10204 forward will be determined based on the information in the oli parameter in the From
10205 header field of the received INVITE message.

10206 (See Section 6.2.2.2 for a discussion of the encoding of the II digits under the above
10207 scenarios.)

10208 The call flow for a legacy PSAP that utilizes an E-MF interface is the same as that depicted
10209 in Figure 6-2 for a PSAP that utilizes a traditional MF interface, with the following
10210 modifications:

- 10211 • In Step 3, the NIF component of the Legacy PSAP Gateway will determine, via
10212 provisioning, whether one or two 10 digit numbers are to be signaled to the
10213 destination PSAP, and will populate that information accordingly in the INVITE
10214 message it sends to the PIF (see Section 6.2.2.3.1). The PIF will determine the
10215 information to be populated in that/those signaling sequence(s) based on the
10216 information received in the INVITE from the NIF.

10217 If, based on provisioning, the PSAP is supposed to receive two 10-digit numbers, the
10218 NIF will include a P-A-I header field containing callback information and a From
10219 header field containing location information in the INVITE message it sends to the
10220 PIF. The PIF will use the callback information in the P-A-I to populate the first MF
10221 sequence, and the location key/reference from the From header field to populate
10222 the second MF sequence.

10223 The PIF will populate the II digits based on the oli parameter in the P-A-I header
10224 field of the INVITE from the NIF.

10225 If, based on provisioning, the PSAP is supposed to receive only a single 10-digit
10226 number, the NIF will populate the associated information in the From header field of
10227 the INVITE message it sends to the PIF. The PIF will take the information from the
10228 From header field of the received INVITE to populate the single outgoing MF
10229 sequence. The PIF will populate the II digits based on the oli parameter in the From
10230 header field of the INVITE from the NIF.

- 10231 • In Step 6, the signaling sequence generated by the PIF SHALL either consist of KP +
10232 II + NPA NXX XXXX ST' or KP + II + NPA NXX XXXX ST KP NPA NXX XXXX ST. If the
10233 PIF only receives a From header field in the INVITE message from the NIF, it SHALL
10234 populate the MF signaling sequence KP + NPA NXX XXXX + ST' based on this
10235 information. If the PIF receives both a From header field and a P-A-I header field in
10236 the INVITE message from the NIF, it SHALL populate the first MF sequence based
10237 on the content of the P-A-I header field, and the second MF sequence based on the
10238 content of the From header field.

10239 If the PIF receives a From header field and no P-A-I header field in the INVITE
10240 message from the NIF, it SHALL populate the II digits based on the oli parameter in
10241 the From header field. If the PIF receives both a From header field and a P-A-I
10242 header field in the INVITE message from the NIF, it SHALL populate the II digits
10243 based on the oli parameter in the P-A-I header field.

10244 **6.2.1.3 Handling of Media Associated with TTY Calls**

10245 If an incoming call is to be delivered by the Legacy PSAP Gateway to the PSAP as a TTY
10246 call, the PIF component will be responsible for recognizing the media format provided in
10247 the SDP as being associated with real-time text and generating Baudot tones for delivery to
10248 the legacy PSAP.

10249 If a legacy PSAP responds to an incoming call by generating Baudot tones, the PIF
10250 component SHALL be responsible for recognizing the Baudot tones in incoming media and
10251 replacing them with RFC 4103 [85] real-time text.

10252 If an emergency call is presented to the PSAP as a "silent" call, (causing the PSAP to
10253 generate Baudot tones toward the caller), the PIF component of the Legacy PSAP Gateway
10254 MUST be capable of generating a re-INVITE message (upon receipt of the Baudot tones
10255 from the PSAP) and sending it to the NIF component to request the establishment of a
10256 real-time text media session over which the RFC 4013 [85] real-time text (which the PIF
10257 component transcodes from the incoming Baudot tones) can be sent. The PIF component
10258 SHALL buffer any real-time text that is converted from the received Baudot tones until such
10259 time as the text media session is established (i.e., until a 200 OK message is received from
10260 the NIF component in response to the re-INVITE) and the real-time text can be passed
10261 forward. The re-INVITE message generated by the PIF component of the Legacy PSAP
10262 Gateway SHALL include the following information:

- 10263 • A Request-URI that contains a URI populated based on the content of the Contact
10264 header field received in the initial INVITE message.
 - 10265 o If the initial emergency call was routed to the LPG via a network that has
10266 implemented the transfer procedures described in Section 4.7.1.1, the
10267 Request-URI SHALL contain a URI that is associated with the Legacy Network
10268 Gateway or caller.
 - 10269 o If the initial emergency call was routed to the LPG via a network that has
10270 implemented the transfer procedures described in Section 4.7.1.2, the
10271 Request-URI SHALL contain a URI that is associated with the B2BUA.
 - 10272 o If the initial emergency call was routed to the LPG via network that has
10273 implemented the Route All Calls Via a Conference Aware UA model (see
10274 Section 4.7.1.3), the Request-URI SHALL contain a URI that is associated
10275 with the Conference Aware UA.

- 10276 • A To header field that contains the information delivered to the Legacy PSAP
10277 Gateway in the From header field of the original INVITE message.
- 10278 • A From header field that contains the digits "911" expressed as a URI (received in
10279 the To header field of the original INVITE message).
- 10280 • A Contact header field that contains the content of the Request-URI provided in the
10281 initial INVITE message (i.e., a PSAP URI resolving at the gateway expressed as a tel
10282 URI or a sip URI of the form "sip:<TN>@psap1.gateway.com;user=phone", along
10283 with the trunk group parameters that identify the outgoing trunk group to the
10284 destination PSAP).
- 10285 • A Via header field that is populated with a URI associated with the Legacy PSAP
10286 Gateway.
- 10287 • An SDP offer that includes a media format associated with real-time text, as
10288 described in RFC 4103 [85].

10289 Upon receiving the re-INVITE message from the PIF component, the NIF component
10290 SHALL pass the re-INVITE message toward the caller/Legacy Network Gateway/ingress
10291 LSRG, as described in Section 6.2.2.4. When the NIF component receives a 200 OK
10292 message indicating that the SDP offer associated with real-time text has been accepted, it
10293 SHALL pass the 200 OK message to the PIF component. The PIF component SHALL
10294 respond by sending an ACK to the NIF component, and the NIF component SHALL send an
10295 ACK toward the caller/Legacy Network Gateway/ingress LSRG.

10296 **6.2.1.4 Handling of Media Associated with SMS/MMS⁷³, Instant Messaging 10297 and RTT**

10298 Interworking of SMS/MMS and Instant Messaging (IM) to MSRP is expected to occur
10299 outside the ESInet, but Legacy PSAPs MUST have the capability to accept SMS/MMS/IM
10300 text messages that are interworked from MSRP to TTY. Interworking between MSRP and
10301 TTY MUST occur within the LPG. The LPG MUST also be capable of receiving RTT RTP
10302 packets and interworking them to TTY (Baudot tones) for delivery to legacy PSAPs. RFC
10303 4103 describes a mechanism for carrying real-time text conversation session contents in
10304 RTP packets, but provides little guidance for handling the "turn-taking" that is inherent in
10305 interworking with TTY devices. There are currently no industry standards that describe this
10306 critical aspect of interworking with TTY. The FCC EAAC Report on "Proposed procedures for
10307 the TTY as a text terminal in legacy 9-1-1 PSAPs without IP connection" [175] provides
10308 some recommendations for the use of TTY terminals in legacy 9-1-1 PSAPs as text

73 As specified in ATIS J-STD-110.v002 [191], only the text portion of an MMS origination is presented to the ESInet.

10309 terminals that can support more modern forms of text communication. In this context, the
10310 EAAC Report provides guidance related to the interworking of TTY with RTT and MSRP.

10311 To support RTT, the PIF MUST interwork the RFC 4103 real-time text forwarded by the NIF
10312 to Baudot tones and MUST interwork Baudot tones generated by a legacy PSAP to RTT RTP
10313 packets and pass them toward the caller via the NIF component. There are also
10314 considerations for this interworking related to collision control and character mapping.

10315 TTY can transmit in one direction at a time (half-duplex) and has created a need for strict
10316 "turn-taking" procedures. In the legacy environment, these procedures are adhered to by
10317 the users at each end. However, when a network element (e.g., an LPG) interworks
10318 between IP and TTY, that network element MUST emulate these procedures. This is also
10319 true given that the caller is unaware that his/her text session is being interworked to TTY
10320 and as such cannot be expected to abide by the turn-taking procedures dictated by TTY.
10321 The NIF component of the Legacy PSAP Gateway is responsible for facilitating the "turn-
10322 taking" expected by the TTY users involved in the conversation. (See Section 6.2.2.5 for
10323 further details.)

10324 When the PIF component receives RFC 4103 real-time text packet from the NIF component
10325 over an established text media stream, the PIF component SHALL interwork the text
10326 characters to Baudot tones.

10327 RFC 4103 states that "...common mean character transmission rate, during a complete
10328 PSTN text telephony session, is around two characters per second". It also states, "A
10329 maximum performance of 20 characters per second is enough even for voice-to-text
10330 applications." The EACC Report states, "TTY transmission is only at a speed of around 5
10331 characters per second." This standard RECOMMENDS that the five (5) character per second
10332 guideline for transmission rate be followed. If RTT packets are received by the PIF
10333 component faster than the TTY transmission rate, they MUST be buffered.

10334 TTY also restricts the character sets that can be used. The PIF component SHALL apply the
10335 following character mapping as defined in the EAAC Report [175] when translating from
10336 RFC 4103 text to TTY.

10337

- 10338 • During transmission, the PIF component SHALL check every character for validity in
the TTY character set.
- 10339 • The PIF component shall convert upper case to lower case
- 10340 • The PIF component SHALL support the following translation of the special characters
10341 that have no representation in TTY:

10342

RTT	TTY
At sign character "@"	Replace with "(at)"
Octothorpe or hash sign character "#"	Replace with dollar sign character "\$"

RTT	TTY
Percentage character “%”	Replace with slash character “/”
Ampersand character “&”	Replace with plus sign character “+”
Asterisk character “*”	Replace with a period character “.”
Underscore character “_”	Replace with space character “ ”
Less than sign character “<”	Replace with left parenthesis character “(“
Greater than sign character “>”	Replace with right parenthesis character “)”
National character	Replace with the closest companion in the a-z character range (e.g., “ñ” => “n”)
Unknown character ⁷⁴	Replace with apostrophe character ‘

- 10343 • The PIF component shall convert to 5-bit code and add shift character if needed.
 10344 • The PIF component SHALL transmit according to TIA 825A [183].

10345 If the PIF component receives simultaneous RTT text and audio media associated with an
 10346 emergency call (or one media type is added to an existing session involving the other
 10347 media type), and since the audio media may include Baudot tones or other audio sounds,
 10348 the PIF component MUST notch the audio frequencies used for Baudot tones from the
 10349 received audio media and then insert the Baudot tones transcoded from the received RFC
 10350 4103 text to minimize the distortion of the Baudot tones delivered to the PSAP.

10351 If a caller requests the use of Hearing Carry Over (HCO) or Voice Carry Over (VCO), the
 10352 PSAP may need to switch between voice and TTY on a single call. The PIF component
 10353 SHALL map voice received from the PSAP into RTP voice and Baudot tones received from
 10354 the PSAP into RFC 4103 text.

10355 SMS/MMS/IM text to 9-1-1 messages are delivered to the LPG using MSRP. MSRP
 10356 messages are sent in “session mode” in which the entire message is sent. The NIF
 10357 component is responsible for caching the MSRP message and converting it to RFC 4103
 10358 real-time text for delivery to the PIF component. The PIF component of the LPG MUST
 10359 convert the RFC 4103 text to TTY for delivery to a legacy PSAP. As for the RTT case, the
 10360 NIF component SHALL be responsible for maintaining the conventions associated with TTY
 10361 calling (See Section 6.2.2.5). Upon determining that the call taker has joined the
 10362 conversation (via receipt of an appropriate preprogrammed or typed message such as “911
 10363 GA”), the PIF component of the LPG SHALL convert the Baudot to RFC 4103 text characters
 10364 and send the text characters to the NIF component.

⁷⁴ Other characters not in the TTY character set

10365 With respect to incoming RFC 4103 text characters received from the NIF component, the
10366 PIF component SHALL apply the same mapping to the text characters as described above
10367 for an RTT message when interworking with Baudot tones sent to the legacy PSAP.

10368 The five (5) character-per-second EACC guideline SHOULD be followed in mapping the RFC
10369 4103 text characters associated with an MSRP message to TTY.

10370 **6.2.1.5 Handling of Video Media**

10371 A Legacy PSAP is unable to handle video, and the PIF will not return an SDP media line for
10372 any video offer. Only the audio media will pass through to the PSAP.

10373 **6.2.2 NG9-1-1-Specific Interwork Function (NIF)**

10374 The NIF component of the Legacy PSAP Gateway functional element is expected to provide
10375 special processing of the information received in incoming call setup signaling to facilitate
10376 call delivery to legacy PSAPs, to assist legacy PSAPs in obtaining the necessary callback and
10377 location information, and to support feature functionality currently available to legacy
10378 PSAPs, such as call transfer and requests for alternate routing.

10379 The NIF component of the Legacy PSAP Gateway MUST be capable of accepting SIP
10380 signaling associated with emergency call originations, as described in Section 3.1.
10381 Specifically, the NIF component of the Legacy PSAP Gateway MUST be capable of receiving
10382 and processing an INVITE that includes the following information:

- 10383 • Request-URI = urn:service:sos
- 10384 • Max Forwards <70
- 10385 • Record Route = ESRP URI (this URI should contain the "lr" parameter to avoid
10386 Request-URI rewriting)
- 10387 • Route header field = PSAP URI (this URI should contain the "lr" parameter to avoid
10388 Request-URI rewriting) resolving at the gateway⁷⁵
- 10389 • From = Callback Number/Address or "Anonymous," if unavailable
- 10390 • To: (e.g., sip:911@vsp.com)
- 10391 • P-A-I = the callback number/address or omitted if call is from a non-initialized
10392 mobile caller (i.e., P-Preferred-Identity containing 911 + "last 7 digits of the ESN or
10393 IMEI expressed as a decimal" is present)

⁷⁵ A Legacy PSAP Gateway could support more than one legacy PSAP. Each legacy PSAP would have a separate URI, but they would all resolve to the gateway. As an example, the PSAP URI for PSAP "A" might be "psapA@gateway1.esinet.net;lr" and the PSAP URI for PSAP "B" might be "psapB@gateway1.esinet.net;lr". The domain of the gateway in this example would be "gateway1.esinet.net".

- 10394 • P-Preferred-Identity = 911 + “last 7 digits of the ESN or IMEI expressed as a
10395 decimal” (if present for emergency calls originated by non-initialized mobile callers)
- 10396 • Via = ESRP URI (added to other Via header fields present in the INVITE message
10397 received by the terminating ESRP)
- 10398 • Contact = one of the following, depending on the transfer model implemented, and
10399 includes either a “text” media feature tag or a “urn:emergency:media-feature.tty-
10400 interworking” media feature tag
 - 10401 ◦ a SIP URI or tel URI identifying the user to facilitate an immediate callback to
10402 the device that placed the emergency call, or a SIP URI associated with a
10403 Legacy Network Gateway, if the RFC 4579-based [39] transfer model
10404 described in Section 4.7.1.1 is implemented
 - 10405 ◦ a SIP URI associated with a B2BUA, if the transfer model described in Section
10406 4.7.1.2 is implemented
 - 10407 ◦ a SIP URI that is associated with the Conference Aware UA, if the transfer
10408 model described in Section 4.8.3 is implemented
- 10409 • Supported = as received by the terminating ESRP
- 10410 • SDP = as received by the terminating ESRP
- 10411 • Geolocation = Content Identifier URI or location reference URI
- 10412 • A Geolocation-Routing header field set to “yes”
- 10413 • Call-Info = a URI which, when de-referenced, would yield additional information
10414 about the call or a cid: URI that points to additional information populated in the
10415 message body
- 10416 • History-Info = as specified in RFC 7044 [35], with a Reason Parameter (as received
10417 in the incoming INVITE from the ESRPs)

10418 Upon receiving an INVITE message from an ESRP, the NIF component SHALL analyze the
10419 signaled information and apply NG9-1-1-specific processing to ensure that the information
10420 delivered to the PSAP is in an acceptable format.

10421 **6.2.2.1 Handling of Emergency Calls with Non-NANP Callback Information**

10422 Traditional MF and E-MF interfaces to legacy PSAPs assume that callback information
10423 signaled to a PSAP will be in the form of a 7/10 digit NANP number. There are specific non-
10424 NANP number strings defined for use in scenarios in which the callback number is either
10425 missing or garbled. It is possible that VoIP or legacy wireless emergency call originations
10426 will contain callback information that is not in the form of (or easily converted to) a 10 digit
10427 NANP number. To address this situation, the NIF component of the Legacy PSAP Gateway
10428 SHALL perform a mapping from the non-NANP callback information to a locally significant
10429 digit string that can be delivered to the legacy PSAP via traditional MF or E-MF signaling. As
10430 described in Sections 6.2.1.1 and 6.2.1.2, the locally significant digit string delivered to the
10431 PSAP SHALL be of the form “NPD/NPA-511-XXXX”. If a pANI of the form

[MM/DD/YYYY]

Page 372 of 675



10432 NPD/NPA-511-XXXX is sent in the MF sequence corresponding to the callback number, the
10433 same digit string can be generated by the Legacy PSAP Gateway and delivered to the
10434 legacy PSAP as a pANI that represents location information received by the Legacy PSAP
10435 Gateway in incoming signaling.
10436 Note that legacy PSAPs will not be able to initiate a callback if the callback information
10437 associated with the emergency call is not in the form of an NANP number.

10438 **6.2.2.2 Special Handling Indication**

10439 Whether a legacy PSAP supports a traditional MF interface or an E-MF interface, it is
10440 possible for the information that appears at the PSAP CPE display to "flash" if the call has
10441 first been default-routed or alternate-routed. Today, in a legacy E9-1-1 environment, the
10442 decision about whether or not to flash the display at the PSAP depends upon local
10443 administration of Emergency Services Number (ESN) information.

10444 In a legacy E9-1-1 environment, default routing occurs when the initial selective routing
10445 process at the first SR fails, due to a valid ESN not being produced, or no valid Calling
10446 Station Information being available on a wireline call, or no valid cell site and sector
10447 information being available on a wireless call. Under these circumstances, the call is sent to
10448 the default ESN associated with the incoming trunk group for that call.

10449 Alternate routing occurs when the interface to a selected PSAP is found to be busy for any
10450 of these conditions: traffic busy (all trunks in use), night transfer (make-busy key
10451 operated), or upon detection of a failure condition (all trunks out of service). The alternate
10452 PSAP (or other destination) to which the call is routed may be on the same SR as the first
10453 PSAP or it may be served by a different SR.

10454 In a legacy environment, whether flashing will occur depends upon the particular ESN used
10455 to point the call to the PSAP. Each SR has a list of ESNs that indicate that flashing should
10456 occur when calls are directed to the associated PSAP. ESN definitions are under local
10457 control. An incoming call could be mapped to a flashing ESN at one SR, and the same call
10458 could be mapped to a non-flashing ESN at the second SR.

10459 An SR indicates to the PSAP CPE that a flashing display should be provided by the NPD
10460 value or the "II" value signaled to the legacy PSAP in the MF signaling sequence. For PSAPs
10461 that support traditional MF interfaces, an NPD digit with a value of 0-3 represents a steady
10462 ANI display. An NPD digit with a value of 4-7 represents a flashing ANI display (An NPD
10463 value of "8" is used for test calls). For PSAPs that support an E-MF interface, an II value of
10464 "40" indicates a steady display, and a value of "44" represents a flashing display. (An II
10465 value of "48" is used for test calls.)

10466 One other scenario in which the II digits are used to communicate "special handling" is
10467 when a PSAP supports the delivery of a single 10-digit number over an E-MF interface and

[MM/DD/YYYY]

Page 373 of 675



10468 expects the Calling Station Number to be delivered, but a 10-digit location reference is
10469 signaled instead because the Calling Station Number is not available.

10470 In the current i3 architecture, the ESRP interacts with a PRF to identify alternate routing
10471 addresses based on policy information associated with the next hop in the signaling path.
10472 The i3 Solution must support a means of signaling forward an indication that
10473 alternate/default routing has been applied to an emergency call so that the Legacy PSAP
10474 Gateway can determine when to include a Special Handling Indication in the MF signaling it
10475 sends to the legacy PSAP⁷⁶. The ESRP shall use the History-Info header field (RFC 7044
10476 [35]) and a Reason header field to communicate an indication of alternate/default routing.
10477 The NIF component of the Legacy PSAP Gateway will determine the appropriate coding of
10478 the NPD or II based on the content of received History-Info and Reason header fields and
10479 provisioning associated with the destination PSAP.

10480 **6.2.2.3 Internal Interface to the PIF Component**

10481 The NIF component SHALL generate an INVITE message to be sent to the PIF component.
10482 This message SHALL contain information from the incoming INVITE message associated
10483 with the emergency call, as well as any pANIs mapped by the NIF component. The NIF
10484 MUST determine, based on provisioning, whether the interface to the target PSAP is a
10485 traditional or Enhanced MF interface so that it can populate the callback and location
10486 information correctly in the INVITE that it sends to the PIF component. The NIF SHALL
10487 obtain callback information from the incoming INVITE message in the following way. If the
10488 incoming INVITE message contains a P-A-I header field, it will use the information in this
10489 header field as callback information. If the incoming INVITE message does not contain a
10490 P-A-I header field, the NIF will look in the From header field. If the From header field
10491 contains a value other than "Anonymous", the NIF will use the content of the From header
10492 field as the callback information. If the From header field contains the value "Anonymous"
10493 and a P-Preferred-Identity header field is present in the message, the NIF will use the
10494 content of the P-Preferred-Identity as the callback information. The NIF will obtain location
10495 information from the Geolocation header field of the incoming INVITE message.

10496 If the PSAP supports a traditional MF interface, then the NIF SHALL determine, based on
10497 provisioning associated with the destination PSAP, whether to populate the From header
10498 field of the INVITE message that it sends to the PIF with an NPD + 7-digit number that is

76 It is not currently assumed that a Legacy PSAP Gateway will have the intelligence to autonomously determine (e.g., via provisioning) an alternate PSAP based on detection of a busy or failure condition on the trunk to the primary PSAP.

- 10499 associated with callback information or with an NPD + 7-digit number that is associated
10500 with the location information.
- 10501 If the PSAP expects callback information to be delivered, but the callback information is
10502 unavailable or is of the form 911+ "last 7 digits of the ESN or IMEI expressed as a
10503 decimal", and location information is available, the NIF SHOULD signal the location
10504 information in the From header field. If the PSAP expects location information to be
10505 delivered and location information is not available, or if neither callback information nor
10506 location information is available, the digits "0-9-1-1-0000" SHALL be signaled in the From
10507 header field.
- 10508 A legacy PSAP that supports an E-MF interface may be capable of receiving one or two MF
10509 signaling sequences. If a PSAP supports the delivery of only one 10-digit number, the NIF
10510 SHALL determine, based on per-PSAP provisioning, whether callback information or
10511 location information should be populated in the From header field of the INVITE message it
10512 sends to the PIF. If the expected 10-digit number (e.g., Calling Station Number) is
10513 unavailable, but the second number (e.g., corresponding to the caller's location) is
10514 available, the available 10-digit number SHOULD be signaled in the From header field. If
10515 neither 10-digit number is available, and only one 10-digit number is expected to be
10516 signaled over the E-MF interface, the digits "000-911-0000" SHALL be signaled in the From
10517 header field.
- 10518 If the legacy PSAP supports an E-MF interface and is capable of receiving two MF signaling
10519 sequences, the NIF SHALL populate a 10-digit number that represents location in the From
10520 header field and a 10-digit number that represents callback information in the P-A-I header
10521 field of the INVITE it sends to the PIF.
- 10522 If the legacy PSAP supports an Enhanced MF interface in which two 10-digit sequences are
10523 expected, and either the Calling Station Number or the location reference is unavailable,
10524 the NIF SHOULD substitute the digits "000-911-0000" for the missing information in the
10525 P-A-I or From header field. If neither 10-digit number is available, and two 10-digit
10526 numbers are expected to be signaled over E-MF interface, the NIF SHALL substitute the
10527 digits "000-911-0000" for both the Calling Station Number and the location reference.
- 10528 **6.2.2.3.1 INVITE Message Sent from NIF Component to PIF Component**
- 10529 The INVITE message sent by the NIF component to the PIF component SHALL contain the
10530 following information:
- 10531 • Request-URI = PSAP URI resolving at the gateway expressed as a tel URI or a sip
10532 URI of the form "sip:<TN>@psap1.gateway.com;user=phone", along with the trunk
10533 group parameters that identify the outgoing trunk group to the destination PSAP, as
10534 defined in RFC 4904.

[MM/DD/YYYY]

Page 375 of 675



- 10535 • Max Forwards <70
- 10536 • Record-Route = ESRP URI, if presenting the SIP INVITE received from the ESRP
- 10537 • From = See Table 6-9
- 10538 • To = sip:911@vsp.com
- 10539 • P-A-I = See Table 6-9
- 10540 • Via = an identifier for the Legacy PSAP Gateway
- 10541 • Contact = as received by the NIF component
- 10542 • Supported = as received by the NIF component
- 10543 • SDP = as received by the NIF component
- 10544 • History-Info = as received (if present in the INVITE message received by the NIF component)
- 10545 • Reason = as received (if present in the INVITE message received by the NIF component)
- 10546
- 10547

Table 6-9 Population of From and P-A-I Header fields in INVITE Message Sent to PIF

PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Traditional MF	Callback information expected and available	NPD-NXX-XXXX or NPD-511-XXXX (associated with callback information)	Not present
Traditional MF	Location information expected and available	NPD-511-XXXX (associated with location information)	Not present
Traditional MF	Callback information desired; only location information available or non-initialized mobile caller	NPD-511-XXXX (associated with location information)	Not present
Traditional MF	Location information desired; only callback information available	0-911-0000	Not present
Traditional MF	Neither callback nor location available	0-911-0000	Not present

[MM/DD/YYYY]

Page 376 of 675



PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Enhanced MF	Interface supports delivery of 20 digits; callback and location information are available	NPA-511-XXXX (associated with location information)	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter
Enhanced MF	Interface supports delivery of 20 digits; callback is available, location is not available	000-911-0000	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter
Enhanced MF	Interface supports delivery of 20 digits; location is available, callback is not available	NPA-511-XXXX (associated with location information)	000-911-0000
Enhanced MF	Interface supports delivery of 20 digits; non-initialized mobile caller, location available	NPA-511-XXXX (associated with location information)	911 + "last 7 digits of the ESN or IMEI expressed as a decimal" oli parameter
Enhanced MF	Interface supports delivery of 20 digits; neither location nor callback is available	000-911-0000	000-911-0000
Enhanced MF	Interface supports delivery of 10 digits; Callback information expected and available	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Location information expected and available	NPD-511-XXXX (associated with location information) oli parameter	Not present

[MM/DD/YYYY]

Page 377 of 675



PSAP Interface Supported	Scenario	From Header field Content	P-A-I Header field Content
Enhanced MF	Interface supports delivery of 10 digits; Callback information desired; only location information available	NPD-511-XXXX (associated with location information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Location information desired; only callback information available	NPA-NXX-XXXX or NPA-511-XXXX (associated with callback information) oli parameter	Not present
Enhanced MF	Interface supports delivery of 10 digits; Neither callback nor location available	000-911-0000	Not present
Enhanced MF	Interface supports delivery of 10 digits; Callback information desired; call is from a non-initialized mobile	911 + "last 7 digits of the ESN or IMEI expressed as a decimal" oli parameter	Not present

10550 **6.2.2.4 SIP Re-INVITE Sent to the ESInet to Support “Silent” Emergency Calls**

10551 Upon receiving a SIP re-INVITE from the PIF component, the NIF component of the Legacy
 10552 PSAP Gateway will generate a SIP re-INVITE message and send it toward the caller or
 10553 Legacy Network Gateway or ingress LSRG via the ESInet. The SIP re-INVITE message will
 10554 include the following information:

- 10555 • A Request-URI that contains a URI from the Contact header field delivered to the
 10556 Legacy PSAP Gateway or ingress LSRG in the initial INVITE message. The URI may
 10557 be associated with the Legacy Network Gateway, the caller, a B2BUA, or a
 10558 Conference Aware UA, as appropriate for the origination type and the transfer model
 10559 implemented.
- 10560 • A To header field that contains the information delivered to the Legacy PSAP
 10561 Gateway in the From header field of the original INVITE message.
- 10562 • A From header field that contains the digits "911" expressed as a URI (received in
 10563 the To header field of the original INVITE message).

[MM/DD/YYYY]

Page 378 of 675



- 10564 • A Contact header field that contains a SIP URI associated with the Legacy PSAP
10565 Gateway along with a “urn:emergency:media-feature.tty-interworking” media
10566 feature tag.
10567 • A Via header field that is populated with a URI associated with the Legacy PSAP
10568 Gateway.
10569 • An SDP offer that includes a media format associated with real-time text, as
10570 described in RFC 4103 [85].

10571 Upon receiving a 200 OK message indicating that the SDP offer associated with real-time
10572 text has been accepted, the NIF component SHALL pass the 200 OK message to the PIF
10573 component. The PIF component shall respond by sending an ACK to the NIF component,
10574 and the NIF component SHALL send an ACK toward the caller/Legacy Network
10575 Gateway/ingress LSRG.

10576 **6.2.2.5 Handling of Media Association with SMS/MMS/IM and RTT**

10577 **6.2.2.5.1 Text Media Seccction Establishment**

10578 As described in Section 6.2.1.4, the NIF component of the Legacy PSAP Gateway SHALL
10579 cache an incoming MSRP message and convert it to RFC 4103 real-time text for delivery to
10580 the PIF component. The NIF component MUST also facilitate the “turn-taking” expected by
10581 the TTY users involved in a conversation between an emergency caller and a legacy PSAP.
10582 Also, unless specific action is taken by the LPG, session establishment associated with
10583 SMS/IMS/IM Text to 9-1-1 messages and RTT will appear to the legacy PSAP as “silent
10584 calls”. The Standard Operating Procedures associated with the processing of silent calls will
10585 result in a delay in processing the 9-1-1 call as compared to a voice 9-1-1 call. To reduce
10586 delays associated with processing silent calls, some TTY device manufacturers support a
10587 feature that causes space characters to be sent (subsequent to call establishment) as an
10588 indication that the call is from a TTY device. Some TTY users may also send space
10589 characters upon initiating a call, although this behavior cannot be relied upon. Based on
10590 the Standard Operating Procedures defined in NENA 56-004 [174], upon hearing beeping
10591 tones, the PSAP should immediately initiate a TTY/TDD call response. To improve the
10592 response time associated with SMS/MMS/IM and RTT originations, this standard
10593 recommends that the NIF component support functionality that emulates the behavior of
10594 TTY devices that generate space characters to more quickly engage TTY equipment at the
10595 legacy PSAP.

10596 When the NIF component receives a 200 OK message from the PIF component in response
10597 to a request from the ESInet to establish an RFC 4103 text media session associated with
10598 an SMS/MMS/IM or RTT origination, it SHALL send a sequence of four (4) space characters
10599 in RFC 4103 text with 350 milliseconds of silence between each space character to the PIF

10600 component, with five (5) seconds between each sequence, until it receives an RFC 4103
10601 text response from the PIF component.
10602 If the NIF component does not receive a response from the PIF component (containing the
10603 interworked Baudot tones from the PSAP) within ten (10) seconds, the NIF component
10604 MUST send a preprogrammed message back to the caller that says something like
10605 "connecting to 9-1-1, please stand by". This may be repeated twice. If, after 30 seconds,
10606 no Baudot tones are received from the PSAP, the NIF component MUST send a
10607 preprogrammed message back to the caller stating, for example, that text service is not
10608 available at this time and suggesting that the user make a voice call to 9-1-1 for
10609 assistance.

10610 **6.2.2.5.2 Text Exchanges between Legacy PSAP and RTT or TTY Caller**

10611 Based on NENA 56-004, the TTY equipment at the PSAP will respond to receipt of the
10612 space character(s) by sending a preprogrammed message or an approved greeting such as
10613 "911 GA" typed by the PSAP. If the call originated as an RTT call (i.e., the media feature
10614 tag conveyed in incoming signaling associated with the emergency call has a value of "text"
10615 and no MSRP session is established with the NIF component), then upon receiving the "911
10616 GA" in RFC 4103 text characters from the PIF component, the NIF component SHALL
10617 replace the "GA" with a line delimiter (e.g., CRLF)⁷⁷ and pass the "911" and line delimiter in
10618 RFC 4103 characters back toward the caller. If the call originated as a TTY call (i.e., the
10619 media feature tag conveyed in incoming signaling associated with the emergency call has a
10620 value of "urn:emergency:media-feature.tty-interworking"), the NIF component SHALL pass
10621 the "911 GA" received in RFC 4103 text characters from the PIF component, unchanged,
10622 back toward the caller. At this point, the text media session is established with a TTY or
10623 RTT calling user, and it is the caller's turn.

10624 The NIF component SHALL then start an idle timer for a period of four (4) seconds as it
10625 waits for the initial text message from the caller (via the ESInet). If there is already text
10626 buffered from the caller, the NIF component SHALL send the RFC 4103 characters to the
10627 PIF component. If the NIF component receives RFC 4103 characters from the caller before
10628 the expiration of the idle timer, the NIF component SHALL convey those characters to the
10629 PIF component, initiating an inter-character timer of 4 seconds. This timer SHALL be
10630 restarted with the value 4 seconds every time a character is transmitted towards the PSAP.
10631 If the time between characters exceeds 4 seconds, the NIF component SHALL send the
10632 characters "_GA" (where the underscore indicates a space character) to the PSAP, as

⁷⁷ Insertion of a line delimiter will allow text to be presented to the SMS/MMS/IM or RTT user in a form that is more readable and expected.

10633 defined in the EAAC Report [175]. The NIF component SHALL then enter idle mode as it
10634 waits for subsequent text from the PSAP (via the PIF component) or the caller (via the
10635 ESInet). During this time the NIF component shall buffer any text received from the caller.
10636 If the NIF component detects a “_GA” from the PSAP before the expiration of the 4-second
10637 inter-character timer, the NIF component SHALL reset the inter-character timer to 1500
10638 ms. If the NIF component receives a space, a line delimiter, or no further text before the
10639 1500 ms timer expires, the NIF component SHALL send any buffered text characters from
10640 the caller (unchanged) to the PIF component and SHALL continue conveying text in real
10641 time from the caller. The NIF component SHALL then enter idle mode. If additional text
10642 (other than a space or line delimiter) is received from the PSAP before the 1500 ms
10643 expires, the “GA” was part of the text conversation and the the NIF component SHALL
10644 reset the 4 second timer and continue waiting for a “_GA” or line delimiter.

10645 If the NIF component detects a line delimiter from the caller before the expiration of the 4
10646 second inter-character timer, the NIF component SHALL replace the line delimiter with a
10647 space and SHALL reset the inter-character timer to 1500 ms. If the 1500 ms inter-character
10648 timer expires without any characters other than “_GA”, or space or a line delimiter being
10649 detected, the NIF component SHALL append the characters “_GA” to the incoming RFC
10650 4103 text and send the text characters with the “_GA” appended to the PIF component for
10651 conversion to Baudot tones. The NIF component SHALL then enter idle mode with the
10652 PSAP having the turn and any incoming text from the caller being buffered. If other
10653 characters are received from the caller within the 1500 ms timer, the NIF SHALL convey
10654 the characters to the PIF component and SHALL reset the timer to 4 seconds.

10655 If the NIF component receives subsequent text characters from the PIF component before
10656 the expiration of the idle timer and prior to any additional text messages being received
10657 from the ESInet, it SHALL examine the text for the presence of the characters “_GA”. Note
10658 that it is common for a PSAP using TTY to end a question with “Q GA”. Upon detecting a “
10659 GA”, the NIF SHALL set the inter-character timer to 1500 ms. If a space, line delimiter or
10660 no other characters are received within the 1500 ms time period, and the caller is a TTY
10661 caller, the characters “_GA” or “Q_GA” will be passed unchanged toward the TTY caller.
10662 The turn is then changed to be the caller’s turn. If the NIF component receives a “_GA”
10663 followed by nothing other than a space or line delimiter before the 1500 ms timer expires,
10664 and the caller is an RTT caller, the NIF SHALL substitute a line delimiter for the “_GA” in
10665 the RFC 4103 text sent toward the RTT caller. In generating RFC 4103 text corresponding
10666 to the characters “Q GA” toward an RTT caller, the NIF component SHALL replace the “Q”
10667 with a “?” and SHALL replace the “GA” with a line delimiter. If other characters are
10668 received before the expiration of the 1500 ms timer, the NIF should view the “_GA” or “Q
10669 GA” as part of the contents of the conversation and SHALL pass the characters unchanged
10670 toward the caller. The NIF SHALL then continue to convey characters from the PSAP to the
10671 caller.

10672 If the NIF component detects that the call taker is sending text (i.e., it has not yet received
10673 the "_GA" from the PSAP via the PIF component), it MUST buffer any incoming text
10674 packets received from the ESInet until either the "_GA" has been received from the PSAP,
10675 or an appropriate period of time has passed without any further text being received from
10676 the PSAP. The EAAC Report [175] proposes a value of seven (7) seconds for this timer.
10677 Note that, as described above, when the NIF component buffers incoming text packets
10678 from the ESInet, it SHALL initiate a provisionable inter-character timer with a default value
10679 of 4 seconds and follow the procedures described above. The NIF component MUST NOT
10680 send additional characters to the PIF component until it either detects a "_GA" from the
10681 PSAP or the PSAP idle timer has expired (whichever occurs first).

10682 If the NIF component receives a "_GASK" or "_SKSK" indication from the PSAP, the NIF
10683 SHALL set the inter-character timer to 1500 ms. If a space, line delimiter or no other
10684 characters are received within the 1500 ms time period, and the caller is a TTY caller the
10685 NIF component SHALL pass these characters unchanged toward the caller. If a space, line
10686 delimiter or no other characters are received within the 1500 ms time period, and the caller
10687 is a RTT caller, the NIF component SHALL send a line delimiter toward the caller, providing
10688 handling that is consistent with what would be seen by a caller communicating with an
10689 NG9-1-1 PSAP using RTT. If other characters are received from the PSAP within the 1500
10690 ms timer, the characters SHALL be conveyed unchanged to the caller, the NIF component
10691 SHALL reset the timer to 7 seconds and the turn will stay with the PSAP.

10692 **6.2.2.5.3 Conveyance of SMS/IMS/IM Messages to Legacy PSAPs**

10693 As described in Section 6.2.2.5.1, in support of incoming SMS/MMS/IM text to 9-1-1
10694 messages, once an MSRP session is established with the NIF, the NIF component SHALL
10695 send a sequence of four (4) space characters in RFC 4103 text with 350 milliseconds of
10696 silence between each space character to the PIF component with five (5) seconds between
10697 each sequence until it receives an RFC 4103 text response from the PIF component. The
10698 NIF component SHALL also cache the incoming SMS/MMS/IM text to 9-1-1 message
10699 received via MSRP.

10700 Upon determining that the call taker has joined the conversation (via receipt of an
10701 appropriate preprogrammed or typed message such as "911 GA" from the PIF component),
10702 the NIF component SHALL convert the MSRP message to RFC 4103 characters. The RFC
10703 4103 text characters sent by the NIF component to the PIF component SHALL begin with
10704 the characters "Message" followed by the characters from the cached SMS/MMS/IM text
10705 message and the characters "_GA". The NIF component SHALL enter idle mode on its
10706 egress side and wait for the PIF/call taker to respond. The NIF component SHALL apply the
10707 same 4-second "idle timer" to MSRP conversation as it uses for RTT conversation. The NIF
10708 remains in active mode on its ingress side. When the NIF component receives RFC 4103

10709 text characters from the PIF component it SHOULD expect “_GA” or “_SKGA”, possibly
10710 followed by a space or line delimiter (received within 1500 ms) at the end of the text of the
10711 message. If this is the case, the NIF component SHOULD replace the “_GA” or “_SKGA”
10712 with a line delimiter, and if there is a “Q” immediately preceding the “_GA”/“_SKGA”, it
10713 should substitute a “?” for that character. If another character is received within the 1500
10714 ms timer, the characters SHALL be conveyed unchanged toward the caller. The NIF
10715 component SHALL implement the same 7-second PSAP idle timer as described above for
10716 instances in which it does not receive “_GA” or “_SKGA”. The NIF component SHALL also
10717 apply the same processing as described for RTT upon receipt of an “SKSK” or “GASK” from
10718 the PSAP.

10719 If the NIF component detects that the caller has sent a subsequent SMS/MMS/IM message
10720 (based on receipt of an MSRP message from the ESInet), the NIF component MUST buffer
10721 the incoming MSRP message until it either receives the RFC 4103 characters “_GA” from
10722 the PIF component, or the 7-second PSAP idle timer has expired. The NIF component
10723 MUST insert the characters “_GA” at the end of the RFC 4103 text characters (converted
10724 from the MSRP message) passed to the PIF component and start buffering any subsequent
10725 incoming MSRP messages.

10726 **6.2.2.6 Support for Emergency Call Transfer**

10727 When a legacy PSAP determines that it is necessary to transfer an emergency call, it sends
10728 a “flash” signal and waits for dial tone. Once the dial tone is received, the PSAP requests
10729 the transfer either by operating a key associated with a particular type of secondary PSAP
10730 (e.g., fire department) or a particular PSAP or other transfer-to destination (e.g., using a
10731 speed calling feature), or by manually dialing the number of the desired transfer-to
10732 destination.

10733 When the PIF component of the Legacy PSAP Gateway detects a flash, it will follow the
10734 procedures defined in RFC 4733 using code 16 for passing the “flash” signal to the NIF
10735 component of the Legacy PSAP Gateway. The PIF component will also provide dial tone to
10736 the legacy PSAP. The NIF component will interpret receipt of the flash as a request from a
10737 legacy PSAP to initiate a call transfer. In response to the dial tone, the PSAP will provide
10738 DTMF signaling in the form of a “*XX code”, “# + 4 digits”, or a 7/10-digit directory
10739 number. Upon receiving the “*XX” code, “# + 4 digits”, or the 7/10-digit directory number
10740 of the destination party, the PIF component of the Legacy PSAP Gateway will pass the
10741 information to the NIF component using the mechanisms defined in RFC 4733. The NIF will
10742 interpret the DTMF information received from the PIF and request that a conference be
10743 created, if one has not already been created (i.e., as would be the case for networks that
10744 have implemented the Route Call Calls Via a Conference Aware UA transfer model). The
10745 NIF will then generate a SIP REFER method to request that the caller (or B2BUA,

10746 depending on the architecture being used by the ESInet to support call transfer) be invited
10747 to the conference. (Note that a REFER inviting the caller/B2BUA to the conference will only
10748 be sent by the NIF if a transfer model other than the Route All Calls Via a Conference
10749 Aware UA transfer model has been implemented.) The NIF component of the Legacy PSAP
10750 Gateway will subsequently generate another SIP REFER method to request that the
10751 conference bridge invite the transfer-to party to the conference. This latter REFER method
10752 will include an indication of the transfer-to party in the Refer-To header field. The NIF will
10753 determine the transfer-to party in one of the following ways:

- 10754 • If the PIF receives a 7/10-digit destination number in the transfer request signaling
10755 from the legacy PSAP and passes this information to the NIF using the mechanisms
10756 defined in RFC 4733, the NIF SHALL use this information to populate the URI in the
10757 Refer-To header field of the outgoing REFER method.
- 10758 • If the PIF receives a "# + 4-digits" in the transfer request signaling from the legacy
10759 PSAP and passes this information to the NIF using the mechanisms defined in RFC
10760 4733, the NIF SHALL add the appropriate NPA-NXX digits at the beginning of the
10761 4-digit string and use this information to populate the URI in the Refer-To header
10762 field of the outgoing REFER method.
- 10763 • If the PIF receives a code of the form "*XX" in the transfer request signaling from
10764 the legacy PSAP and passes this information to the NIF using the mechanisms
10765 defined in RFC 4733, the NIF SHALL do one of the following, based on trunk group
10766 provisioning:
 - 10767 ○ The NIF SHALL map the received "*XX" code to a static URI, and populate
10768 this URI in the Refer-To header field of the outgoing REFER method
 - 10769 ○ The NIF SHALL map the received "*XX" code to a service URN and query an
10770 ECRF using this service URN and the location information received with the
10771 call.⁷⁸ The NIF will then use the URI returned in the response from the ECRF
10772 to populate the Refer-To header field of the outgoing REFER method.⁷⁹

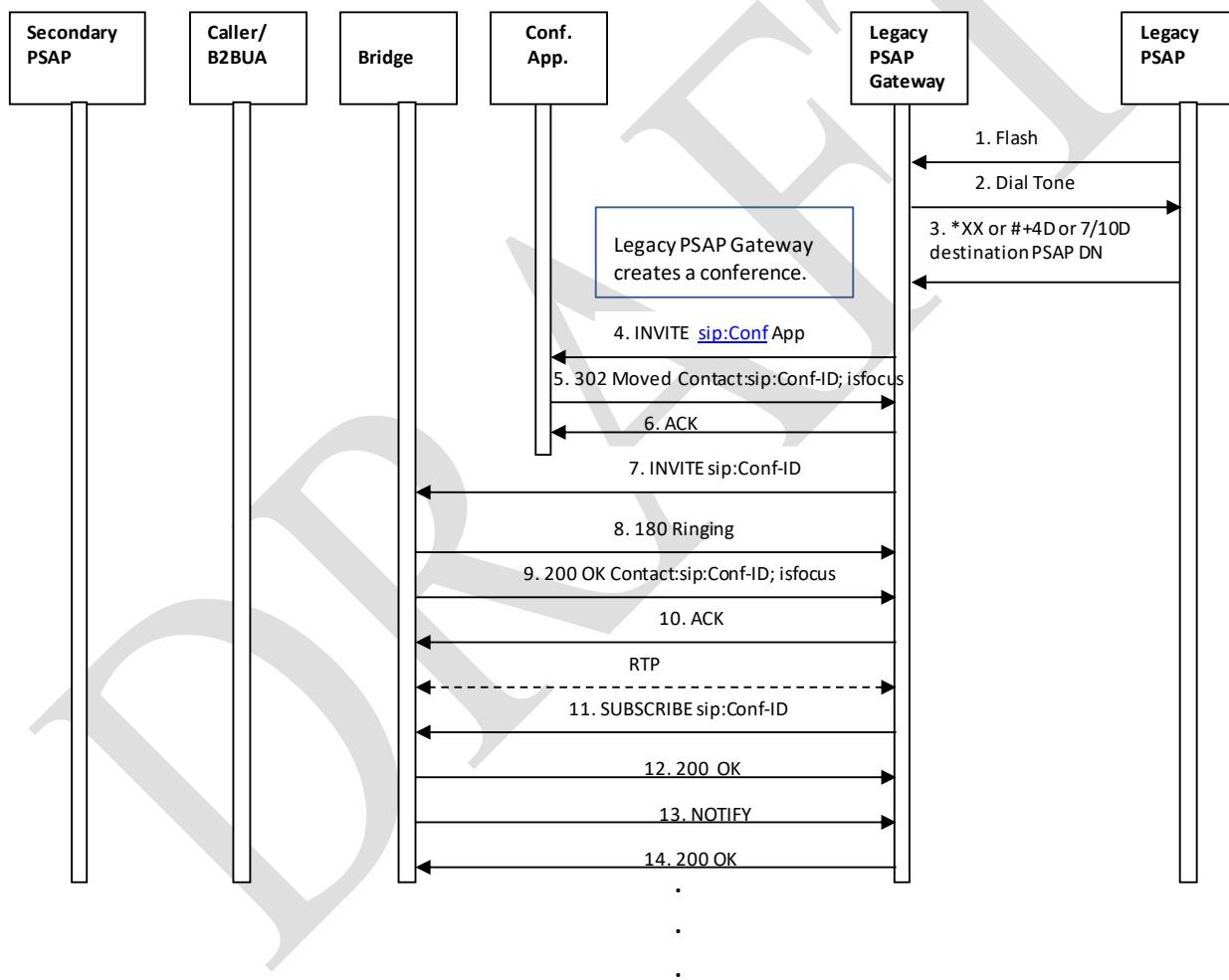
10773 Figure 6-4 and Figure 6-5 provide an example of an emergency call transfer flow to
10774 illustrate different aspects of an emergency call transfer that has been requested by a
10775 legacy PSAP. Figure 6-4 shows the establishment of a conference by the Legacy PSAP
10776 Gateway in response to a transfer request from a legacy PSAP. Note that the flow

78 Note that if the location information received with the call is a location-by-reference, the Legacy PSAP Gateway will have to first send a dereference request to a LIS or Legacy Network Gateway, using an appropriate dereferencing protocol, to obtain a routing location value for the call.

79 This will require that the Legacy PSAP Gateway be able to map all of the *XX codes supported by each PSAP that it serves to an appropriate service URN value that it can use to obtain the associated transfer-to destination address from the ECRF.

10777 illustrated in Figure 6-4 does not apply if the Route All Calls Via a Conference Aware UA/
10778 transfer model has been implemented. Figure 6-5 shows the completion of the transfer of
10779 the emergency call to the transfer-to PSAP. Section 3.1.1.2 provides a more complete
10780 discussion of the REFER method, and Section 4.7 provides detailed flows describing the
10781 alternatives for supporting bridging and transfer in an i3 environment.

10782 **Note:** RFC 2833 defined the use of code 16 for flash. RFC 4733 obsoleted RFC 2833 but
10783 did not define a code for flash, although it did reserve code 16. Efforts will be made to
10784 restore the definition of Flash to the code registry using 16. Until such time, code 16 MUST
10785 be used as per RFC 2833.



10786
10787 **Figure 6-4 Emergency Call Transfer Request from Legacy PSAP – Conference**
10788 **Established**

10789 The emergency call transfer flow illustrated above begins when the legacy PSAP
10790 determines that an emergency call needs to be transferred.

10791 1. Upon determining that an emergency call needs to be transferred, the legacy PSAP
10792 initiates a transfer request by sending a flash signal to the Legacy PSAP Gateway.
10793 2. When the Legacy PSAP Gateway receives the flash signal, it returns dial tone to the
10794 legacy PSAP and prepares to receive DTMF signaling.
10795 3. The legacy PSAP provides a “*XX code”, a string consisting of “# + 4-digits”, or the
10796 7/10-digit directory number associated with the transfer-to PSAP/public safety
10797 agency.
10798 4. The Legacy PSAP Gateway creates a conference by first sending an INVITE to a
10799 conference application, using a URI that is known or provisioned at the Legacy PSAP
10800 Gateway.
10801 5. The Conference Application responds by sending a 302 Moved message that
10802 redirects the Legacy PSAP Gateway to the conference bridge and provides the
10803 Conference-ID that should be used for the conference.
10804 6. The Legacy PSAP Gateway acknowledges the receipt of the 302 Moved message.
10805 7. The Legacy PSAP Gateway generates an INVITE to establish a session with the
10806 conference bridge.
10807 8. The conference bridge responds to the INVITE by returning a 180 Ringing message.
10808 9. The conference bridge then returns a 200 OK message, and a media session is
10809 established between the Legacy PSAP Gateway and the conference bridge.
10810 10. The Legacy PSAP Gateway returns an ACK message in response to the 200 OK.
10811 11. through 14. Once the media session is established, the Legacy PSAP Gateway
10812 subscribes to the conference URI obtained from the Contact URI provided in the 200
10813 OK message from the conference bridge.

10814 After the Legacy PSAP Gateway establishes the conference, it sends a REFER method to
10815 the conference bridge asking it to invite the caller/B2BUA to the conference, following the
10816 procedures described in Sections 4.7.1.1 and 4.7.1.2. (Note that a REFER requesting that
10817 the bridge invite the caller/B2BUA to the conference will not be sent if the Route all Calls
10818 Via a Conference Aware UA transfer model is implemented.) Once the conference bridge
10819 has done so, the Legacy PSAP Gateway asks the conference bridge to invite the transfer-to
10820 party to the conference. It does this by generating a REFER method with a Refer-To
10821 header field that contains the URI of the transfer-to PSAP/agency, determined using one of
10822 the methods described above. The REFER SHOULD include any location information
10823 associated with the original caller that was received in the initial INVITE message in an
10824 escaped Emergency Incident Data Object (EIDO), as described below. The EIDO SHALL
10825 also include callback information. The Legacy PSAP Gateway will populate the remaining
10826 fields of the REFER based on RFC 3515.

- 10827 As described in Section 4.7, the Legacy PSAP Gateway SHALL be capable of receiving a 200
10828 OK message in response to the REFER, followed by a NOTIFY that contains the status of
10829 the REFER request. The Legacy PSAP Gateway then returns a 200 OK in response to the
10830 NOTIFY.
- 10831 When the call to the transfer-to PSAP is answered, the Legacy PSAP Gateway will receive a
10832 NOTIFY message indicating this event. The Legacy PSAP Gateway SHALL respond to the
10833 NOTIFY by returning a 200 OK message.
- 10834 The Legacy PSAP Gateway SHALL create an EIDO, as described in the EIDO JSON standard
10835 [111] that contains location information (by value or reference), as well as any Additional
10836 Data blocks received by the Legacy PSAP Gateway with the call. The EIDO SHALL also
10837 contain callback information. The Legacy PSAP Gateway SHALL pass this information to the
10838 transfer-to PSAP via the conference bridge. If the Additional Data was received by value, it
10839 SHALL be sent in the EIDO by value, and if it was received by reference, it SHALL be sent
10840 in the EIDO by reference. While the Legacy PSAP Gateway does not know all of the
10841 information the transfer-from PSAP developed in its handling of the call, it SHOULD pass
10842 what it does know to the transfer-to PSAP using this mechanism.
- 10843 When the transfer-from PSAP determines that it should drop off the conference and
10844 complete the transfer, it SHALL follow the steps illustrated below.

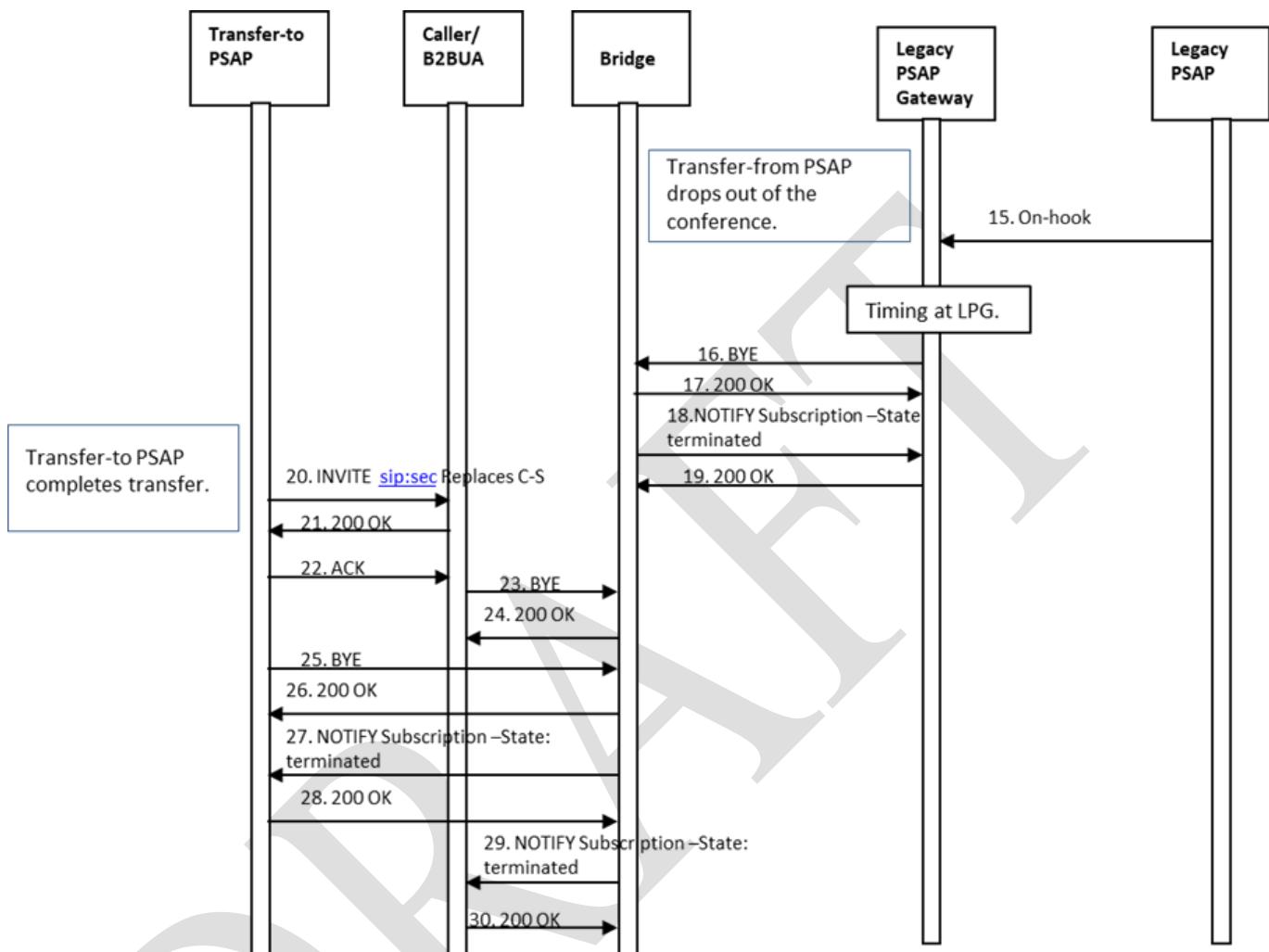


Figure 6-5 Emergency Call Transfer Request from Legacy PSAP – Transfer Completed

The emergency call transfer flow illustrated above begins when the legacy PSAP determines that it can drop off the conference with the caller and the transfer-to PSAP and complete the transfer.

Upon determining that the emergency call transfer should be completed, the legacy PSAP disconnects from the call by sending an on-hook signal to the Legacy PSAP Gateway.

The Legacy PSAP Gateway sets a timer for 1.1 seconds to distinguish a disconnect indication from a flash signal.

10857 16. When the Legacy PSAP Gateway determines that the PSAP has disconnected, it
10858 sends a BYE message to the conference bridge.
10859 17. The conference bridge responds by returning a 200 OK message.
10860 18. The conference bridge then returns a NOTIFY message indicating that the
10861 subscription to the conference has been terminated.
10862 19. The Legacy PSAP Gateway returns a 200 OK in response to the NOTIFY.
10863 20. If applicable, based on the transfer model used, the transfer-to PSAP completes the
10864 transfer by sending an INVITE to the caller/B2BUA requesting that they replace their
10865 connection to the bridge with a direct connection to the transfer-to PSAP.
10866 21. The caller/B2BUA responds by returning a 200 OK message.
10867 22. The transfer-to PSAP responds by returning an ACK to the caller/B2BUA.
10868 23. The caller/B2BUA then sends a BYE to the conference bridge to terminate the
10869 session.
10870 24. The conference bridge responds by sending the caller/B2BUA a 200 OK message.
10871 25. The transfer-to PSAP also terminates its session with the conference bridge by
10872 sending a BYE message.
10873 26. The conference bridge responds by sending a 200 OK message to the transfer-to
10874 PSAP.
10875 27. The conference bridge then returns a NOTIFY message to the transfer-to PSAP
10876 indicating that the subscription to the conference has been terminated.
10877 28. The transfer-to PSAP responds with a 200 OK message.
10878 29. The conference bridge sends a NOTIFY message to the caller/B2BUA indicating that
10879 the subscription to the conference has been terminated.
10880 30. The caller/B2BUA responds with a 200 OK message.

10881 The LPG MUST handle the case of a transfer between two legacy PSAPs that it serves.

6.2.2.7 Alternate Routing Invocation and Notification

10883 Alternate routing allows a network to temporarily re-route calls to a different PSAP when
10884 the primary PSAP is unavailable to answer the call, or when connectivity to the primary
10885 PSAP is not available due to network failure.

10886 In a legacy environment, when a PSAP determines that alternate routing needs to be
10887 manually invoked (e.g., the PSAP needs to evacuate), it calls the alternate PSAP to inform
10888 them of the situation, so they are prepared to begin to receive all of the primary PSAP's
10889 calls. Today, the capability to manually invoke/cancel alternate routing is controlled by the
10890 primary PSAP. Typically, when alternate routing is to be invoked, the primary PSAP
10891 manually activates a switch or other control item to change the state of a control circuit
10892 connected to a scan point or other sensing device at the SR. When the state of the circuit
10893 is changed (e.g., by "shorting out" the circuit or closing a relay on a Network Control

10894 Module [NCM]), the scan points get saturated and, from the perspective of the SR, it
10895 appears as an "all circuits busy" condition on the trunk group. This causes the SR to route
10896 calls intended for the primary PSAP to the alternate PSAP. To remove alternate routing, the
10897 primary PSAP restores the normal state of the control circuit (or re-opens the relay(s) at
10898 the NCM). In some cases, manual alternate routing is invoked when the primary PSAP
10899 places a call to their E9-1-1 System Service Provider to request that action. This is also
10900 something a Legacy PSAP Gateway MUST be able to replicate.

10901 In an i3 Solution environment, a Legacy PSAP Gateway MUST be capable of recognizing a
10902 request to activate alternate routing. This request may come in the form of a physical
10903 switch, or it may be made via a GUI or web server. Upon detecting the alternate routing
10904 request, the Legacy PSAP Gateway MUST generate a ServiceState change event
10905 notification back to the ESRP to inform it of the change in PSAP state. Note that, using this
10906 event notification mechanism, the ESRP will be able to distinguish between alternate
10907 routing that is due to traffic volumes (i.e., events related to queue state) and "make busy"
10908 scenarios, in which the PSAP is experiencing some type of failure or evacuation situation
10909 (i.e., events related to PSAP state). It is assumed that the policy rules associated with
10910 alternate routing requests related to a specific PSAP will have been previously populated in
10911 the PRF.

10912 **6.2.2.8 Test Calls**

10913 The NIF MUST support and act as the termination point for the test call interface although
10914 administrative provisioning processes SHOULD be available to disable it, especially under
10915 overload situations. The test interface includes the ability of the test caller to offer media
10916 and to receive a response and loop back a small number of packets of each media
10917 accepted at the PSAP. This provides a mechanism for a caller to determine that a call to a
10918 legacy PSAP behind a Legacy PSAP Gateway could not accept video. Legacy PSAP
10919 Gateways MUST refuse offers for video and accept offers for audio and text (which will be
10920 converted by the PIF component and conveyed using existing mechanisms, i.e., TTY). The
10921 LPG is responsible for the media loopback required by the test call mechanism. Test calls
10922 SHOULD NOT be passed through the LPG to the Legacy PSAP.

10923 **6.2.2.9 Handling of Advanced Automatic Crash Notification Calls**

10924 As described in Section 3.1.19, when an NG-AACN call is presented to the ESInet, the SIP
10925 INVITE message associated with that call will contain a VEDS telematics dataset and a
10926 metadata/control object indicating the capabilities of the vehicle/TSP. If the NIF component
10927 of the Legacy PSAP Gateway receives such a SIP INVITE message, it SHALL NOT attach a
10928 metadata/control object to its final response to the SIP INVITE message. This will convey
10929 to the vehicle or TSP that the call is not end-to-end NG-AACN and will cause the

10930 vehicle/TSP to fall back to legacy mechanisms for conveying crash and location data (e.g.,
10931 using text-to-speech, pre-recorded audio, or verbal interaction with the TSP assistant).

10932 **6.2.3 Location Interwork Function (LIF)**

10933 As described in Section 6.2, the Legacy PSAP Gateway MUST support an ALI interface that
10934 can accept an ALI query from the legacy PSAP and return location information based on
10935 the formats specified in NENA-STA-027 [164] and NENA 04-005 [165]. There is additional
10936 information beyond just callback number and location information that may be included in
10937 an ALI response. There are various ways that ALI data may be obtained by the Legacy
10938 PSAP Gateway so that it can be returned to the legacy PSAP in the expected format.

10939 If the Legacy PSAP Gateway receives callback information (i.e., in the form of a 10-digit
10940 NANP number) and location-by-value in the incoming INVITE message from the ESRP, the
10941 Legacy PSAP Gateway can use this information to populate the callback number and
10942 location fields of the ALI response. Note that the Legacy PSAP Gateway will have to
10943 interact with the MSAG Conversion Service (MCS) if the location information received in
10944 incoming signaling (or obtained via dereferencing) is in civic format. This is necessary to
10945 ensure that the location information populated in the ALI response message is in the
10946 correct format for the legacy PSAP to which it is being delivered. (See Section 4.4 for
10947 further details regarding the MCS.) If the interaction with the MCS is unsuccessful, the
10948 Legacy PSAP Gateway will provide an indication of "no record found" to the PSAP.

10949 If the legacy PSAP Gateway receives callback information in the incoming INVITE message
10950 from the ESRP that is not in the form of (or easily converted to) a 10-digit NANP number,
10951 the Legacy PSAP Gateway SHALL populate the pANI generated by the NIF component (as
10952 described in Section 6.2.2.1) as the callback number in the ALI response.

10953 If location-by-reference is received in the incoming INVITE message from the ESRP, the
10954 Legacy PSAP Gateway SHALL support the ability to query other elements (i.e., LISes,
10955 Legacy Network Gateways) using an appropriate dereferencing protocol, as specified in
10956 Section 3.2, to obtain caller location for the call. If the location value returned in the
10957 dereference response is a civic location, the Legacy PSAP Gateway will use the MCS and
10958 convert the caller location value to the appropriate format for population in the ALI
10959 response message.

10960 If the location-by-value received in a SIP INVITE message from an ESRP or in a
10961 dereference response contains a geodetic coordinate-based location that identifies a shape
10962 other than a point or circle with radius, the Legacy PSAP Gateway MUST convert that geo-
10963 coordinate location to a point with uncertainty, using an appropriate algorithm, before
10964 populating it in the ALI response message.

10965 The Legacy PSAP Gateway will use Additional Data structures to populate other fields in the
10966 ALI response. If the Additional Data has been delivered to the Legacy PSAP Gateway "by-
10967 reference", the Legacy PSAP Gateway SHALL support the HTTPS GET method described in
10968 IETF RFC 7230 [162] to obtain the Additional Data "by-value"⁸⁰. The Legacy PSAP Gateway
10969 SHALL use the information contained in the Call-Info header field of the received INVITE to
10970 either identify the address of the target ADR to which the GET will be directed, or the place
10971 in the message body where the Additional Data is provided "by-value". The Legacy PSAP
10972 Gateway SHALL be capable of processing the XML-formatted Additional Data structures in
10973 the message body or received in the dereference response and using it to populate the
10974 appropriate fields of the ALI response message. The Additional Data used to populate the
10975 ALI response comes from the data in the call signaling and not from the data in the
10976 PIDF-LO.

10977 See Appendix A for a detailed description of where the Legacy PSAP Gateway will obtain
10978 the necessary information to populate ALI response messages.

10979 **6.2.4 Timing at the Legacy PSAP Gateway**

10980 **6.2.4.1 Call Setup Timing**

10981 Call Setup timing SHALL be used by the PIF component of the Legacy PSAP Gateway to
10982 determine if the legacy PSAP CPE is correctly interfacing with the Legacy PSAP Gateway.
10983 Call Setup timing for Enhanced MF (E-MF) and Traditional MF (NPD + 7-digit ANI) is the
10984 same, so only one example of setup timing will be outlined. Precise details of Call Setup
10985 timing can be found in NENA 03-002 [163], ATIS-0900414.2012(R2017) [192], and/or
10986 Telcordia GR-350--CORE [189].

10987 Legacy 9-1-1 system policies dictate that a 9-1-1 call is terminated if it encounters two
10988 successive call setup failures. If the Legacy PSAP Gateway cannot deliver a call to a legacy
10989 PSAP trunk on the first attempt, it SHALL then attempt to deliver the call to another PSAP
10990 trunk, according to its standard hunting or routing algorithms. If the Legacy PSAP Gateway
10991 has a call setup failure on the second attempt, it SHALL terminate the call, and return an
10992 appropriate message (i.e., a SIP 500 Server Internal Error message) toward the originating
10993 network(s) to indicate such.

⁸⁰Legacy PSAPs do not differentiate between access networks and originating networks. Additional Data from the access network may be present in a PIDF-LO received by the LPG as well as Additional Data from the originating network received via a Call-Info header field. The LPG uses the originating network information in the Call-Info header field instead of any access network Additional Data in the PIDF-LO. Devices and Service providers other than the access and originating networks may provide Additional Data. The LPG does not send this data to the PSAP.

10994 The Legacy PSAP Gateway SHALL determine that a call setup has or will fail when the PIF
10995 component fails to receive a wink from the CPE in response to its off-hook condition
10996 (Seizure) toward the legacy PSAP within a specific period of time. Traditional values would
10997 suggest that the PSAP return a wink to the Legacy PSAP Gateway within a minimum of four
10998 (4) to twenty (20) seconds. Most 9-1-1 systems use the four-second interval as the
10999 minimum time period in order to reduce potential call delays on a first try failure. If the
11000 Legacy PSAP Gateway has not received a wink condition from the PSAP CPE within the
11001 minimum period (i.e., four seconds) after sending an off-hook indication, it SHALL mark the
11002 call as a failure, and proceed as described above (i.e., by sending a SIP 500 Server Internal
11003 Error message toward the originating network).

11004 **6.2.4.2 Call Disconnect Timing**

11005 Call disconnect timing depends on whether the caller⁸¹ or the PSAP disconnects first. It
11006 determines how soon the Legacy PSAP Gateway may offer a new call to the legacy PSAP
11007 on the same circuit. The Legacy PSAP Gateway MUST ensure that there is sufficient timing
11008 between the disconnection of one call and the presentation of a new call to the legacy
11009 PSAP so that the legacy PSAP CPE can reset and be ready in time for the next call.

11010 **6.2.4.2.1 Call Disconnect Timing When PSAP Disconnects First**

11011 If the PSAP disconnects first, the Legacy PSAP Gateway SHALL wait a sufficient time period
11012 after the receipt of the on-hook signal from the CPE to determine that the on-hook
11013 condition is a disconnect, and not a hook flash (i.e., a request to generate or cancel a
11014 three-way conference). In most legacy implementations, the minimum time period is
11015 generally assumed to be approximately 1100 ms to consider the on-hook condition a
11016 disconnect request. At this point, the Legacy PSAP Gateway may offer a new call to the
11017 Legacy PSAP.

11018 **6.2.4.2.2 Call Disconnect Timing When Caller Disconnects First**

11019 If the caller disconnects (resulting in the Legacy PSAP Gateway sending an on-hook signal
11020 to the legacy PSAP) prior to the legacy PSAP disconnecting, the Legacy PSAP Gateway
11021 MUST wait a sufficient period of time after the PSAP has gone into an on-hook condition so
11022 that it is ready to respond to a new call being offered from the Legacy PSAP Gateway. This
11023 is sometimes described as a guard interval. Industry has not yet established a typical value
11024 for this timer. It varies by system, and by PSAP CPE type. Typical minimum values are: 700

⁸¹ Note that in some jurisdictions, certain wireline-type services support PSAP Call Control features disallowing the caller to disconnect first. See Appendix C- Support for PSAP Call Control Features (Normative) for details.

11025 ms, 1250 ms, or even 1650 ms between the on-hook condition from the PSAP CPE and the
11026 Legacy PSAP Gateway offering a new call to the legacy PSAP. (Under no circumstances
11027 SHALL the Legacy PSAP Gateway offer a call to the legacy PSAP when the legacy PSAP is
11028 still in an off-hook condition toward the Legacy PSAP Gateway.) The Legacy PSAP Gateway
11029 may set this guard timer value as appropriate for the CPE type, but MUST NOT offer new
11030 calls until a minimum interval after an on-hook indication has been received by the Legacy
11031 PSAP Gateway from the legacy PSAP CPE.

11032 **6.2.5 Trouble Detection/Reporting at the Legacy PSAP Gateway**

11033 The Legacy PSAP Gateway SHALL generate messages, alarms, etc. when it encounters
11034 problems with a legacy PSAP. The conditions under which a Legacy PSAP Gateway SHALL
11035 generate such messages/alarms shall include:

- 11036 • PSAP initiates a request for alternate routing/activates a make-busy switch
- 11037 • The Legacy PSAP Gateway detects a wink failure
- 11038 • A PSAP trunk stays in an off-hook condition longer than expected (keeping a circuit
11039 from being used).

11040 It is also desirable that the Legacy PSAP Gateway allows one or more members or circuits
11041 to a legacy PSAP to be taken out of service as necessary to test, modify, or manage the
11042 network.

11043 **7 Data and the Emergency Incident Data Object**

11044 With the implementation of NG9-1-1 there will be many forms of additional data available
11045 to policy routing rules, PSAPs and responders. Additional Data is communicated by
11046 reference or by value in the SIP INVITE and MESSAGE, in the PIDF-LO, or within responses
11047 to queries against IS-ADR functional elements or ADR URIs obtained from an ECRF.
11048 Additional Data has many conceivable uses, including informing telecommunicators and
11049 first responders, and providing a means to drive call routing and handling rules which look
11050 beyond caller location alone. Data generated by the PSAP while handling the call is
11051 captured in an Emergency Incident Data Object (EIDO) and passed to other agencies that
11052 are involved with the incident.

11053 **Note:** Specification for the conveyance of EIDOs between agencies, systems, and
11054 applications will appear in a future version of this document.

11055 **7.1 Additional Data**

11056 Any of the additional data elements in RFC 7852 [107], NG9-1-1 Additional Data, National
11057 Emergency Number Association, NENA 71-001 [73], or its successor document,

[MM/DD/YYYY]

Page 394 of 675



- 11058 NENA-STA-012.2.-2017 [193] may be used by PSAP management to establish business
11059 rules/policies for call handling and routing.
- 11060 Additional Data is defined as a set of blocks, with each block having different kinds of data
11061 contained within it. One block type is used to identify the provider of the data. Each block
11062 is passed individually. Additional Data is conveyed by reference or by value via a Call-Info
11063 header fields, or via URIs obtained from an ECRF, or by searching an IS-ADR.
11064 Dereferencing the URI is accomplished with an HTTPS GET (with fallback to HTTP if
11065 appropriate). ESInet elements use credentials traceable to the PCA, which must be
11066 accepted by the entity holding the data. Any source can provide any of the blocks
11067 registered in the IANA Emergency Call Data registry [179], but the following table provides
11068 examples of typical sources of blocks of Additional Data:

11069 **Table 7-1 Typical Sources of Additional Data**

Block	Typical Source
ProviderInfo	All
ServiceInfo	Originating Network or Service Provider
DeviceInfo	Device, Originating Network, or Service Provider
SubscriberInfo	Device, Originating Network, or Service Provider
Comment	All
VEDS	Vehicle or Telematics Service Provider

11070 The sources listed are not exclusive. In the above table, the device, originating network or
11071 caller could operate an ADR containing the data itself, or it could supply the data to a 3rd
11072 party which operates the ADR, or it can include the data by value in the call. Any
11073 intermediary (service provider) handling the call MUST provide a ProviderInfo block. Per
11074 RFC 7852 [107], when no originating network or service provider is in the path of the call,
11075 the calling device MUST provide Additional Call Data.

11076 Section 3.1.15 Originating Network Interface requires every emergency call to include
11077 certain Additional Data blocks conveyed via Call-Info header fields with an
11078 "EmergencyCallData" prefixed purpose parameter. Calls may include further Call-Info
11079 header fields with an "EmergencyCallData" prefixed purpose. The device MAY insert one for
11080 its DeviceInfo block and one for its ProviderInfo block, and an intermediary MAY insert its
11081 own set. When there are multiple intermediaries, each intermediary MAY insert a set for
11082 the blocks it is supplying. For example, a telematics service provider may provide one and
11083 the mobile carrier handling the call may provide one. (See Section 3.1.19 for more
11084 information about telematics calls and datasets.)

[MM/DD/YYYY]

Page 395 of 675



- 11085 To protect the privacy of the caller, the amount of information returned by the ADR query
11086 may vary depending on the TLS session credentials established by the entity executing the
11087 query. PSAPs SHALL have credentials traceable to the PCA that MUST be accepted by the
11088 data provider.
- 11089 Ultimately, a given call may have multiple sources of Additional Data from one or more
11090 ADRs. If conflicting information is discovered, the information identified as most recently
11091 updated by the data source SHALL take precedence over information determined to be
11092 older. See the note at the end of Section 4.2.2.5 Additional Data Interfaces.
- 11093 Additional Data received by reference MUST be passed by reference to any other entities.
11094 Additional Data URIs obtained from an ECRF may be added to the call in Call-Info header
11095 fields, as discussed in Section 4.2.2.5 Additional Data Interfaces.

11096 **7.2 Additional Data associated with a PSAP, the Emergency Incident Data 11097 Object**

- 11098 The Emergency Incident Data Object (EIDO) is defined in the NG9-1-1 Emergency Incident
11099 Data Object (EIDO) [111].
- 11100 When a PSAP handles a call, it develops information about the call which MAY be passed to
11101 subsequent PSAPs' dispatchers and/or responders. A reference to this structure SHALL be
11102 passed with a transferred call (see Section 4.7.4) and, if the transferred-to party wishes to
11103 obtain the EIDO as part of a dispatch operation, the structure MUST be retrieved using the
11104 EIDO Conveyance mechanisms defined in NENA/APCO-STA-024.1-201x [185] (work in
11105 progress).

11106 **8 3rd Party Origination**

- 11107 Service providers who operate call centers and wish to facilitate emergency calls from their
11108 subscribers with the call center agent remaining on the line (i.e., initially a three-way call
11109 with the caller, the call agent and the PSAP call taker) MAY use 3rd Party Origination.
- 11110 The caller is assumed to have a two-way SIP call between the caller and the call agent.
11111 Service providers who do not use SIP between the caller and the call agent MAY use a
11112 gateway to interwork the call signaling from the caller to SIP and MUST similarly use a
11113 gateway to interwork the signaling from the call agent to the caller from SIP. In such
11114 cases, the following signaling description applies, even though the call starts without a SIP
11115 call between the caller and call agent.

11116 **8.1 3rd Party Client is Referred to PSAP; PSAP Establishes Conference**

- 11117 In the first portion of the flow, the 3rd party client has encountered an emergency situation
11118 and a call is placed to the 3rd party call agent. The 3rd party call agent requests that the

[MM/DD/YYYY]

Page 396 of 675



11119 caller initiate an emergency call. Upon receiving an emergency session request that
11120 contains an indication of referral by a 3rd party agency, the PSAP establishes a session
11121 with a conference bridge and requests that the bridge refer the 3rd party call agent to the
11122 conference.

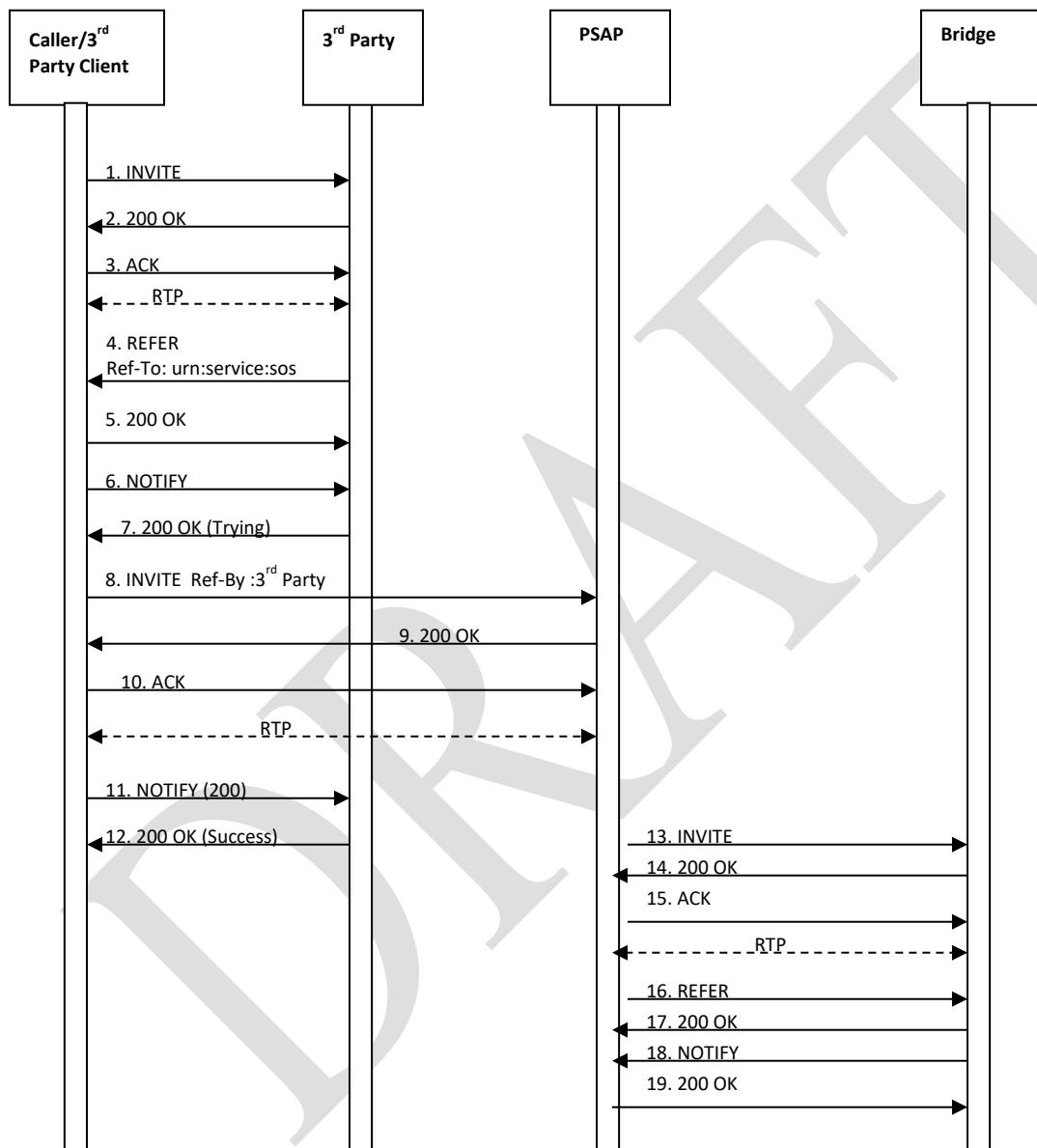


Figure 8-1 3rd Party Origination Call Flow – PSAP Conference

11123
11124 1. Upon encountering an emergency situation, an INVITE message is sent by a 3rd
11125 party client requesting that a session be established with a 3rd party call agent.
11126

- 11127 2. The 3rd party call agent responds to the INVITE message by returning a 200 OK
11128 message.
11129 3. The caller/3rd party client returns an ACK to the 3rd party call agent in response.
- 11130 *At this point a session is established between the caller/3rd party client and the 3rd*
11131 *party call agent. The agent determines that a 9-1-1 call is required.*
- 11132 4. The 3rd party call agent sends a REFER message to the caller/3rd party client with a
11133 Refer-To header field containing the destination "urn:service:sos", which indicates
11134 that an emergency session request should be initiated. Note that the call agent
11135 includes an Additional Data URI in an escaped Call-Info header field in the REFER.
11136 5. The caller/3rd party client responds by returning a 200 OK message to the 3rd party
11137 call agent.
11138 6. The caller/3rd party client also returns a NOTIFY message, indicating the
11139 subscription state of the REFER request (i.e., active).
11140 7. The 3rd party call agent returns a 200 OK message in response to the NOTIFY
11141 message.
11142 8. The caller/3rd party client then initiates an emergency call by sending an INVITE
11143 message to "urn:service:sos". This INVITE is a normal 9-1-1 call, and has all of the
11144 content specified by RFC 6881 [46]. This INVITE message contains a Referred-by
11145 header field [28]indicating that this emergency session request is associated with a
11146 REFER that was generated by a 3rd party call agent. It also includes the Additional
11147 Data URI that it received in the escaped Call-Info header field in the REFER from the
11148 3rd party call agent.
11149 9. When the PSAP receives the emergency session request with the Referred-By
11150 header field, it returns a 200 OK message to the caller/3rd party client.
11151 10.The caller/3rd party client responds by returning an ACK to the PSAP.
- 11152 *At this point, a session is established between the caller/3rd party client and the PSAP.*
- 11153 11.The caller/3rd party client sends a NOTIFY message to the 3rd party call agent
11154 updating the status of the REFER request.
11155 12.The 3rd party call agent responds by returning a 200 OK confirming the success of
11156 the REFER.
11157 13.Based on receipt of the Referred-By header field in the INVITE message from the
11158 caller/3rd party client indicating a need for a bridge to handle a 3-way call, the PSAP
11159 sends an INVITE to its conference bridge to establish a session with the bridge.
11160 14.The bridge responds by returning a 200 OK message to the PSAP.
11161 15.The PSAP responds by sending an ACK to the bridge.
11162 16.The PSAP sends a REFER message to the bridge requesting that it invite the 3rd
11163 party call agent to the conference.
11164 17.The bridge responds by sending a 200 OK message to the PSAP.

- 11165 18. The bridge then sends a NOTIFY message indicating the status of the REFER request.
11166
11167 19. The PSAP responds to the NOTIFY by returning a 200 OK message to the bridge.

11168 **8.2 3rd Party Call Agent and Caller Added to Conference**

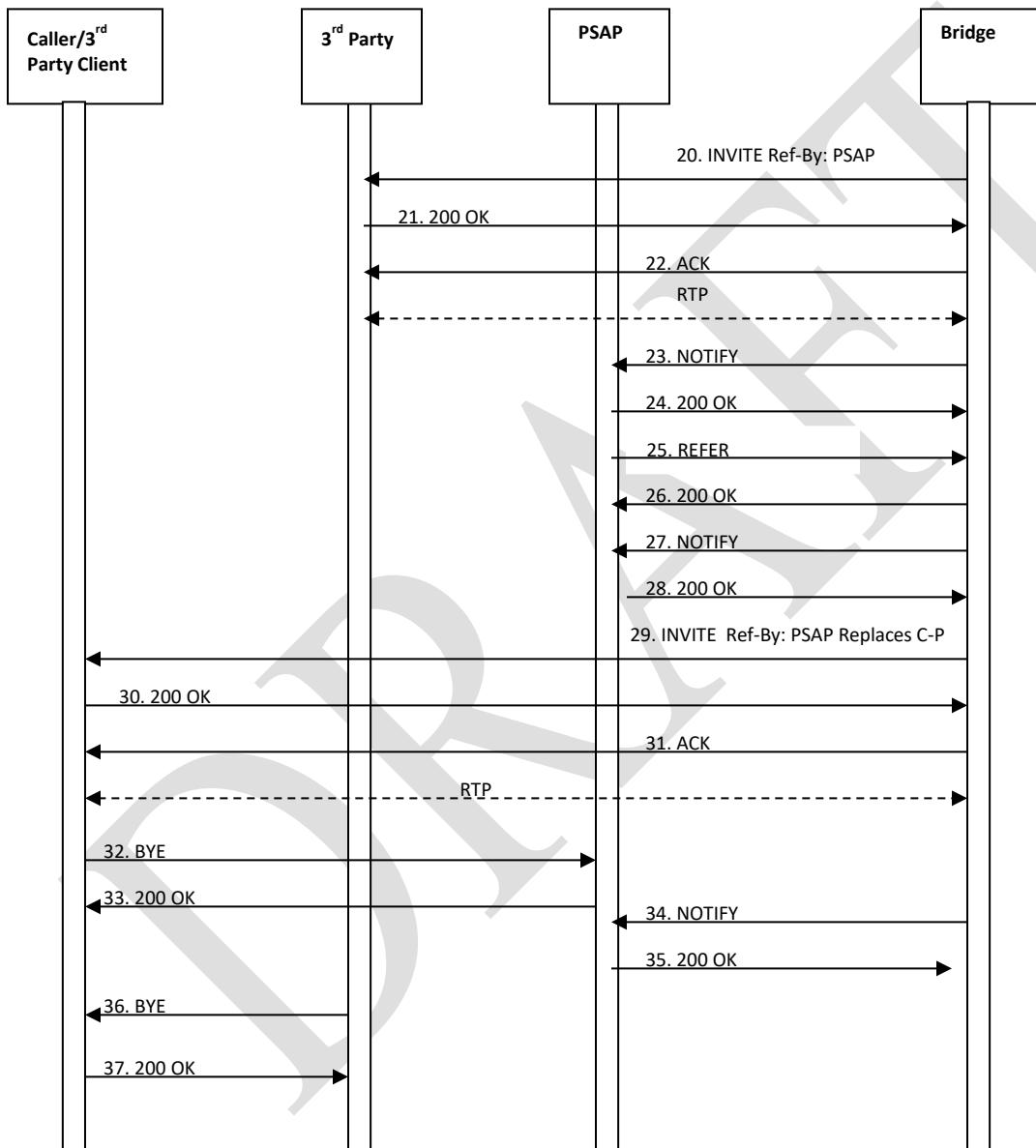


Figure 8-2 3rd Party Call Agent - Caller Added

- 11171 20. The bridge sends an INVITE message to the 3rd party call agent. The INVITE
11172 contains an indication in a Referred-by header field [28] that it is related to a REFER
11173 initiated by the PSAP.
- 11174 21. The 3rd party call agent responds by returning a 200 OK message to the bridge.
- 11175 22. The bridge returns an ACK to the 3rd party call agent.
- 11176 *At this point a session is established between the 3rd party call agent and the bridge.*
- 11177 23. The bridge sends a NOTIFY message to the PSAP indicating the status of the REFER
11178 request.
- 11179 24. The PSAP responds by returning a 200 OK message.
- 11180 25. The PSAP then sends a REFER message to the bridge requesting that it invite the
11181 caller/3rd party client to the conference. The REFER includes a Replaces header field
11182 to indicate to the caller/3rd party that the session with the bridge replaces its
11183 existing session with the PSAP.
- 11184 26. The bridge responds by sending a 200 OK message to the PSAP.
- 11185 27. The bridge then sends a NOTIFY message to the PSAP indicating the status of the
11186 REFER request.
- 11187 28. The PSAP responds by returning a 200 OK message.
- 11188 29. The bridge then sends an INVITE message to the caller/3rd party client asking that
11189 they replace their connection to the PSAP with a connection to the bridge.
- 11190 30. The caller/3rd party client responds by returning a 200 OK message to the bridge.
- 11191 31. The bridge responds by returning an ACK to the caller/3rd party client.
- 11192 *At this point the caller/3rd party client has established a session with the bridge.*
- 11193 32. The caller/3rd party client then sends a BYE message to the PSAP to terminate its
11194 session with the PSAP.
- 11195 33. The PSAP responds by sending a 200 OK message to the caller/3rd party client.
- 11196 34. The bridge sends a NOTIFY message to the PSAP indicating the status of the REFER
11197 request.
- 11198 35. The PSAP responds by sending a 200 OK message to the bridge.
- 11199 36. The 3rd party call agent sends a BYE message to the caller/3rd party client to
11200 terminate the session it had with the caller/3rd party client.
- 11201 37. The caller/3rd party client responds by returning a 200 OK to the 3rd party call
11202 agent.
- 11203 The above sequence assumes that the caller/3rd party client has the most accurate
11204 location information to route and dispatch the call. In some circumstances, the 3rd party
11205 call agent may have better location. It can supply the location in an EIDO, or it can arrange
11206 to have the caller/3rd party client send its emergency call INVITE (Step 8) through the 3rd
11207 party call agent and add the more accurate location to the call.

11208 Either the 3rd party client or the caller can initiate the disconnection of the original session
11209 between them (Step 36).

11210 **9 Test Calls**

11211 NG9-1-1 PSAPs MUST implement the test function described in RFC 6881 [46]. As the
11212 function is designed to test if a 9-1-1 call was placed from the test-initiating device, the
11213 test mechanism SHOULD mimic the entire actual 9-1-1 call path as closely as practical. The
11214 test mechanism is completely automatic, with no manual intervention required. To route
11215 the same as an actual emergency call, route urns in the “urn:emergency:service” tree are
11216 provided for test calls.

11217 An INVITE message with the Service URN (found in the Request-URI) of
11218 “urn:service:test.sos” SHALL be interpreted as a request to initiate a test call. The PSAP
11219 SHOULD return a 200 OK response in normal conditions, indicating that it will complete the
11220 test function. The PSAP MAY limit the number of test calls. If that limit is exceeded, the
11221 response MUST be 486 Busy Here. PSAPs MAY accept requests for sub-services such as
11222 “urn:service:test.sos.fire.” and complete a test call, or the PSAP MAY reject the call and
11223 return 404 Not Found. PSAP management MAY disable the test function (using PSAP
11224 policy).

11225 If the PSAP accepts the test, it SHOULD return in the 200 OK a body with MIME type
11226 text/plain consisting of the following contents:

- 11227 a. The name of the PSAP, terminated by a CR and LF;
- 11228 b. The string “urn:service:test.sos” terminated by a CR and LF;
- 11229 c. The location reported with the call (in the Geolocation header field). If the location
11230 was provided by value, the response would be a natural text version of the received
11231 location. If the location was provided by reference, the PSAP SHOULD dereference
11232 the location, using credentials acceptable to the LIS issued specifically for test
11233 purposes. Credentials issued by a PCA-rooted CA MUST have the token “test” as the
11234 agent name or the first token in the FQDN. The location returned may not be the
11235 same as the LIS would issue for an actual emergency call.

11236 The PSAP SHOULD insert its identity in the Contact header field of the response. To
11237 provide authentication, the Identity header field (RFC 8224 [60]) SHOULD be inserted,
11238 signed by an entity in the path (such as an ESRP) with a certificate traceable to the PCA.

11239 A PSAP accepting a test call SHOULD accept a media loopback test (RFC 6849) [100] and
11240 SHOULD support the “rtp-pkt-loopback” and “rtp-start-loopback” options. The PSAP user
11241 agent would specify a loopback attribute of “loopback-source”, the PSAP being the mirror.
11242 The PSAP SHOULD loop back no more than 3 packets of each media type accepted (voice,
11243 video, text), after which the PSAP SHOULD send BYE.

11244 PSAP CPE SHOULD refuse repeated requests for test from the same device (same Contact
11245 URI or source IP address/port) in a short period of time (within 2 minutes). Any refusal is
11246 signaled with a 486 Busy Here.

11247 **Note:** A PSAP Management interface will be provided in a future version of this document.

11248 **10 IANA Actions**

11249 Registries mentioned below are all within the "emergency" registry.

11250 **10.1 "urn:emergency" namespace**

11251 IANA is requested to add the following values to the urn:emergency registry.

Name	Purpose	Reference
service	Internal LoST queries	This document
policy	Route Policy	This document
normalnexthop	Normal route for Route Policy	This document
servicenotimplemented	Error response for no service within boundary of ECRF	This document
media-feature	TTY interworking and PSAP Call Control features	This document
uid	Unique identifiers	This document

11252

11253 **10.2 "urn:emergency:service" URN Subregistry**

11254 IANA is requested to add the following values to the urn:emergency:service registry

Name	Purpose	Reference
additionalData	Return a URI to an Additional Data block	This document
serviceAgencyLocator	Return a URI to a Service or Agency	This document
psap	Return a URI to a PSAP	This document
responder	Routing emergency calls within the ESInet towards a responder.	This document
sos	Routing emergency calls within the ESInet toward a primary PSAP call taker.	This document

11255

11256 **10.3 "urn:emergency:service:sos" Registry**

11257 IANA is requested to add the following values to the urn:emergency:service:sos registry

[MM/DD/YYYY]

Page 402 of 675



Name	Purpose	Reference
psap	Route calls to primary PSAP.	This document
call_taker	Route calls to a call taker within a PSAP.	This document
level_2_esrp	Route calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP)	This document
level_3_esrp	Route calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).	This document

11258

10.4 “urn:emergency:service:test” Registry

11260 IANA is requested to add the following values to the urn:emergency:service:test registry

Name	Purpose	Reference
psap	Route test calls to primary PSAP	This document
call_taker	Normally not used, but some implementations may make use of this urn	This document
level_2_esrp	Route test calls to a second level ESRP (for an example, a state ESRP routing towards a county ESRP)	This document
level_3_esrp	Route test calls to a third level ESRP (for example, a regional ESRP that received a call from a state ESRP and in turn routes towards a county ESRP).	This document

10.5 “urn:emergency:service:responder” Registry

11261 IANA is requested to add the following values to the urn:emergency:service:responder registry

Name	Description	Reference
coast_guard	Coast Guard station	This document
ems	Emergency Medical Service	This document
fire	Fire Department	This document
mountain_rescue	Mountain Rescue Service	This document
poison_control	Poison Control Center	This document
police	Police Agency	This document

[MM/DD/YYYY]

Page 403 of 675



Name	Description	Reference
psap	other purposes beyond use for dispatch via ECRF	This document

11264

11265 **10.6 “urn:emergency:service:responder.police” Registry**

11266 IANA is requested to add the following values to the
11267 urn:emergency:service:responder.police registry

Name	Description	Reference
federal	An appropriate federal agency (subregistry defined below)	This document
stateProvincial	State or provincial police office	This document
tribal	Native American police (reservation)	This document
countyParish	County or Parish police (not Sheriff)	This document
sheriff	Sheriff's office, when both a police and Sheriff dispatch may be possible	This document
local	City, Town, Township, Borough or Village police	This document

11268 **10.7 “police.federal” Registry**

11269 IANA is requested to add the following values to the
11270 urn:emergency:service:responder.police.federal registry

Name	Full Name	Reference
fbi	Federal Bureau of Investigation	This document
rcmp	Royal Canadian Mounted Police	This document
ussss	U.S. Secret Service	This document
dea	Drug Enforcement Agency	This document
marshal	Marshals Service	This document
cbp	Customs and Border Protection	This document
ice	Immigration and Customs Enforcement	This document
atf	Bureau of Alcohol, Tobacco, Firearms and Explosives	This document
pp	U.S. Park Police	This document
dss	Diplomatic Security Service	This document
fps	Federal Protective Service	This document
military	Used for military installations	This document

[MM/DD/YYYY]

Page 404 of 675



11271 **10.8 “urn:emergency:service:responder.fire” Registry**

11272 IANA is requested to add the following values to the urn:emergency:service:responder.fire registry
11273

Name	Description	Reference
forest	Forest Fire Service	This document
airport	Airort Fire Service	This document
military	Used for military installations	This document
private	Private Fire Service	This document

11274 **10.9 “urn:emergency:service:responder.ems” Registry**

11275 IANA is requested to add the following values to the urn:emergency:service:responder.ems registry
11276

Name	Description	Reference
tribal	Native American EMS (reservation)	This document
countyParish	County or Parish EMS	This document
local	City, Town, Township, Borough or Village EMS	This document
private	Contracted Ambulance Service	This document
military	Used for military installations	This document

11277 **10.10 “urn:emergency:uid” Registry**

11278 IANA is requested to add the following values to the urn:emergency:uid registry

Name	Purpose	Reference
callid	Call Tracking Identifier	This document
incidentid	Incident Tracking Identifier	This document
logid	LogEvent Identifier	This document
lostsrc	LoST Source Identifier	This document
lostQuery	LoST Query Identifier	This document
queryd	Query identifier (links a response to its query)	This document
subid	Subscription identifier (links a SUBSCRIBEs/RESPONSEs)	This document

11279 **10.11 “serviceNames” Registry**

11280 IANA is requested to add the following values to the serviceNames registry

Service Name	Service	Reference
ADR	Additional Data Repository (if hosted on an ESInet)	This document

[MM/DD/YYYY]

Page 405 of 675



Bridge	Bridge	This document
ECRF	Emergency Call Routing Function	This document
ESRP	Emergency Service Routing Proxy	This document
GCS	Geocode Conversion Service	This document
IMR	Interactive Media Response Service	This document
Logging	Logging Service	This document
LVF	Location Validation Function	This document
MCS	MSAG Conversion Service	This document
MDS	Mapping Data Service	This document
PolicyStore	Policy Store	This document
PSAP	PSAP	This document
SAL	Service/Agency Locator	This document

11281

10.12 "serviceState" Registry

11283 IANA is requested to add the following values to the serviceState registry

Name	Description	Reference
Normal	The service is operating normally. Calls can be sent to this destination normally.	This document
Unstaffed	(applies to PSAPs only) The PSAP has indicated that it is not currently answering calls. Calls must be sent to another destination.	This document
ScheduledMaintenanceDown	The service is undergoing maintenance activities and is not accepting service requests. Calls must be sent to another destination.	This document
ScheduledMaintenanceAvailable	The service is undergoing maintenance activities, but will respond to service requests, possibly with reduced availability. Calls can be sent to this destination normally.	This document
MajorIncidentInProgress	The element is operating normally but is handling a major incident and may be unable to accept some requests. Calls could be sent to this destination	This document

[MM/DD/YYYY]

Page 406 of 675



Name	Description	Reference
	but doing so may precipitate that destination into an overloaded state.	
Partial	Processing some requests, but response may be delayed. Calls could be sent to this destination.	This document
Overloaded	The service is completely overloaded. Calls must be sent to another destination.	This document
GoingDown	The service is being taken out of service. Calls must be sent to another destination.	This document
Down	The service is unavailable. Calls must be sent to another destination.	This document
Unreachable	Subscriber is unable to contact the service.	This document

11284

10.13 “elementState” Registry

11285 IANA is requested to add the following values to the elementState registry

Name	Description	Reference
Normal	The element is operating normally	This document
ScheduledMaintenance	The element is undergoing maintenance activities and is not processing requests	This document
ServiceDisruption	The element has significant problems and is unable to process all requests	This document
Overloaded	The element is completely overloaded	This document
GoingDown	The element is being taken out of service	This document
Down	The element is unavailable	This document
Unreachable	Subscriber is unable to contact the service	This document

11287

10.14 “urn:emergency:service:serviceagencyLocator” Registry

11288 IANA is requested to add the following values to the
11289 urn:emergency:service:serviceagencylocator registry:

[MM/DD/YYYY]

Page 407 of 675



Service Identifier	Service	Reference
ADR	Additional Data Repository (if hosted on an ESInet)	This document
Bridge	Bridge	This document
BCF	Border Control Function	This document
ECRF	Emergency Call Routing Function	This document
ESRP	Emergency Service Routing Proxy	This document
GCS	Geocode Conversion Service	This document
IMR	Interactive Media Response Service	This document
Logging	Logging Service	This document
LVF	Location Validation Function	This document
MCS	MSAG Conversion Service	This document
MDS	Mapping Data Service	This document
PolicyStore	Policy Store	This document
PSAP	PSAP	This document
SAL	Service/Agency Locator	This document

11291

10.15 “SIPheaderIsOperatorConditions” Registry

11293 IANA is requested to add the following values to the SIPheaderIsOperatorCondition registry

Name	Description	Reference
present	The header field is present	This document
missing	The header field is not present	This document
badSyntax	The header field is syntactically incorrect	This document
erroneous	The header field contains syntactically correct but erroneous contact	This document

11294

10.16 “urn:emergency:media-feature” Registry

11295 IANA is requested to add the following values to the urn:emergency:media-feature registry:
11297

Tag	Purpose	Reference
psap-call-control	UA can support Call Party Hold per Appendix C	This document
tty-interworking	UA supports TTY interworking	This document

[MM/DD/YYYY]

Page 408 of 675



11298 **10.17 “queueState” Registry**

11299 IANA is requested to add the following values to the queueState registry:

Name	Description	Reference
Active	One or more entities are actively available or are currently handling calls being enqueued	This document
Inactive	No entity is available or actively handling calls being enqueued	This document
Disabled	The queue is disabled by management action and no calls may be enqueued	This document
Full	The queue is full, and no new calls can be enqueued on it	This document
Standby	The queue has one or more entities that are available to take calls, but the queue is not presently in use. When a call is enqueued, the state changes to “Active”	This document
ResourceExhausted	The downstream entity cannot accept any more calls for a reason other than one of the above conditions.	This document
Unreachable	The queue is unreachable. Used by the subscriber to provide a value when it is unable to subscribe.	This document

11300

11301 **10.18 “securityPosture” Registry**

11302 IANA is requested to add the following entries to the securityPosture registry:

Value	Purpose	Reference
Green	The entity is operating normally. Calls can be sent to this destination normally.	This document
Yellow	The entity is receiving suspicious activity but is able to operate normally. Calls could be sent to this destination.	This document
Orange	The entity is receiving fraudulent calls/events, is stressed, but is able to continue most operations. Calls could be sent to this destination but doing so may precipitate that destination into an overloaded state.	This document
Red	The entity is under active attack and is overwhelmed. Calls must be sent to another destination.	This document

[MM/DD/YYYY]

Page 409 of 675



11303

10.19 "ESRP Notify Event Code" Registry

IANA is requested to add the following entries to the EsrpNotifyEventCode registry:

Value	Purpose	Category	Reference
Normal	A normal route action was performed. This is a courtesy notification	Safety	This document
Default	There was insufficient location information to determine the next hop, a default location was used for routing	Safety	This document
Congestion	The normal route was congested; an alternate route was taken	Safety	This document
Disaster	The normal destination is in disaster mode and this call was diverted	Safety	This document
IMR	The call met the conditions for diversion to an IMR (Interactive Media Response)	Safety	This document
Busy	There were no routes available and busy was returned for this call	Safety	This document
Error	The ESRP encountered an error and a default route was taken	Safety	This document
Fatal Error	The ESRP encountered a fatal error that caused the call to fail (i.e., got a 600 Busy Everywhere response)	Safety	This document
TimeOfDay	An alternate PSAP handles calls in off hours	Safety	This document
GenericPolicy	Diversion occurred because of policy, not covered above	Safety	This document
Test	This is a test call	Safety	This document

10.20 "Route Cause" Registry

IANA is requested to add the following entries to the RouteCause registry:

Value	Code	Text	Reference
Normal-NextHop	200	Normal Next Hop	This document
TimeOfDay	401	Time of Day	This document
Congestion	402	Congestion	This document
Disaster	403	Disaster	This document
IMR	404	Interactive Media Response	This document
GenericPolicy	405	Policy decision not covered above	This document

[MM/DD/YYYY]

Page 410 of 675



Value	Code	Text	Reference
Default	406	Default with no/bad location	This document

11308

10.21 “LogEvent” Registry

11310 IANA is requested to add the following entries to the LogEvent registry:

Value	Purpose	Reference
CallProcessLogEvent	Logged by an FE that is not call stateful, to denote its handling of a call.	This document
CallStartLogEvent	Logged by an FE that is call stateful, when it begins processing a call.	This document
CallEndLogEvent	Logged by an element that is call stateful, when its processing of a call ends.	This document
RecCallStartLogEvent	RecCallStartEvent is identical to CallStartEvent, but is logged by the Logging Service (SRS) and the client (SRC) to denote the beginning of a SIPREC recording session.	This document
RecCallEndLogEvent	RecCallEndEvent is identical to CallEndEvent, but is logged by the Logging Service (SRS) and the client (SRC) to denote the end of a SIPREC recording session.	This document
CallTransferLogEvent	Logged by an FE when it transfers a call.	This document
RouteLogEvent	Logged by Proxy Servers (e.g., ESRPs) to denote the route selected and the rule or reason that caused the route to be selected.	This document
MediaStartLogEvent	Logged by an FE that anchors media, to denote the start of a given call medium. Includes the SDP that describes the medium.	This document
MediaEndLogEvent	Logged by an FE that anchors media, to denote end of a medium. Includes the specific media label from the SDP which describes the medium that has ended.	This document
RecMediaStartLogEvent	RecMediaStartEvent is identical to MediaStartEvent but is logged by the SRS and SRC to denote the start of a medium in a SIPREC recording session.	This document

[MM/DD/YYYY]

Page 411 of 675



Value	Purpose	Reference
RecMediaEndLogEvent	RecMediaEndEvent is identical to MediaEndEvent but is logged by the SRS and SRC to denote the end of a medium in a SIPREC recording session.	This document
RecordingFailedLogEvent	Logged by an SRC or SRS when its attempt to record media via a SIPREC session fails.	This document
MessageLogEvent	Logged by an FE when it handles a SIP MESSAGE request.	This document
AdditionalAgencyLogEvent	Logged by an FE when it is discovered that another agency may be involved in an Incident.	This document
IncidentMergeLogEvent	Logged by an FE to denote that this is an additional call about an Incident that is already being handled, effectively assigning the call to the existing Incident.	This document
IncidentUnMergeLogEvent	Logged by an FE to counteract a IncidentMergeEvent that it previously logged.	This document
IncidentSplitLogEvent	Logged by an FE when it creates a new Incident by "cloning" (copying the data from) an existing Incident.	This document
IncidentLinkLogEvent	Logged by an FE to associate an Incident with another Incident, when the two Incidents are somehow related but are not the same Incident.	This document
IncidentUnLinkLogEvent	Logged by an FE to counteract a IncidentLinkEvent that it previously logged.	This document
IncidentClearLogEvent	When an agency finishes its handling of an Incident, the responsible FE logs an IncidentClearEvent record. Other agencies may still be processing the Incident.	This document
IncidentReopenLogEvent	If an agency needs to log new events on an Incident for which it has previously logged an IncidentClearEvent, the responsible FE logs an IncidentReopenEvent.	This document
LostQueryLogEvent	Logged by an FE that sends or receives a LoST query. Includes a unique "LostQueryId" that will be returned in the response to allow matching the query to the response.	This document
LostResponseLogEvent	Logged by an FE when it sends or receives a LoST response. Includes the "LostQueryId" that was	This document

Value	Purpose	Reference
	included in the corresponding LoST query, to allow matching the response to the query.	
CallSignalingMessageLogEvent	An FE logs call signaling messages (e.g., SIP requests and responses) that it sends or receives.	This document
SiprecMetadataLogEvent	Used by the Logging Service to log any SIPREC metadata it receives from the SRC.	This document
NonRtpMediaMessageLogEvent	Used by the Logging Service to log media that do not use RTP for transport.	This document
AliLocationQueryLogEvent	Used by an LSRG to log an ALI query it sends or receives. Includes a unique "AliLocationQueryId" that will be returned in the response to allow matching the query to the response.	This document
AliLocationResponseLogEvent	Used by an LSRG to log an ALI response it sends or receives. Includes the "AliLocationQueryId" that was included in the corresponding ALI query, to allow matching the response to the query.	This document
MalformedMessageLogEvent	Used by an FE to log a malformed SIP request it received.	This document
EidoLogEvent	Logged by an FE that sends or receives an Emergency Incident Data Object (EIDO), or a reference to an EIDO.	This document
DiscrepancyReportLogEvent	Logged by an FE that sends or receives a Discrepancy Report (DR) or an update to a DR (Status, Resolution, etc.).	This document
ElementStateChangeLogEvent	Logged by an FE to denote a change to one of the states listed in the elementState registry.	This document
ServiceStateChangeLogEvent	Logged by a Service to denote a change to one of the states listed in the serviceState.	This document
AdditionalDataQueryLogEvent	Used by an FE to log an Additional Data query it sends or receives. Includes an "AdditionalDataQueryId" used to match the query to its response.	This document
AdditionalDataResponseLogEvent	Used by an FE to log an Additional Data response it sends or receives. Includes the "AdditionalDataQueryId" from the original query, which is used to match the response to its query.	This document
LocationQueryLogEvent	Used by an FE to log a HELD dereference or SIP SUBSCRIBE request for location data. Includes a	This document

[MM/DD/YYYY]

Page 413 of 675



Value	Purpose	Reference
	“LocationQueryId” used to match the dereference or subscription to its response.	
LocationResponseLogEvent	Used by an FE to log a HELD response or a SIP NOTIFY with location. Includes the “LocationQueryId” from the original query or SUBSCRIBE, which is used to match the response to its dereference or query.	This document
CallStateChangeLogEvent	Used by an FE to log a call state change to one of the states listed in the CallStates registry.	This document
GatewayCallLogEvent	Used by an LNG, LPG, or LSRG to log a call entering or leaving it on a legacy interface.	This document
HookflashLogEvent	An LPG logs the HookflashEvent when a “hookflash” is detected on a legacy interface.	This document
LegacyDigitsLogEvent	Used by an LPG to log DTMF or MF digits received or generated on a legacy interface.	This document
AgentStateChangeLogEvent	Used by an FE to log an Agent state change to one of the states in the AgentStates registry in the IANA registry.	This document
QueueStateChangeLogEvent	Logged by an FE that manages a queue to denote a change in state to one of the states listed in the QueueState registry.	This document
KeepAliveFailureLogEvent	Used by an FE to log a malformed, invalid, or timed-out response for an OPTIONS request it sent to another FE or Service.	This document
RouteRuleMsgLogEvent	Logs the “log” element from the Route Policy Syntax containing details on the given rule set.	This document
PolicyChangeLogEvent	An FE logs the PolicyChangeEvent when a policy is created, updated, or deleted.	This document
VersionsLogEvent	Used by an FE to log the response it receives for a Versions request it issued to a web service on an initial request or when the response has changed.	This document
SubscribeLogEvent	Logs subscription requests for any defined Event Package.	This document

11311 10.22 “LogEvent Protocol” Registry

11312 IANA is requested to add the following entries to the LogEventProtocol registry:

[MM/DD/YYYY]

Page 414 of 675



Name	Reference
SIP	RFC3261
MSRP	RFC4975

11313 **10.23 “LogEvent CallTypes” Registry**

11314 IANA is requested to add the following entries to the LogEvent CallTypes registry:

Name	Description	Classification
emergency	Call is deemed urgent call and treated as such	Primary
nonEmergency	Call is not deemed urgent	Primary
silentMonitoring	Silently monitor the activities of the target	Primary
intervene	Intervene on the activities of the target	Primary
legacyWireline	Call from a wireline device received from a legacy network	Secondary
legacyWireless	Call from a wireless device received from a legacy network	Secondary
legacyVoip	Call from a VoIP device received from a legacy network	Secondary

11315 **10.24 “Call States” Registry**

11316 IANA is requested to add the following entries to the CallStates registry:

Name	Description
callBegin	Indicates the start of a new call. If the call is also a SIP call, the CallStart LogEvent must be logged. “CallStateLegCallId” must not be supplied as no third leg is involved. “CallStateTargetID” must either be the address of the destination target (in the case of a call being originated) or the address of the originator (in the case the call is being received)
callAlerting	A notification of the call is being presented. “CallStateLegCallId” and “CallStateTargetID” must not be supplied.
callQueued	A call is on a queue to be answered. “CallStateLegCallId” must not be supplied; “CallStateTargetID” must be the name of the queue.
callAnswered	Indicates that the call has been answered. “CallStateTargetID” may indicate the device used to answer the call (not the agent, agentID is for that purpose). “CallStateLegCallId” must not be supplied.
callEnd	Indicates the end of a call. If the call is also a SIP call, the CallEnd LogEvent must be logged. “CallStateLegCallId” and “CallStateTargetID” must not be supplied.

Name	Description
callCancel	A cancel request has been received for the call. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.
callHold	Indicates that the call has been put on hold for later retrieval. If the use of an external device such as a Music-on-Hold server is used, the "CallStateLegCallId" should contain the identifier of that call leg and "CallStateTargetID" may contain its identity.
callPark	Indicates that the call has been parked for later retrieval. "CallStateTargetID" must contain the park identifier orbit that was used. If an external device is used, the "CallStateLegCallId" should contain the identifier of that call leg.
callRetrieve	Indicates that a held or parked call has been re-activated. "CallStateLegCallId" and "CallStateTargetID" must not be supplied.
partyAdd	Indicates that the addition of a party to the call is being requested (thus creating a conference in the case there was only two parties). "CallStateTargetID" must specify the identity of the party being added and "CallStateLegCallId" must specify the identifier of the call leg used to contact the party. This LogEvent must be generated at the beginning of the attempt to add a party. The outcome of the attempt is determined by the events related to the call leg specified by "CallStateLegCallId".
partyRemove	Indicates that a party has been removed from a conference (either by user request or by loss of call leg). "CallStateTargetID" must specify the identity of the party removed. "CallStateLegCallId" must not be supplied.
callBargeIn	Indicates that an outside party requests to join an active call. For the originator of the barge in request, "CallStateLegCallId" specifies the identity of the call to be joined. For the recipient of the barge in request, "CallStateLegCallId" specifies the identity of the call leg to be added to the active call. The outcome of the barge in request is determined by the events related to the call leg barging into the active call.

11317 **10.25 "LogEvent Announcement Types" Registry**

11318 IANA is requested to add the following entries to the LogEventAnnoucementTypes registry:

Name	Description
AutoAnswerGreeting	Indicates an announcement played automatically after a call is answered by an agent. Typically recorded with the agent's voice, this type of recorded greeting is used to standardize the answering of calls.

Name	Description
NoAgentsAvailableAnnouncement	Indicates an announcement indicating no agents are currently available to take the call and the call will be answered by the next available agent.
StandardAnnouncement	Indicates an announcement played to all calls regardless of the availability of agents to take the call.

11319 **10.26 “Non-RTP Media Types” Registry**

11320 IANA is requested to add the following entries to the nonRTPmediaTypes registry:

Name	Description
MSRP	Media Session Relay Protocol

11321

11322 **10.27 “Agency Roles” Registry**

11323 IANA is requested to add the following entries to the AgencyRoles registry:

Role	Description	Reference
PSAP	Per NENA ADM-000 Master Glossary: "... responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy."	This document
Dispatch	Per ANSI.107.1.2015: "... alerting and directing the response of public safety responders to the desired location".	This document
911 Authority	Per NENA ADM-000 Master Glossary: "... governmental entity responsible for 9-1-1 service operations.	This document
ESInet Service Provider	The entity responsible for the operation of an Emergency Services IP Network.	This document
ESRP Service Provider	The entity responsible for the operation of an Emergency Service Routing Proxy	This document
ECRF/LVF Service Provider	The entity responsible for the operation of an Emergency Call Routing Function/Location Validation Function.	This document
LIS Service Provider	The entity responsible for the operation of a Location Information Server.	This document

[MM/DD/YYYY]

Page 417 of 675



Role	Description	Reference
National	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
State	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
Regional	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document
Local	Agency Role modifier are scopes that can be applied to the above agency roles to further clarify the extent of the authority.	This document

11324 **10.28 "Agent Roles" Registry**

11325 IANA is requested to add the following entries to the AgentRoles registry:

Role	Description	Reference
Dispatching	Per ANS1.107.1.2015: "... alerting and directing the response of public safety responders to the desired location".	This document
Call Taking	Per ANS1.107.1.2015: "... processes incoming calls through the analyzing, prioritizing, and disseminating of information to aid in the safety of the public and responders".	This document
GIS Analysis	assembles and maintains geospatial and addressing information.	This document
IP Network Administration	monitors, manages and controls network elements and services (e.g., switches, routers, gateways, firewalls and network services such as DNS and DHCP); plans for and responds to service outages and other problems.	This document
Database Administration	installs, configures, manages, monitors and controls access to databases.	This document
IT Systems Administration	installs, configures, supports and maintains system hardware, operating systems, application elements and services; plans for and responds to service outages and other problems.	This document

[MM/DD/YYYY]

Page 418 of 675



Role	Description	Reference
Application Administration	installs, configures, supports and maintains applications; plans for and responds to service outages and other problems.	This document
Security Administration	creates, assigns, configures, maintains and supports user authentication and authorization elements and services; monitors for possible security violations and vulnerabilities, and ensures that vulnerabilities are corrected.	This document
Records Production	searches, retrieves and reproduces records and recordings for internal and external uses, including FOIA requests, subpoenas, and media requests.	This document
Data Analysis	researches and analyzes specific kinds of data to identify trends, anomalies and conditions important to supporting emergency services.	This document
Quality Assurance Evaluation	Per ANSI.1.107.1.2015: "... reviews telecommunicator work performance and documents an evaluation of the level of compliance with Agency directives and standards."	This document
Management	Role Modifier (may be added to further specify the above roles).	This document
Supervisor	Role Modifier (may be added to further specify the above roles).	This document
Trainer	Role Modifier (may be added to further specify the above roles).	This document
Trainee	Role Modifier (may be added to further specify the above roles).	This document
Assist Manager	Role Modifier (may be added to further specify the above roles).	This document
Shift Supervisor	oversees individuals who perform the Roles of Dispatching, Call Taking or a combination of both.	This document
GIS Specialist	plans, develops, and implements systems and databases for storing and accessing geospatial data.	This document
GIS Supervisor	oversees individuals who perform the Role of GIS Specialist.	This document

[MM/DD/YYYY]

Page 419 of 675



Role	Description	Reference
Maintenance Supervisor	oversees individuals who perform the Role of Maintenance Technician.	This document
Maintenance Technician	responsible for performing general maintenance and repairs on equipment and assets, assists with the installation of equipment and manages the upkeep of tools, equipment and machinery.	This document
Temporary Technician	on a short-term basis, responsible for performing general maintenance and repairs on equipment and assets, assists with the installation of equipment and manages the upkeep of tools, equipment and machinery.	This document
ESInet Network Operator	monitors and troubleshoots communication and application-related issues through the use of management and diagnostic tools for an Emergency Services IP Network.	This document
ESInet Network Operations Supervisor	oversees individuals who perform Role of ESInet Network Operator.	This document
911 Authority Director	controls the management and operation of a 911 Authority.	This document
911 Authority Agent	performs duties related to the operation of a 911 Authority.	This document
Database Administrator	uses specialized software to store and organize data, ensuring that data are available to users and secure from unauthorized access.	This document
IT Systems Analyst	uses analysis and design techniques to solve business problems using information technology	This document
Records Production Specialist	organizes and manages information data by ensuring that it maintains its quality, accuracy, accessibility, and security in both paper files and electronic systems.	This document

11326 **10.29 "Status Codes" Registry**

11327 IANA is requested to add the following entries to the StatusCodes registry:

Status Code	Description	Reference
333	Iterative Refer	This document
433	No such sourceId	This document

[MM/DD/YYYY]

Page 420 of 675



Status Code	Description	Reference
434	Signature Verification Failure	This document
436	Duplicate or Invalid Priority	This document
437	Bad Policy Structure	This document
438	Unacceptable Algorithm	This document
441	Index beyond available names	This document
442	Unacceptable Parameters	This document
451	Unknown or bad Policy Name	This document
452	Unknown or bad Agency Name	This document
453	Not available here, no referral available	This document
454	Unspecified Error	This document
456	Bad queue	This document
457	Bad dequeuePreference	This document
458	Policy Violation	This document
459	Bad PolicyExpirationTime	This document
460	Bad LogEvent	This document
461	LogEvent too big	This document
462	LogEvent extension not on allowed list	This document
463	LogEvent extension on disallowed list	This document
464	No Text in this Call	This document
465	Bad Timestamp	This document
466	EndTime occurs before StartTime	This document
467	Bad or missing Geoshape	This document
469	Unknown MCS/GCS	This document
470	Unknown Service/Database ("not ours")	This document
471	Unauthorized Reporter	This document
472	Unauthorized Responder	This document
473	Unknown ReportId	This document
474	Resolution already provided	This document
475	Response not available yet	This document

11328 10.30 "Interface Names" Registry

IANA is requested to add the following entries to the Interface Names registry:

Name	Reference
SIPcall	This document
LoST	This document
ElementState	This document

[MM/DD/YYYY]

Page 421 of 675



Name	Reference
ServiceState	This document
HELDdereference	This document
SIMPLEpresence	This document
PolicyStore	This document
DiscrepancyReport	This document
QueueState	This document
DequeueRegistration	This document
ESRPNotify	This document
AbandonedCall	This document
SI	This document
GapOverlap	This document
PIDFLOtoMSAG	This document
Geocode	This document
ReverseGeocode	This document
ConferenceEvent	This document
Logging	This document
SIPREC	This document
LoggingRetrieval	This document
AgencyLocatorDereference	This document
AgencyLocatorNameSearch	This document
MapDatabase	This document
LNGadr	This document

11330

10.31 “Match Type” Registry

IANA is requested to add the following entries to the Match Type registry:

Token	Description
Address	A datum representing a site, structure, or portion of a structure having a specific address.
RoadCenterline	A datum representing a road centerline, which may be associated with one or more ranges of addresses.
PoliticalBoundary	A datum representing a political subdivision, typically designated with country and one or more of A1, A2, A3, A4, and/or A5 (civic address elements).
MsagCommunity	A datum representing a legacy MSAG community. There is no defined method for routing by MSAG community in this document.

[MM/DD/YYYY]

Page 422 of 675



Token	Description
CoverageRegion	A datum used by a LoST server to define an area for which it can authoritatively answer queries.
Hybrid	Any combination of data that spans multiple layers or categories.
Other	Any source of data which is not otherwise defined in this registry.

11333

10.32 "GIS Data Layers" Registry

11335 IANA is requested to add the following entries to the GIS Data Layers registry:

Name	Reference
RoadCenterLine	This document
SiteStructurePoint	This document
PsapPolygon	This document
PolicePolygon	This document
FirePolygon	This document
FireForestPolygon	This document
FireAirportPolygon	This document
FireMilitaryPolygon	This document
FirePrivatePolygon	This document
EmsPolygon	This document
EmsPrivatePolygon	This document
EmsAirPolygon	This document
EmsMilitaryPolygon	This document
PoisonControlPolygon	This document
MountainRescuePolygon	This document
CoastGuardPolygon	This document
PoliceCountyPolygon	This document
PoliceStateProvincialPolygon	This document
PoliceFederalPolygon	This document
PoliceFederalFbiPolygon	This document
PoliceFederalRcmpPolygon	This document
PoliceFederalSecretServicePolygon	This document
PoliceFederalDeaPolygon	This document
PoliceFederalMarshalPolygon	This document
PoliceFederalCustomsBorderProtectionPolygon	This document
PoliceFederalImmigrationCustomsPolygon	This document
PoliceFederalAtfPolygon	This document

[MM/DD/YYYY]

Page 423 of 675



Name	Reference
PoliceFederalParkPolygon	This document
PoliceFederalDiplomaticSecurityPolygon	This document
PoliceFederalProtectiveServicePolygon	This document
PoliceSheriffPolygon	This document
PoliceMilitaryPolygon	This document
PoliceCampusPolygon	This document
PolicePrivatePolygon	This document
PoliceAirportPolygon	This document
PoliceHousingPolygon	This document
PoliceParkPolygon	This document
StreetNameAliasTable	This document
LandmarkNamePartTable	This document
LandmarkNameCompleteAliasTable	This document
A1Polygon	This document
A2Polygon	This document
A3Polygon	This document
A4Polygon	This document
A5Polygon	This document
RailroadCenterLine	This document
HydrologyLine	This document
HydrologyPolygon	This document
CellSectorPoint	This document
LocationMarkerPoint	This document

11336

11337 **10.33 “Policy Type” Registry**

11338 IANA is requested to add the following entries to the Policy Type registry:

Type	Format	Use	Reference
OriginationRoutePolicy	PRR	Policy Routing Rules for incoming queue	This document
NormalNextHopRoutePolicy	PRR	Policy Routing Rules for Normal Next Hop	This document
OtherRoutePolicy	PRR	Policy Routing Rules for common policies	This document

[MM/DD/YYYY]

Page 424 of 675



Type	Format	Use	Reference
DequeueExpirationTime	XACML	How long subscriptions to DequeueRegistration are allowed	This document
GISReplicas	XACML	Which entities are allowed to maintain replicas of GIS data	This document
ECRF-LVFreplica	XACML	Which entities are allowed to maintain replicas of ECRF/LVF data	This document
TestCalls	XACML	Which originators may process PRR test calls	This document
SIPcall	XACML	Access rights for a SIP Call Interface.	This document
LoST	XACML	Access rights for a LoST Interface	This document
ElementState	XACML	Access rights for ElementState subscription	This document
ServiceState	XACML	Access rights for ServiceState subscription	This document
HELDdereference	XACML	Access rights for HELD dereference interface	This document
AgentPresencePublish	XACML	Access rights for presence (sip) PUBLISH interface	This document
AgentPresencePut	XACML	Access rights for presence (http) status change interface	This document
AgentPresenceSubscribe	XACML	Access rights for presence subscription	This document
PolicyStore	XACML	Access rights for Policy Store interface	This document
DiscrepancyReport	XACML	Access rights for Discrepancy Report interface	This document
QueueState	XACML	Access rights for QueueState subscription	This document
DequeueRegistration	XACML	Access rights for DequeueRegistration interface	This document

[MM/DD/YYYY]

Page 425 of 675



Type	Format	Use	Reference
ESRPNotify	XACML	Access rights for ESRP Notify subscription	This document
AbandonedCall	XACML	Access rights for AbandonedCall subscription	This document
SpatialInterface	XACML	Access rights for Spatial Interface	This document
GapOverlap	XACML	Access rights for GapOverlap subscription	This document
MCS	XACML	Access rights for MCS interface	This document
GCS	XACML	Access rights for GCS interface	This document
ConferenceEvent	XACML	Access rights for ConferenceEvent subscription	This document
LoggingService	XACML	Access rights for Logging Service interface	This document
LoggingSIPREC	XACML	Access rights for Logging Service SIPREC interface	This document
ServiceAgencyLocatorDereference	XACML	Access rights for S/A L dereference interface	This document
ServiceAgencyLocatorNameSearch	XACML	Access rights for S/A L name search interface	This document
ServiceAgencyLocatorIndex	XACML	Access rights for S/A L Locator Index interface	This document
MapDatabase	XACML	Access rights for Map Database interface	This document

11339

11340 **10.34 “Discrepancy Report Status Token” Registry**

11341 IANA is requested to add the following entries to the DiscrepancyReportStatusToken registry:

Token	Name	DiscrepancyReports	Reference
AbleDelete	Problem	PermissionsDiscrepancyReport	This document
AbleRead	Problem	PermissionsDiscrepancyReport	This document
AbleSubscribe	Problem	PermissionsDiscrepancyReport	This document
AbleWrite	Problem	PermissionsDiscrepancyReport	This document

[MM/DD/YYYY]

Page 426 of 675



Token	Name	DiscrepancyReports	Reference
AddressRange	Problem	GISDiscrepancyReport	This document
BadAdditionalData	Problem	OriginatingServiceDiscrepancyReport	This document
BadCDR	Problem	BCFDiscrepancyReport	This document
BadCertificateChain	Problem	PermissionsDiscrepancyReport	This document
BadGeometry	Problem	GISDiscrepancyReport	This document
BadPIDFLO	Problem	LISDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
BadSDP	Problem	BCFDiscrepancyReport	This document
BadSIP	Problem	OriginatingServiceDiscrepancyReport	This document
BelievedInvalid	Problem	LoSTDiscrepancyReport	This document
BelievedValid	Problem	LoSTDiscrepancyReport	This document
CallDropped	Problem	OriginatingServiceDiscrepancyReport	This document
CallDrought	Problem	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
CallFlood	Problem	OriginatingServiceDiscrepancyReport	This document
CallReceived	Problem	ESRPDiscrepancyReport	This document
CallTakerAdvised	Validation Response	CallTakerDiscrepancyResponse	This document
CallTransferIncorrect	Problem	IMRDiscrepancyReport	This document
ConflictingRoute	Problem	PolicyDiscrepancyReport	This document
Critical	Severity	DiscrepancyReportRequest	This document
DataCorrected	Validation Response	GISDiscrepancyResponse	This document
DataExpired	Problem	LoSTDiscrepancyReport	This document
Degraded	Severity	DiscrepancyReportRequest	This document
DeviceConfigError	Validation Response	LISDiscrepancyResponse	This document
DiscrepancyCorrected	Validation Response	LoSTDiscrepancyResponse, BCFDiscrepancyReport, LoggingDiscrepancyResponse, SIPDiscrepancyResponse, PermissionsDiscrepancyResponse	This document
DiscrepancyNotFound	Validation Response	LoSTDiscrepancyResponse, BCFDiscrepancyReport	This document
DisplayData	Problem	GISDiscrepancyReport	This document
DuplicateAttribute	Problem	GISDiscrepancyReport	This document

[MM/DD/YYYY]

Page 427 of 675



Token	Name	DiscrepancyReports	Reference
EngorgedQ	Problem	ESRPDiscrepancyReport, IMRDiscrepancyReport, SIPDiscrepancyReport	This document
EntryAdded	Validation Response	LoSTDiscrepancyResponse	This document
ExcessiveSilence	Problem	IMRDiscrepancyReport	This document
FALSE	LocationCorrect	OriginatingServiceDiscrepancyReport	This document
findService	Query	LoSTDiscrepancyReport	This document
Firewall	Problem	BCFDiscrepancyReport	This document
Gap	Problem	GISDiscrepancyReport	This document
GeneralProvisioning	Problem	GISDiscrepancyReport	This document
getServiceBoundary	Query	LoSTDiscrepancyReport	This document
GIS	Validation Response	ESRPDiscrepancyResponse	This document
Impaired	Severity	DiscrepancyReportRequest	This document
IncorrectDataType	Problem	GISDiscrepancyReport	This document
IncorrectDHCP	Problem	NetworkDiscrepancyReport	This document
IncorrectDNS	Problem	NetworkDiscrepancyReport	This document
IncorrectLocation	Problem	LISDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
IncorrectLoST	Problem	GISDiscrepancyReport	This document
IncorrectRecords	Problem	LISDiscrepancyReport	This document
IncorrectURI	Problem	LoSTDiscrepancyReport	This document
IncorrectURN	Problem	PolicyDiscrepancyReport	This document
InitialINVITE	Problem	PSAPDiscrepancyReport	This document
InitialTrafficBlocked	Problem	BCFDiscrepancyReport	This document
InputFailed	Problem	IMRDiscrepancyReport	This document
InsufficientCredentials	Validation Response	PolicyStoreDiscrepancyResponse	This document
InvalidADR	Problem	OriginatingServiceDiscrepancyReport	This document
InvalidRecord	Validation Response	OriginatingServiceDiscrepancyResponse	This document
InvalidURN	Problem	PolicyDiscrepancyReport	This document
InviteSRSError	Problem	LoggingDiscrepancyReport	This document
listServices	Query	LoSTDiscrepancyReport	This document
listServicesByLocation	Query	LoSTDiscrepancyReport	This document

[MM/DD/YYYY]

Page 428 of 675



Token	Name	DiscrepancyReports	Reference
LocationErrorInError	Problem	LoSTDiscrepancyReport	This document
LocationMissing	Problem	OriginatingServiceDiscrepancyReport	This document
LocationNotLVFValid	Problem	OriginatingServiceDiscrepancyReport	This document
LocationNotUsable	Problem	OriginatingServiceDiscrepancyReport	This document
LocationReferenceNotResolved	Problem	LISDiscrepancyReport	This document
LogEventError	Problem	LoggingDiscrepancyReport	This document
Loop	Problem	PolicyDiscrepancyReport	This document
Malformed	Problem	ADRDiscrepancyReport PolicyDiscrepancyReport	This document
MalformedURI	Problem	GISDiscrepancyReport	This document
MediaLoss	Problem	BCFDiscrepancyReport	This document
MediaProblem	Problem	SIPDiscrepancyReport	This document
MESSAGE	Problem	SIPDiscrepancyReport	This document
MidDialog	Problem	SIPDiscrepancyReport	This document
MidTrafficBlocked	Problem	BCFDiscrepancyReport	This document
Minor	Severity	DiscrepancyReportRequest	This document
Moderate	Severity	DiscrepancyReportRequest	This document
MSAGtoPIDFLO	ServiceCal I	MCSDiscrepancyReport	This document
MultipleMappings	Problem	LoSTDiscrepancyReport	This document
NoANI	Problem	OriginatingServiceDiscrepancyReport	This document

[MM/DD/YYYY]

Page 429 of 675



Token	Name	DiscrepancyReports	Reference
NoDiscrepancy	Validation Response	ADRDiscrepancyResponse, BCFDiscrepancyResponse, CallTakerDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, GISDiscrepancyResponse, IMRDiscrepancyResponse, LISDiscrepancyResponse, LoggingDiscrepancyResponse, PSAPDiscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse, PermissionsDiscrepancyResponse, PolicyDiscrepancyResponse, PolicyStoreDiscrepancyResponse, SIPDiscrepancyResponse	This document
NoError	Validation Response	PolicyDiscrepancyResponse	This document
NoSuchLocation	Validation Response	LoSTDiscrepancyResponse	This document
NoSuchPolicy	Validation Response	PolicyStoreDiscrepancyResponse	This document
OmittedField	Problem	GISDiscrepancyReport	This document
OPTIONS	Problem	SIPDiscrepancyReport	This document
OtherADR	Problem	ADRDiscrepancyReport	This document
OtherBCF	Problem	BCFDiscrepancyReport	This document
OtherConflict	Problem	PolicyDiscrepancyReport	This document
OtherGIS	Problem	GISDiscrepancyReport	This document
OtherIMR	Problem	IMRDiscrepancyReport	This document
OtherLIS	Problem	LISDiscrepancyReport	This document
OtherLogging	Problem	LoggingDiscrepancyReport	This document
OtherLost	Problem	LoSTDiscrepancyReport	This document
OtherOSP	Problem	OriginatingServiceDiscrepancyReport	This document
OtherPermissions	Problem	PermissionsDiscrepancyReport	This document

[MM/DD/YYYY]

Page 430 of 675



Token	Name	DiscrepancyReports	Reference
OtherResponse	Validation Response	ADRDiscrepancyResponse, BCFDiscrepancyReport, CallTakerDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, GISDiscrepancyResponse, IMRDiscrepancyResponse, LISDiscrepancyResponse, LoggingDiscrepancyResponse, LoSTDIscrepancyReport, LoSTDIscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse, PermissionsDiscrepancyResponse, PolicyDiscrepancyResponse, PolicyStoreDiscrepancyResponse, SIPDiscrepancyResponse	This document
OtherLVF	Problem	LoSTDIscrepancyReport	This document
OtherNetwork	Problem	NetworkDiscrepancyReport	This document
OtherPolicy	Problem	PolicyDiscrepancyReport	This document
Overlap	Problem	GISDiscrepancyReport	This document
OwnLocationUnavailable	Problem	LISDiscrepancyReport	This document
PacketLatency	Problem	NetworkDiscrepancyReport	This document
PacketLoss	Problem	NetworkDiscrepancyReport	This document
PermissionsCorrected	Validation Response	LISDiscrepancyResponse	This document
PerPolicy	Validation Response	BCFDiscrepancyReport, ESRPDiscrepancyResponse, LISDiscrepancyResponse, PermissionsDiscrepancyResponse	This document
PIDFLOtoMSAG	ServiceCall	MCSDiscrepancyReport	This document
Policy	Validation Response	ESRPDiscrepancyResponse	This document

[MM/DD/YYYY]

Page 431 of 675



Token	Name	DiscrepancyReports	Reference
PolicyAdded	Validation Response	PolicyStoreDiscrepancyResponse	This document
PolicyAltered	Problem	PolicyStoreDiscrepancyReport	This document
PolicyCorrected	Validation Response	PolicyDiscrepancyResponse	This document
PolicyInvalid	Problem	PolicyStoreDiscrepancyReport	This document
PolicyMissing	Problem	PolicyStoreDiscrepancyReport	This document
PolicyUpdated	Validation Response	PolicyStoreDiscrepancyResponse	This document
ProblemCorrected	Validation Response	ADRDiscrepancyResponse, CallTransferDiscrepancyResponse, ESRPDiscrepancyResponse, IMRDiscrepancyResponse, MCSDiscrepancyResponse, NetworkDiscrepancyResponse, OriginatingServiceDiscrepancyResponse	This document
QoS	Problem	BCFDiscrepancyReport	This document
QueryTimeOut	Problem	OriginatingServiceDiscrepancyReport	This document
ReceivedIncorrectData	Problem	ADRDiscrepancyReport	This document
RecordsCorrected	Validation Response	LISDiscrepancyResponse	This document
ReferenceNotResolved	Problem	ADRDiscrepancyReport	This document
RequiredMedia	Problem	PSAPDiscrepancyReport	This document
ResponseConfusing	Problem	IMRDiscrepancyReport	This document
ResponseIncorrect	Problem	IMRDiscrepancyReport	This document
RetrieveLogEventError	Problem	LoggingDiscrepancyReport	This document
RouteIncorrect	Problem	LoSTDiscrepancyReport	This document
Routing	Problem	NetworkDiscrepancyReport	This document
ScriptLogicFailure	Problem	IMRDiscrepancyReport	This document
ServiceBoundaryIncorrect	Problem	LoSTDiscrepancyReport	This document
ServiceNumberIncorrect	Problem	LoSTDiscrepancyReport	This document
Severe	Severity	DiscrepancyReportRequest	This document
Signaling	Problem	SIPDiscrepancyReport	This document

Token	Name	DiscrepancyReports	Reference
SignatureVerificationFailure	Problem	PolicyStoreDiscrepancyReport	This document
STIerror	Problem	OriginatingServiceDiscrepancyReport	This document
TimeoutDHCP	Problem	NetworkDiscrepancyReport	This document
TimeoutDNS	Problem	NetworkDiscrepancyReport	This document
TooManyURIs	Problem	ADRDiscrepancyReport	This document
TrafficNotBlocked	Problem	BCFDiscrepancyReport	This document
TrafficNotBlockedBadActor	Problem	BCFDiscrepancyReport	This document
TransferCorrect	Validation Response	CallTakerDiscrepancyResponse	This document
TRUE	LocationCorrect	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
TTY	Problem	BCFDiscrepancyReport	This document
UnableAuthenticate	Problem	PermissionsDiscrepancyReport	This document
UnableDelete	Problem	PermissionsDiscrepancyReport	This document
UnableRead	Problem	PermissionsDiscrepancyReport	This document
UnableSubscribe	Problem	PermissionsDiscrepancyReport	This document
UnableWrite	Problem	PermissionsDiscrepancyReport	This document
Unknown	LocationCorrect	ESRPDiscrepancyReport, OriginatingServiceDiscrepancyReport	This document
UnknownBlock	Problem	ADRDiscrepancyReport	This document
UnknownPSAP	Problem	PolicyDiscrepancyReport	This document
UnknownScript	Problem	IMRDiscrepancyReport	This document
VerificationFailure	Problem	PolicyDiscrepancyReport	This document

11343

10.35 “Event Package” Registry

IANA is requested to add the following entries to the Event Package registry:

Name	Reference
ElementState	This document
ServiceState	This document
QueueState	This document
ESRPNotify	This document
AbandonedCall	This document
GapOverlap	This document

[MM/DD/YYYY]

Page 433 of 675



11346

10.36 "Agent States" Registry

11348 IANA is requested to add the following entries to the AgentStates registry:

State	Description	Reference
LoggedOut	Not currently logged in to the queue	This document
Break	Not at the console and unavailable to take a call	This document
Waiting	Not engaged	This document
Active	On a call	This document
Hold	On a call, have the call on hold	This document
Reserved	Temporarily alertyed to receive a specific call, not ready to take another. Will transition to Active when call is answered.	This document

11 Impacts, Considerations, Abbreviations, Terms, and Definitions

11.1 Operations Impacts Summary

11351 This standard will have a profound impact on the operation of 9-1-1 services and PSAPs.
11352 New data formats, more rigid data structure requirements, new functions, new databases,
11353 new call sources, new media types, new security challenges, and more, will impact the
11354 operation of 9-1-1 systems, PSAPs, their contractors, and access and originating networks.

11355 Nevertheless, the basic function, and the fundamental processes used to process calls, will
11356 not change substantially. NENA Committees are working diligently to provide appropriate
11357 procedures to match this specification.

11.2 Technical Impacts Summary

11359 This standard supports end-to-end IP connectivity; gateways are used to accommodate
11360 legacy wireline and wireless originating networks that are non-IP as well as legacy Public
11361 Safety Answering Points (PSAPs) that interconnect to the i3 solution architecture, as
11362 described herein. NENA i3 introduces the concept of an Emergency Services IP network
11363 (ESInet), which is designed as an IP-based inter-network (network of networks) that can
11364 be shared by all public safety agencies that may be involved in any emergency, and a set
11365 of core services that process 9-1-1 calls on that network (NGCS – NG9-1-1 Core Services).
11366 The i3 Public Safety Answering Point (PSAP) is capable of receiving IP-based signaling and
11367 media for delivery of emergency calls conformant to the i3 standard.

11368 Getting to the i3 solution from the current E9-1-1 infrastructure implies a transition from
11369 existing legacy originating network and 9-1-1 PSAP interconnections to next generation

[MM/DD/YYYY]

Page 434 of 675



interconnections. This document describes how NG9-1-1 works after transition, including ongoing interworking requirements for IP-based and TDM-based PSAPs and originating networks. It does not provide solutions for how PSAPs, originating networks, SRs, and ALI systems evolve. Rather, it describes the end point at which conversion is complete. At that point, SRs and existing ALI systems are decommissioned and all 9-1-1 calls are routed by the Emergency Call Routing Function (ECRF) and arrive at the ESInet/NGCS via SIP. This document supports both IP-based and legacy TDM-based systems.

TDM-based PSAPs are connected to the ESInet/NGCS via a gateway (the Legacy PSAP Gateway). The definition of the Legacy PSAP Gateway is broad enough so this type of gateway may serve both primary and secondary PSAPs that have not been upgraded.

Similarly, the scope includes gateways for legacy wireline and wireless originating networks (the Legacy Network Gateway) used by originating networks which cannot yet create call signaling matching the interfaces described in this document for the ESInet. It is not envisioned that legacy originating networks will evolve to IP interconnect in all cases, and thus the Legacy Network Gateways will be needed for the foreseeable future. This document considers all wireline, wireless, and other types of networks with IP interfaces, including IMS [49] networks, although the document only describes the external interfaces to the ESInet/NGCS, which a conforming network must support. This document describes a common interface to the ESInet/NGCS, to be used by all types of originating networks or devices. How originating networks, or devices within them, conform is not visible to the ESInet/NGCS and is out of scope. The interface conforms to the best practice described in IETF RFC 6881 [46]. ATIS 0700015 [151], which is based on 3GPP TS 24.229 [226] and TS 23.167 [49], describes how IMS originating networks deliver calls to the ESInet NGCS as defined in this document.

11.3 Security Impacts Summary

This document introduces many new security mechanisms that will impact network and PSAP operations. The most significant changes to current practices are:

- All transactions must be protected with authentication, authorization, integrity protection, and privacy mechanisms specified by this document;
- Common authentication (single sign-on) and common rights management/authorization functions are used for ALL elements in the network;
- Of necessity, PSAPs will be connected, indirectly through the ESInet, to the global Internet to accept calls. This means that PSAPs will likely experience deliberate attacks on their systems. The types of vulnerabilities that NG9-1-1 systems must manage and protect against will fundamentally change and will require constant vigilance to create a secure and reliable operating environment. NG9-1-1 systems must have robust detection and mitigation mechanisms to deal with such attacks.

11407 **11.4 Recommendation for Additional Development Work**

11408 This is the second revision of this document. There are several sections in which it is noted
11409 that further work is needed, and future revisions will cover topics in more depth. The
11410 authoring committee chose to describe future work within the document, rather than
11411 maintain a separate document with future work. Where this version states that future work
11412 is needed, vendors may need to implement the function in a way that may not yet be
11413 interoperable with other implementations, and when the work is complete (in a future
11414 version of this document), changes in such implementations may be necessary. The
11415 following table lists sections in this document that refer to possible future work.

Section	Reference to future work
<various>	There are several references to "near real-time" in this document. Definitions, maximums, and/or implementation guidance is necessary for each instance of the term
2.5	An equivalent definition for Canadian addresses will be referenced in a future version of this document.
2.7	The effect on emergency calls already in progress when mitigation is enabled will be addressed in a future version of this document.
2.11	A future version of this document will standardize SNMP MIBs for each FE.
3.1.10	There is considerable flux in standardized Instant Messaging protocols. It is anticipated that there may be additional IM protocols supported by NG9-1-1 in the future, specifically XMPP. If such protocols are adopted, a future version of this document will describe the ESInet interface.
3.6	A standard NENA schema for WFS as used in the i3 SI layer replication protocol will be provided in a future version of this document.
3.7.14	A Discrepancy Report by an OSP toward the OCIF reporting an identity verification failure for a call from the OCIF will be addressed in a future edition of this document.
4.2.1.6	A future version of this document will describe how to include the condition values that triggered the notify in the body of the NOTIFY.
4.2.2.5	Using the latest data may be problematic in some situations. Making the rules for merging objects more explicit would limit cases of conflicting information. This will be covered in a future version of this document.

[MM/DD/YYYY]

Page 436 of 675



Section	Reference to future work
4.2.3	Specific policy document structures will be specified for each of the policy instances defined for the ESRP in a future version of this document.
4.3.3.4	Service to access Additional Data for a location: Additional Data is associated with a site/structure. This will be addressed in a future version of this document.
4.6.1	Handling of media other than voice-only callbacks is incompletely specified and will be addressed in a future version of this document.
4.7.6	An ad hoc transfer call flow involving MSRP may be provided in a future version of this document.
4.8.1	Work is currently ongoing in the Internet Engineering Task Force (IETF) to define RTT mixing and a future version of this document will specify appropriate standards.
4.11.1	A privacy issue was identified associated with this mechanism. Since it will require substantive changes, this will be addressed in a future version of this document.
4.13.3	A future version of this document will describe how policies can restrict retrieval by more fine-grained criteria, for example allowing only agencies participating in a multi-agency incident to retrieve LogEvents about that incident.
4.12.3.7	In the EventTypes described below, there is a very large amount of logging including cases in which information is logged at both the sender and receiver. Future versions of this document will describe a way to control what must be logged, whether digital signatures will be deployed, and their mechanism for deployment.
4.12.3.7	A description of which elements generate which LogEvent types will be described in a future version of this document.
4.12.3.7	Mechanisms to support blind and supervised transfer are not defined in this document and will be standardized in a future version of this document. Logging of such transfers is still required.
4.15.3	A future version of this document will specify a more general way to connect the Service/Agency Locator Search Services.
4.21	The use of the CVT FE in the processing of 9-1-1 calls is for future study.

Section	Reference to future work
4.21	The concept of Secure Telephone Identity is nascent. As such, it is expected that the referenced standards will evolve. A future version of this document will ensure alignment with the evolution of these standards, when appropriate.
4.22	A detailed description of IDX functionality/interfaces will be part of a future version of this document
5.2	The PCA CP/CPS MUST be in conformance with minimum standards to be provided in a future version of this document.
5.3	Specific definitions of the roles enumerated in this section will be defined in an informational document (NENA-INF) to be referenced in a future version of this document.
5.6	Occasionally data becomes orphaned and must come under new ownership to provide updates. A mechanism to re-home orphaned data will be provided in a future version of this document.
7	Specification for the conveyance of EIDOs between agencies, systems, and applications will appear in a future version of this document.
9	PSAP Management interface will be provided in a future version of this document.
Appendix A	A future version of this document will further clarify how conversion between legacy formats and NG9-1-1 formats is accomplished.

11416 **11.5 Anticipated Timeline**

11417 As this is a major change to the 9-1-1 system, adoption of this standard will take several
11418 years and is also dependent on the pace of change and evolution of originating network
11419 providers, access network providers, and PSAPs. Experience with the immediately prior
11420 major change to 9-1-1 (i.e., Phase II wireless) suggests that unless consensus among
11421 government agencies at the local, state, and federal levels, as well as network operators,
11422 vendors, and other service providers is reached, implementation for the majority of PSAPs
11423 could take a decade. The i3 Architecture Working Group chose technology commensurate
11424 with a 2- to 5-year implementation schedule.

11425 **11.6 Cost Factors**

11426 This is an all-new 9-1-1 system; the cost of everything will change. At this time, it is
11427 difficult to predict the costs of the system and more work will be needed by vendors and
11428 service providers to determine the impact of the changes on their products and operations.
11429 If implemented at a regional (multi-county) or state level, the cost of the new system may

[MM/DD/YYYY]

Page 438 of 675



11430 be significantly less, although in the transition from the existing system to the new one,
11431 duplicate elements and services may have to be maintained at a higher overall cost. The
11432 case may also be that costs are not reduced, but the improved service to the public
11433 justifies these costs. Note that the charge to the i3 Architecture Working Group was to NOT
11434 make costs a primary consideration in making technical decisions. Nevertheless, due to the
11435 pragmatic experience of the participants, the document tended to consider cost as one of
11436 the variables in making choices. Estimating the cost to deploy the entire NG9-1-1 system is
11437 the purview of other groups within and outside NENA.

11438 **11.7 Cost Recovery Considerations**

11439 Traditionally, much of the cost of the existing E9-1-1 Service Provider infrastructure has
11440 been supported through the collection of fees and surcharges on wireline and wireless
11441 telephone service. Changes in the telecommunications industry have caused the basis upon
11442 which the fees and surcharges are collected to be modified, and the architecture described
11443 in this document further sunders the assumptions on which the current revenue streams
11444 are based. It should be noted that the costs associated with operating the 9-1-1
11445 environment envisioned within this document are no longer accurately predicted by the
11446 number of originating network subscribers residing in a given service area. This document
11447 does not make recommendations on how funding should be changed. See the NG Partner
11448 Program Funding Policy paper [105] for more on this subject.

11449 **11.8 Additional Impacts (non-cost related)**

11450 This effort is a part of the overall Next Generation 9-1-1 project. There are far-reaching
11451 impacts to the entire 9-1-1 system and public safety policies engendered by the changes in
11452 networks, databases, devices, interfaces, and mechanisms this document describes. See
11453 the NG Partner Program Policy Guidelines documents for more on these areas [106]. It is
11454 expected that originating networks will ultimately evolve, but i3 assumes this evolution to
11455 take place over time and in stages by use of supporting gateways to allow existing
11456 interfaces from originating networks to be supported until such time as the originating
11457 network provider is ready to migrate to IP. Nearly all systems in a PSAP must (eventually)
11458 evolve. All databases change, some are eliminated, some new ones created, others are
11459 modified. New relationships between agencies must be established, for example, to
11460 facilitate answering of calls out of area.

11461 Some of the more significant impacts are the methods and procedures to migrate the
11462 current 9-1-1 system to Next Generation 9-1-1. The NG9-1-1 Transition Planning
11463 Committee is developing documents that describe the transition. This document only
11464 describes external interfaces to a PSAP. The internal PSAP subsystems and the

11465 interconnection between those subsystems must change. This is the responsibility of the
11466 NENA NG9-1-1 PSAP Systems Working Group.

11467 **11.9 Abbreviations, Terms, and Definitions**

11468 See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing
11469 of terms used in NENA documents. All abbreviations used in this document are listed
11470 below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/ Upd ate (U)
3GPP (3 RD Generation Partner Project)	A collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners".	
3GPP2 (3 rd Generation Partnership Project 2)	A collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radio telecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. A sister project to 3GPP.	
AACN (Advanced Automatic Crash Notification)	An emergency call placed by a vehicle, initiated either automatically or manually, conveying telematics data. Also called a "telematics call".	A
ACK (Acknowledgement)	A message to indicate the receipt of data.	
ACM (Address Complete Message)	An ISDN (Integrated Services Digital Network) User Part (ISUP) message returned from the terminating switch when the subscriber is reached and the phone starts ringing, or when the call traverses an interworking point and the intermediate trunk is seized.	
Additional Data	Further information intended to be useful to a call taker or responder (e.g., about how the call was placed, the person(s) associated with the device placing the call, the location of the call, vehicle sensor data, medical device data, etc.)	

[MM/DD/YYYY]

Page 440 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
ADR (Additional Data Repository)	A data retrieval facility for Additional Data. The ADR dereferences a URI passed in a Call-Info header field or PIDF-LO <provided-by> and returns an Additional Data object block. An Identity-Searchable Additional Data Repository (IS-ADR) returns Additional Data associated with an identity.	U
AES (Advanced Encryption Standard)	A Federal Information Processing Standard (FIPS)-approved cryptographic algorithm that is used to protect electronic data.	
Agency	In NG9-1-1, an organization that is connected directly or indirectly to the ESInet. Public safety agencies are examples of Agency. An entity such as a company that provides a service in the ESInet can be an Agency. Agencies have identifiers and credentials that allow them access to services and data.	
Agent	In NG9-1-1, an Agent is an authorized person – employee, contractor, or volunteer – who has one or more roles in an Agency. An Agent can also be an automaton in some circumstances (e.g., an IMR answering a call).	
AIP (Access Infrastructure Provider)	The entity providing physical communications access to the subscriber. This access may be provided over telco wire, CATV cable, wireless, or other media. Usually, this term is applied to purveyors of broadband internet access but is not exclusive to them.	
ALRS (Agency Locator Record Store)	A web service that, when presented with an agency locator URI, returns the agency locator record.	
AMR (Adaptive Multi-Rate (codec))	An audio compression format optimized for speech coding that automatically changes coding rates in response to the input audio stream. Refer to RFC 4867 .	
AMR-WB (Adaptive Multi Rate (codec) – Wide Band)	An audio compression format optimized for wideband speech coding that automatically changes coding rates in response to the input audio stream. Refer to RFC 4867 .	
ANI (Automatic Number Identification)	Telephone number associated with the access line from which a call originates.	

[MM/DD/YYYY]

Page 441 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
ANSI (American National Standards Institute)	Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. www.ansi.org	
APCO (Association of Public Safety Communications Officials)	APCO is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications. http://www.apcointl.org/	
ATIS (Alliance for Telecommunications Industry Solutions)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operational standards for the communications and related information technologies industry worldwide using a pragmatic, flexible, and open approach. www.atis.org	
Authoritative	Definitive, master. Information has an authoritative source, normally the owner of the information or its designee. There is only one authoritative source. A specific element or service may be authoritative for a given implementation or jurisdiction.	A
B2BUA (Back-to-Back User Agent)	A SIP element that relays signaling mechanisms while performing some alteration or modification of the messages that would otherwise not be permitted by a proxy server. A logical entity that receives a request and processes it as a UAS (User Agent Server). In order to determine how the request should be answered, it acts as a UAC (User Agent Client) and generates requests. Unlike a proxy server it maintains dialog state and must participate in all requests sent on the dialogs it established.	
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.	

[MM/DD/YYYY]

Page 442 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
BISACS (Building Information Services And Control System)	A computer-based system that allows access to building information such as its structural layout and/or to monitor a particular building or set of buildings for alerts.	
CAMA (Centralized Automatic Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.	
CAP (Common Alerting Protocol)	A general format for exchanging emergency alerts, primarily designed as an interoperability standard for use among warning systems and other emergency information systems. Refer to http://docs.oasis-open.org/emergency/cap/	
CDR (Call Detail Record)	A record stored in a database recording the details of a received or transmitted call (from NENA-STA-010). The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, etc)	
cid (Content Identifier [Content-ID])	A unique identifier assigned to a body part that allows the body part to be referenced in a SIP header field.	U
codec (COder/DECoder)	A standardized means for encoding and decoding media, especially audio and video.	
CoS (Class of Service)	A designation in E9-1-1 that defines the service category of the telephony service. Examples are residential, business, Centrex, coin, PBX, VoIP, and wireless Phase II (WPH2).	
CPE (Customer Premises Equipment)	Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP.	
CSRC (Contributing Source)	As specified in RFC 3550, a source of a stream of RTP packets that has contributed to the combined stream produced by an RTP mixer.	
Dereference	The act of exchanging a reference to an item by its value. For example, the dereference operation for location uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).	A

[MM/DD/YYYY]

Page 443 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
DES (Data Encryption Standard)	The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, (i.e., one for encryption and one for decryption).	A
DHCP (Dynamic Host Control Protocol (i2); Dynamic Host Configuration Protocol)	A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address.	
DNS (Domain Name Server)	Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates those names into routable IP addresses.	
DNS (Domain Name System)	A globally distributed database for the resolution of host names to numeric IP addresses.	
DoS (Denial of Service)	<p>A type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides.</p> <p>DDoS (Distributed Denial of Service Attack)</p> <p>A cyber-attack where the source is more than one, often thousands of, unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.</p> <p>TDoS (Telephone Denial of Service)</p> <p>Illegal attacks targeting the telephone network by generating numerous 9-1-1 phone calls, tying up the network and preventing an agency from receiving legitimate calls.</p>	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
DSCP (Differentiated Services Code Point)	A means of classifying and managing network traffic and of providing quality of service (QoS) in modern Layer 3 IP networks. It uses the 6-bit Differentiated Services (DS) field in the IP header for the purpose of packet classification.	A
DSig (Digital Signature)	The XML syntax used to associate the cryptographic signature value with Web resources using XML markup.	A
DSL (Digital Subscriber Line)	A "last mile" solution that uses existing telephony infrastructure to deliver high speed broadband access. DSL standards are administered by the DSL Forum http://dslforum.org/ .	
DTLS (Datagram Transport Layer Security)	A communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	A
E9-1-1 (Enhanced 9-1-1)	<p>A telephone system which includes network switching, database, and Public Safety Answering Point premise elements capable of providing automatic location identification data, selective routing, selective transfer, fixed transfer, and a call back number.</p> <p>The term also includes any enhanced 9-1-1 service so designated by the Federal Communications Commission in its Report and Order in WC Docket Nos. 04-36 and 05-196, or any successor proceeding.</p>	
ECRF (Emergency Call Routing Function)	<p>A functional element in an ESInet which is a LoST protocol server in which location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency.</p> <ul style="list-style-type: none"> • External ECRF: An ECRF instance that resides outside of an ESInet instance. • Internal ECRF: An ECRF instance that resides within and is only accessible from an ESInet instance. 	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
E-CSCF (Emergency Call Session Control Function)	The entity in the IMS core network that handles certain aspects of emergency sessions, e.g. routing of emergency requests to the correct emergency center or PSAP.	
EDXL (Emergency Data eXchange Language)	A broad initiative to create an integrated framework for a wide range of emergency data exchange standards to support operations, logistics, planning, and finance.	
EIDD (Emergency Incident Data Document)	A National Information Exchange Model (NIEM) conformant object that is used to share emergency incident information between and among authorized entities and systems.	
EIDO (Emergency Incident Data Object)	A JSON-based object that is used to share emergency incident information between and among authorized entities and systems. NENA has adopted the JSON-based EIDO (Emergency Incident Data Object) for sharing incident information among authorized NG9-1-1 entities and systems.	A
ESInet (Emergency Services IP Network)	A managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national, and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.	
ESN (Emergency Service Number)	A 3-5 digit number that represents one or more ESZs. An ESN is defined as one of two types: Administrative ESN and Routing ESN.	
ESRK (Emergency Services Routing Key)	A 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
ESRP (Emergency Service Routing Proxy)	<p>An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them.</p> <ul style="list-style-type: none"> • Originating ESRP: The first routing element within the Next Generation Core Services (NGCS). It receives calls from the BCF at the edge of the ESInet. • Terminating ESRP: The last ESRP for a call in NGCS. 	
EVRC (Enhanced Variable Rate Codec) Narrowband	A speech codec developed to offer mobile carriers more network capacity while not increasing bandwidth requirements.	
EVRC-WB (Enhanced Variable Rate Wideband Codec)	A speech codec providing enhanced (wideband) voice quality.	
FAC (Facility [SS7 message])	A message sent in either direction at any phase of the call to request an action at another exchange.	
FCC (Federal Communications Commission)	An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.	
FCI (Feature Code Indicator)	Information sent in either direction to invoke a specific feature operation at the terminating or originating switch	
FE (Functional Element) AKA: Functional Entity	A set of software features that may be combined with hardware interfaces and operations on those interfaces to accomplish a defined task.	U
FQDN (Fully Qualified Domain Name)	The complete domain name for a specific computer, or host, on the Internet.	
g.711 a-law	An ITU-T Recommendation for an audio codec for telephony in non-North American regions.	
g.711 mu-law	An ITU-T Recommendation for an audio codec for telephony in the North American region.	

[MM/DD/YYYY]

Page 447 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
GCS (Geocode Service)	An NG9-1-1 service providing geocoding and reverse-geocoding.	
GDP (Generic Digits Parameter)	Identifies the type of address to be presented in calls set up or additional numeric data relevant to supplementary services such as LNP or E9-1-1.	
geopriv (Geographic Location/Privacy)	The name of an IETF work group, now dormant, which created location representation formats such as PIDF-LO and protocols for transporting them, such as HELD used in NG9-1-1. See https://datatracker.ietf.org/wg/geopriv/charter/	
GeoRSS (Geodetic Really Simple Syndication)	A simple mechanism used to encode GML in RSS feeds for use with the ATOM protocol.	
geoShape element (Geodetic Shape)	One of a list of shapes defined originally by the IETF and standardized by the Open Geospatial Consortium that can be found in a PIDF-LO. Includes point, circle, ellipse, arc band, polygon, and 3-D versions of same.	
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing, and managing data and associated attributes which are spatially referenced.	
GML (Geography Markup Language)	An XML grammar for expressing geographical features standardized by the OGC.	
GRUU (Globally Routable User agent URI)	A SIP URI which identifies a specific endpoint at which a user is signed on that is routable on the Internet.	
H.264/MPEG-4	An ITU-T Recommendation and Motion Picture Expert Group standard for a video codec	
HELD (HTTP-Enabled Location Delivery Protocol)	A protocol that can be used to acquire Location Information (LI) from a LIS within an access network as defined in IETF RFC 5985.	
HTTP (HyperText Transfer Protocol)	Typically used between a web client and a web server that transports HTML and/or XML.	U
HTTPS (HyperText Transfer Protocol Secure)	HTTP with secure transport (Transport Layer Security or its predecessor, Secure Sockets Layer)	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
i3	"i3" refers to the NG9-1-1 system architecture defined by NENA, which standardizes the structure and design of Functional Elements making up the set of software services, databases, network elements and interfaces needed to process multi-media emergency calls and data for NG9-1-1. (See NG9-1-1 Core Services (NGCS), ESInet and NG9-1-1.)	U
IAM (Initial Address Message)	The first message sent in a call set-up by a Switch or Exchange to other partner exchange. Refer to http://www.wapopia.com/techfaq/gsm-faq/what-is-initial-address-message-iam/	
IANA (Internet Assigned Numbers Authority)	The entity that oversees global IP address allocation; DNS root zone management, and other Internet protocol assignments. www.iana.org	
ICE (Interactive Connectivity Establishment)	A mechanism for endpoints to establish RTP connectivity in the presence of NATs and other middle-boxes.	
IDP (Identity Provider)	An entity which authenticates users and supplies services with a "token" that can be used in subsequent operations to refer to an authorized user.	
IDX (Incident Data eXchange)	A Functional Element that facilitates the exchange of Emergency Incident Data Objects (EIDOs) among other Functional Elements both within and external to an agency.	U
IETF (Internet Engineering Task Force)	Lead standard-setting authority for Internet protocols.	
IM (Instant Messaging)	A method of communication, generally using text, in which more than a character at a time is sent between parties nearly instantaneously.	
IMR (Interactive Media Response)	An automated service used to play announcements, record responses, and interact with callers using any or all of audio, video, and text.	U

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
IMS (Internet Protocol Multimedia Subsystem)	The IP Multimedia Subsystem comprising all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, and pictures, alone or in combination, delivered over a packet-switched domain.	U
Incident Tracking Identifier	An identifier assigned by the first element in the first ESInet that handles an emergency call or declares an incident. Incident Tracking Identifiers are globally unique.	
INVITE	A SIP transaction used to initiate a session (See re-INVITE).	
IP (Internet Protocol)	The method by which data is sent from one computer to another on the Internet or other networks.	
IPv4 (Internet Protocol version 4)	The fourth version of the Internet Protocol; uses 32-bit addresses.	
IPv6 (Internet Protocol version 6)	The most recent version of the Internet Protocol; uses 128-bit addresses.	
IS-ADR (Identity Searchable Additional Data Repository)	An Additional Data Repository providing a service that can search for Additional Data based on a sip/sips or tel URI: (e.g., Additional Data about the caller).	U
ISDN (Integrated Services Digital Network)	International standard for a public communication network to handle circuit-switched digital voice, circuit-switched data, and packet-switched data.	
ISP (Internet Service Provider)	A company that provides Internet access to other companies and individuals.	
ISUP (Integrated Services Digital Network User Part)	A message protocol to support call set up and release for interoffice voice call connections over SS7 Signaling.	
ITU (International Telecommunication Union)	The telecommunications agency of the United Nations established to provide worldwide standard communications practices and procedures. Formerly CCITT.	
KP (Key Pulse)	An MF signaling tone (digit).	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
LIF (Location Interwork Function)	The functional component of a Legacy Network Gateway which is responsible for taking the appropriate information from the incoming signaling (i.e., calling number/ANI, ESRK, cell site/sector) and using it to acquire location information that can be used to route the emergency call and to provide location information to the PSAP. In a Legacy PSAP Gateway, this functional component takes the information from an ALI query and uses it to obtain location from a LIS.	
LIS (Location Information Server)	A functional element that provides locations of endpoints. A LIS can provide Location-by-Reference, or Location-by-Value, and, if the latter, in geodetic or civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID, or MAC address, and returns the location (value or reference) associated with that identifier. The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value.	U
LNG (Legacy Network Gateway)	An NG9-1-1 Functional Element that provides an interface between a non-upgraded legacy originating network and a Next Generation Core Services (NGCS)-enabled network.	

[MM/DD/YYYY]

Page 451 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
LO (Location Object)	<p>In an emergency calling environment, the LO is used to refer to the current position of an endpoint that originates an emergency call. The LO is expected to be formatted as a Presence Information Data Format – Location Object (PIDF-LO) as defined by the IETF in RFC 4119, updated by RFCs 5139, 5491, and 7459, and extended by RFC 6848. The LO may be:</p> <ul style="list-style-type: none"> • Geodetic – shape, latitude(s), longitude(s), elevation, uncertainty, confidence and the datum which identifies the coordinate system used. NENA prescribes that geodetic location information will be formatted using the World Geodetic System 1984 (WGS 84) datum; • Civic location – a set of elements describing detailed street address information. For NG9-1-1 in the U.S., the civic LO must conform to the NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard (NENA-STA-004); • or a combination thereof. 	
LogEvent	A standardized JSON object containing information about a processing event that is stored in and retrieved from the Logging Service.	
LoST (Location to Service Translation) Protocol	A protocol that takes location information and a Service URN and returns a URI. Used generally for location-based call routing. In NG9-1-1, used as the protocol for the ECRF and LVF.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
LPG (Legacy PSAP Gateway)	A signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG9-1-1 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.	
LRF (Location Retrieval Function)	The IMS-associated functional entity that handles the retrieval of location information for the emergency caller including, when required, interim location information, initial location information, and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information for an emergency call.	
LSRG (Legacy Selective Router Gateway)	Provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1.	
LVF (Location Validation Function)	A functional element in an NGCS that is a LoST protocol server where civic location information is validated against the authoritative GIS database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call and adequate and specific enough to direct responders to the right location.	
MCS (MSAG Conversion Service)	A web service providing conversion between PIDF-LO and MSAG data.	
MDN (Mobile Directory Number)	The telephone number dialed to reach a wireless telephone.	
MDS (Mapping Data Service)	Provides a PSAP call taker with information showing the location of an out-of-area caller.	A

[MM/DD/YYYY]

Page 453 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks.	
MIB (Management Information Base)	An object used with the Simple Network Management Protocol to manage a specific device or function.	
MIME (Multipurpose Internet Mail Extensions)	A specification for formatting non-ASCII messages so that they can be sent over the Internet.	
MPC/GMLC (Mobile Positioning Center/Gateway Mobile Location Center)	A Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network. The MPC/GMLC retrieves, forwards, stores, and controls position data within the location services network. It interfaces with the location server (e.g. Position Determining Entity [PDE]) for initial and updated position determination. The MPC/GMLC restricts access to provide position information only while an emergency service call is active.	
MSAG (Master Street Address Guide)	A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.	
MSC (Mobile Switching Center)	The wireless equivalent of a Central Office, which provides switching functions for wireless calls.	U
MSRP (Message Session Relay Protocol)	A standardized mechanism for exchanging instant messages using SIP where a server relays messages between user agents.	
MTP (Message Transfer Part)	A layer of the SS7 protocol providing the routing and network interface capabilities to support call setup.	
NANP (North American Numbering Plan)	An integrated telephone numbering plan serving 20 North American countries that share telephone numbers in the +1 country code. www.nationalnanpa.com	
NAPT (Network Address and Port Translation)	A methodology of remapping one IP address and port into another by modifying network address information in Internet Protocol (IP) datagram packet header fields while they are in transit across a traffic routing device.	

[MM/DD/YYYY]

Page 454 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
NAT (Network Address Translation)	Maps a single public address to one or many internal addresses and all network IP addresses on the connected computers are local and cannot be seen by the outside world.	U
NENA (National Emergency Number Association)	<p>A not-for-profit corporation established in 1982 to further the goal of "One Nation-One Number." NENA is a networking source and promotes research, planning, and training. NENA strives to educate, set standards, and provide certification programs, legislative representation, and technical assistance for implementing and managing 9-1-1 systems.</p> <p>www.nena.org</p>	
NG9-1-1 (Next Generation 9-1-1)	<p>"Next Generation 9-1-1 services" means a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that</p> <ul style="list-style-type: none"> (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, text, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller; (E) supports data, video, and other communications needs for coordinated incident response and management; and (F) interoperates with services and networks used by first responders to facilitate emergency response. <p>REF: Agreed to by NENA, NASNA, iCERT, and the National 9-1-1 Office representatives on 01/12/2018.</p>	

[MM/DD/YYYY]

Page 455 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
NGCS (Next Generation 9-1-1 [NG9-1-1] Core Services)	The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network	U
NIF (NG9-1-1 Specific Interwork Function)	The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG9-1-1-specific processing of the call not provided by an off-the-shelf protocol interwork gateway.	
NPD (Numbering Plan Digit)	A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes.	
NRS (NENA Registry System)	The entity provided by NENA to manage registries. http://technet.nena.org/nrs/registry/_registries.xml	
NTP (Network Time Protocol)	A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.	
OASIS (Organization for the Advancement of Structured Information Standards)	An organization that promulgates standards for data interchange. www.oasis-open.org	
OGC (Open Geospatial Consortium)	A standards development organization that promulgates standards for the global geospatial community. http://www.opengeospatial.org/	
OLI (Originating Line Identification parameter)	A parameter that conveys class of service information about the originator of a call.	

[MM/DD/YYYY]

Page 456 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
OSI (Open Systems Interconnection)	<p>A 7-layer hierarchical reference model structure developed by the International Standards Organization for defining, specifying, and relating communications protocols; not a standard or a protocol.</p> <p>Layer Description</p> <ul style="list-style-type: none"> • (7) Application: Provides interface with network users • (6) Presentation: Performs format and code conversion • (5) Session: Manages connections for application programs • (4) Transport: Ensures end-to-end delivery • (3) Network: Handles network addressing and routing • (2) Data Link: Performs local addressing and error detection • (1) Physical: Includes physical signaling and interfaces 	U
P-A-I (P-Asserted-Identity)	A header field in a SIP message containing a URI that the originating network asserts is the correct identity of the caller.	A
PCA (PSAP Credentialing Agency)	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an i3-compliant infrastructure.	
P-DCS-OSPS (PacketCable-Distributed Call Signaling-Operator Services Position System)	The architecture designed to facilitate the exchange of trusted information between telephone service providers that conveys customer-specific information and expectations about the parties involved in the call.	
PHB (Per Hop Behaviors)	The action a router takes for a packet marked with a specific code point in the Diffserv QoS mechanism in IP networks.	
PIDF (Presence Information Data Format)	Specified in IETF RFC 3863; it provides a common presence data format for Presence protocols, and also defines a new media type. A presence protocol is a protocol for providing a presence service over the Internet or any IP network.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
PIDF-LO (Presence Information Data Format – Location Object)	Provides a flexible and versatile means to represent location information in a SIP header field using an XML schema.	
PIF (Protocol Interworking Function)	That functional component of a Legacy Network Gateway or Legacy PSAP Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling.	
PKI (Public Key Infrastructure)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.	
PRF (Policy Routing Function)	That functional component of an Emergency Service Routing Proxy that determines the next hop in the SIP signaling path using a policy.	
PSAP (Public Safety Answering Point)	<p>An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.</p> <ul style="list-style-type: none"> • Primary PSAP: A PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office. • Secondary PSAP: A PSAP to which 9-1-1 calls are transferred from a Primary PSAP. • Alternate PSAP: A PSAP designated to receive calls when the primary PSAP is unable to do so. • Consolidated PSAP: A facility where multiple Public Safety Agencies choose to operate as a single 9-1-1 entity. • Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 9-1-1 emergency calls. • Serving PSAP: The PSAP to which a call would normally be routed. • NG9-1-1 PSAP: This term is used to denote a PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA NENA-STA-010, and referred to therein as an "i3 PSAP". 	

[MM/DD/YYYY]

Page 458 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
PSP (Provisioning Service Provider)	The component in an ESInet functional element that implements the provider side of an SPML interface used for provisioning	
PSTN (Public Switched Telephone Network)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.	
QoS (Quality of Service)	As related to data transmission, a measurement of latency, packet loss, and jitter.	U
RDF (Routing Determination Function)	The IMS-associated functional entity, which may be integrated in a Location Server (e.g. GMLC) or in an LRF, and provides the proper outgoing address to the E-CSCF for routing the emergency request towards a PSAP. It can interact with a location functional entity (e.g., GMLC) to manage ESQK allocation and management and deliver location information to the PSAP.	
REFER/Replaces	Use of the SIP REFER method together with a Replaces header field as part of a transfer operation to indicate that a new leg is to be created that replaces an existing call leg.	
re-INVITE	A SIP INVITE transaction within an established session used to change the parameters of a call or refresh a session. See INVITE.	A
REL (Release) message	An ISUP message sent in either direction to release the circuit.	
Request-URI	That part of a SIP message that indicates where the call is being routed. SIP Proxy servers commonly change the Request ID ("retargeting") to route a call towards the intended recipient.	
Resource Priority	A header field used on SIP calls to indicate priority that proxy servers give to specific calls. The Resource Priority header field does not indicate that a call is an emergency call (see Request-URI).	U
REST (Representational State Transfer)	An interface that transmits domain-specific data over HTTP without an additional messaging layer such as SOAP or session tracking via HTTP cookies.	

[MM/DD/YYYY]

Page 459 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
RFC (Request for Comment)	A document published by the Internet Engineering Task Force (IETF). Note that the name is an historic artifact—An RFC is finalized. RFCs are never revised; updates are published as new RFCs. Errata are noted separately. (Documents for which input and comments are requested are called Internet Drafts. Most RFCs are originally published as an Internet Draft).	U
RLC (Release Complete)	An ISUP message sent to acknowledge the release (REL) message indicating that the circuit is idle afterward and can be used again.	
ROH (Receiver Off-Hook)	A call state in which the recipient's hand set is not in the cradle.	A
ROHC (Robust Header Compression)	A standardized method to compress the IP, UDP, UDP-Lite, RTP, and TCP headers of Internet packets.	
RTCP (Real-time Transport Control Protocol)	A sister protocol of RTP and provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP. It gathers statistics on a media connection and information such as bytes sent, packets sent, lost packets, jitter, feedback, and round trip delay. An application may use this information to increase the quality of service perhaps by limiting flow, or maybe using a low compression codec instead of a high compression codec. RTCP is used for Quality of Service (QoS) reporting.	
RTP (Real-time Protocol)	An IP protocol used to transport media (voice, video, text) which has a real-time constraint.	
RTSP (Real-time Streaming Protocol)	A network control protocol designed for use in entertainment and communications systems to control streaming media servers.	
RTT (Real-time Text)	Text transmission that is one character at a time, as in TTY.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
SAML (Security Assertion Markup Language)	An XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and another party.	
SAP (Service Activation Parameter)	A parameter included in an SS7 call control message to invoke an action at another node or report the result of such an action.	
SCTP (Stream Control Transport Protocol)	Defined by IETF RFC 4960 as the transport layer to carry signaling messages over IP networks. SCTP/T is just one of the many products in the Adax Protocol Software (APS) SIGTRAN suite that has been designed for Convergence, Wireless, and Intelligent Networks. Compliant with IETF RFC 4960 and RFC 3309, SCTP/T (SCTP for Telephony) is implemented in the OS kernel. SCTP/T provides a transport signaling framework for IP networks that enhances the speed and capability of SSCS/HSL and can be deployed over T1/E1, Ethernet, and ATM OC3 physical media interfaces. In addition to the services specified in IETF RFC 4960, Adax SCTP/T also provides a transport framework with levels of service quality and reliability as those expected from a Public Switched Telephone Network (PSTN).	
SDO (Standards Development Organization)	An entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization.	
SDP (Session Description Protocol)	A standard syntax contained in a signaling message to negotiate a real-time media session. See RFC 4566.	
Security Posture	An event, part of Service State, which represents a downstream entity's current security state (Green for normal, Yellow for suspicious activity, Orange for fraudulent events, Red for under active attack).	U

[MM/DD/YYYY]

Page 461 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
Service URN (Uniform Resource Name)	A URN with “service” as the first component supplied as an input in a LoST request to an ECRF to indicate which service boundaries to consider when determining a response. A Request-URI with the service URN of “urn:service:sos” is used to mark a call as an emergency call. See Request-URI.	
SHA (Secure Hash Algorithm)	One of a number of fixed-size, cryptographic algorithms promulgated by the National Institute of Standards and Technology used to provide integrity protection for messages, files, and other data objects.	U
SI (Spatial Interface)	A standardized interface between the GIS and the functional elements that consume GIS data, such as the ECRF/LVF, Map Database Services, etc.	
SIO (Service Information Octet)	An eight-bit data field that is present in an SS7 message signal unit and is comprised of the service indicator and the sub-service field. It is used to determine the user part to which an incoming message should be delivered.	
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2, and NENA i3 .	
SLA (Service Level Agreement)	A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.	
SMS (Short Message Service)	A service typically provided by mobile carriers that sends short (160 characters or fewer) messages to an endpoint. SMS is often fast, but is not real-time.	
SNMP (Simple Network Management Protocol)	A protocol defined by the IETF used for managing devices on an IP network.	
SOA (Service Oriented Architecture)	A model in computer software design in which application components provide a repeatable business activity to other components using a communications protocol, typically over a network.	

[MM/DD/YYYY]

Page 462 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
SOAP (Simple Object Access Protocol)	A protocol for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework that more abstract layers can build upon.	U
SOS URN	A service URN starting with "urn:service:sos" which is used to mark calls as emergency calls as they traverse an IP network and to specify the desired emergency service in an ECRF request. See Service Uniform Resource Name.	
SR (Selective Router) AKA: Enhanced 9-1-1 Control Office	The Central Office switch that provides the tandem switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP.	
SR (Selective Routing)	The process by which 9-1-1 calls/messages are routed to the appropriate PSAP or other designated destination, based on the caller's location information, and may also be impacted by other factors, such as time of day, call type, etc. Location may be provided in the form of an MSAG-valid civic address or in the form of geodetic coordinates (longitude and latitude). Location may be conveyed to the system that performs the selective routing function in the form of ANI or pseudo-ANI associated with a pre-loaded ALI database record (in Legacy 9-1-1 systems), or in real-time in the form of a Presence Information Data Format-Location Object (PIDF-LO) (in NG9-1-1 systems) or whatever forms are developed as 9-1-1 continues to evolve.	
SRTP (Secure Real-time Protocol)	An IP protocol used to securely transport media (voice, video, text) which have a real-time constraint.	
SRV (Service)	A specification of data in the Domain Name System defining the location, (i.e. the hostname and port number) of servers for specified services.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
SS7 (Signaling System 7)	An out-of-band signaling system used to provide basic routing information, call set-up, and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network.	
SSRC (Synchronization Source)	As specified in RFC 3550, the source of a stream of RTP packets, identified by a 32-bit numeric SSRC identifier carried in the RTP header so as not to be dependent upon the network address.	A
STUN (Session Traversal Utilities for NAT)	A protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal	A
TCP (Transmission Control Protocol)	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the Open System Interconnection (OSI) model.	
TDM (Time Division Multiplexing)	A digital multiplexing technique for combining a number of signals into a single transmission facility by interweaving pieces from each source into separate time slots.	
TLS (Transport Layer Security)	An Internet protocol that operates between the IP layer and TCP and provides hop-by-hop authentication, integrity, protection, and privacy using a negotiated cipher-suite.	U
TN (Telephone Number)	A sequence of digits assigned to a device to facilitate communications via the public switched telephone network or other private network.	A
TRD (Technical Requirements Document)	NENA Technical Requirements Document, developed by a Technical Committee, is used as basis for a NENA Technical Committee or outside Standards Development Organization (SDO) to develop formal industry-accepted standards or guidelines.	A
TSP (Telematics Service Provider)	Companies which provide telematics (communications and data) services.	

[MM/DD/YYYY]

Page 464 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
TTY (Teletypewriter) AKA TDD (Telecommunications Device for the Deaf)	The phrase TTY (or Teletype device) is how the deaf community used to refer to the extremely large machines they used to type messages back and forth over the phone lines. A TDD operates in a similar way, but is a much smaller desktop machine. The deaf community has used the phrase "TTY" and sometimes uses it interchangeably with "TDD." http://www.gallaudet.edu/about/history-and-traditions/tty-relays-and-closed-captions	
TURN (Traversal Using Relays Around NAT)	A mechanism for establishing RTP connections through some kinds of NAT devices that won't allow two endpoints to connect directly. TURN uses a relay outside the NAT boundaries.	
TYS (Type of Service)	A designation in E9-1-1 that specifies if caller's service is published or non-published and if it is a foreign exchange outside the E9-1-1 serving area.	
UA (User Agent)	As defined for SIP in IETF RFC 3261[10], the User Agent represents an endpoint in the IP domain, a logical entity that can act as both a user agent client (UAC) that sends requests, and as user agent server (UAS) responding to requests.	
UAC (User Agent Client)	Refer to IETF RFC 3261 for the following definition. "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction."	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
UAS (User Agent Server)	<p>Refer to IETF RFC 3261 for the following definition.</p> <p>"A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction."</p>	
UDDI (Universal Description, Discovery and Integration)	An XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet.	
UDP (User Datagram Protocol)	One of several core protocols commonly used on the Internet. Used by programs on networked computers to send short messages, called datagrams, between one another. UDP is a lightweight message protocol compared to TCP, is stateless, and more efficient at handling lots of short messages from many clients.	

Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
URI (Uniform Resource Identifier)	<p>An identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. A URI can be further classified as a locator, a name, or both. The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). The term "Uniform Resource Name" (URN) has been used historically to refer to both URIs under the "urn" scheme [RFC2141], which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name. An example of a URI that is neither a URL nor a URN is sip:psap@example.com</p>	
URL (Uniform Resource Locator)	<p>A type of URI specifically used for describing and navigating to a resource (e.g., http://www.nena.org)</p>	
URN (Uniform Resource Name)	<p>A type of URI. Uniform Resource Names (URNs) are intended to serve as persistent, location-independent resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space. An example of a URN is urn:service.sos. RFC 2141.</p>	

[MM/DD/YYYY]

Page 467 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
US-CERT (United States Computer Emergency Readiness Team)	Part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) , the US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation.	A
USPS (United States Postal Service)	An independent agency of the United States government responsible for providing mail service in the United States.	A
UTC (Universal Coordinated Time)	The primary time standard in the world based on the time zone in Greenwich, England. Also known as Zulu or Greenwich Mean Time (GMT). Time provided by National Institute of Standards and Technology (NIST) and United States Naval Observatory (USNO).	
VEDS (Vehicle Emergency Data Sets)	A uniform data set for the transmission of Advanced Automatic Collision Notification (AACN) data by automobiles and automotive Telematics Service Providers (TSPs).	
VESA (Valid Emergency Services Authority)	This organization is the root source of all certificates. It is responsible for identifying and issuing certificates either directly to end-using entities or through delegate credential authorities. It is responsible for ensuring that any delegate credential authority that it identifies is properly qualified and operating with sufficient security and legitimacy to perform this role. Where VESA issues certificates directly to end users, it also has the responsibilities of a delegate credential authority in those cases.	
VoIP (Voice over Internet Protocol)	Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks.	
VPN (Virtual Private Network)	A network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation.	
VSP (VoIP Service Provider)	A company that offers VoIP telecommunications services that may be used to generate a 9-1-1 call, and interconnects with the 9-1-1 network.	

[MM/DD/YYYY]

Page 468 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
WFS (Web Feature Service)	A web service that allows a client to retrieve and update geospatial data encoded in Geography Markup Language (GML).	
WSDL (Web Service Definition Language)	<p>The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically. WSDL is the cornerstone of the Universal Description, Discovery, and Integration (UDDI) initiative spearheaded by Microsoft, IBM, and ARIBA. UDDI is an XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet. WSDL is the language used to do this..</p> <p>WSDL is derived from Microsoft's Simple Object Access Protocol (SOAP) and IBM's Network Accessible Service Specification Language (NASSL). WSDL replaces both NASSL and SOAP as the means of expressing business services in the UDDI registry.</p> <p>An XML-based interface definition language that is used for describing the functionality offered by a web service.</p>	
X.509	An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key.	
XACML (eXtensible Access Control Markup Language)	A general-purpose access control policy language that provides an XML-based syntax for defining rules to control access to resources.	U
XML (eXtensible Markup Language)	An internet specification for web documents that enables tags to be used that provide functionality beyond that in Hyper Text Markup Language (HTML). Its reference is its ability to allow information of indeterminate length to be transmitted to a PSAP call taker or dispatcher versus the current restriction that requires information to fit the parameters of pre-defined fields.	

[MM/DD/YYYY]

Page 469 of 675



Term or Abbreviation (Expansion)	Definition / Description	Add (A)/Update (U)
XMPP (Extensible Messaging and Presence Protocol)	A standardized protocol for exchanging instant messages, presence, files, and other objects.	
YAML (YAML Ain't Markup Language)	A human-readable data-serialization language ; commonly used for configuration files and in applications where data is being stored or transmitted.	A

11471

11472 12 References

11473 Note that this version of the document contains some references to documents that are
11474 works in progress at the IETF and other organizations. This document may be revised as
11475 these references stabilize.

- 11476 [1] National Emergency Number Association. *Master Glossary of 9-1-1 Terminology*.
11477 [NENA-ADM-000.23-2020](#). Arlington, VA: NENA, approved January 20, 2020.
- 11478 [2] National Emergency Number Association. *i3 Technical Requirements Document*.
11479 [NENA 08-751](#). Arlington, VA: NENA, approved September 28, 2006.
- 11480 [3] National Emergency Number Association. *Interim VoIP Architecture for Enhanced
11481 9-1-1 Services (i2)*. [NENA 08-001](#). Arlington, VA: NENA, approved August 11, 2010.
- 11482 [4] Internet Engineering Task Force. *Framework for Emergency Calling in Internet
11483 Multimedia*. B. Rosen, J. Polk, H. Schulzrinne, and A. Newton. [RFC 6443](#), December
11484 2011.
- 11485 [5] Internet Engineering Task Force. *Geopriv Requirements*. J. Cuellar, J. Morris, D.
11486 Mulligan, J. Peterson, and J. Polk. [RFC 3693](#), February 2004.
- 11487 [6] Internet Engineering Task Force. *A Presence-based GEOPRIV Location Object
11488 Format*. J. Peterson. [RFC 4119](#), December 2005.
- 11489 [7] Internet Engineering Task Force. *HTTP Enabled Location Delivery (HELD)*. M. Barnes,
11490 ed. [RFC 5985](#), September 2010.
- 11491 [8] Internet Engineering Task Force. *Session Initiation Protocol Location Conveyance*. J.
11492 Polk, B. Rosen and J. Peterson. [RFC 6442](#), December 2011.
- 11493 [9] Internet Engineering Task Force. *A Hitchhikers Guide to the Session Initiation
11494 Protocol (SIP)*. J. Rosenberg. [RFC 5411](#), February 2009.

[MM/DD/YYYY]

Page 470 of 675



- 11495 [10] Internet Engineering Task Force. *Session Initiation Protocol*. H. Schulzrinne, G.
11496 Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. [RFC 3261](#),
11497 June 2002.
- 11498 [11] Internet Engineering Task Force. *RTP: A Transport Protocol for Real-Time
11499 Applications*. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. [RFC 3550](#),
11500 July 2003.
- 11501 [12] Internet Engineering Task Force. *SDP: Session Description Protocol*. J. Handley, V.
11502 Jacobson, and C. Perkins. [RFC 4566](#), July 2006.
- 11503 [13] Internet Engineering Task Force. *Session Initiation Protocol (SIP): Locating SIP
11504 Servers*. J. Rosenberg and H. Schulzrinne. [RFC 3263](#), June 2002.
- 11505 [14] Internet Engineering Task Force. *Session Initiation Protocol (SIP)-Specific Event
11506 Notification*. A. Roach. [RFC 6665](#), July 2012.
- 11507 [15] Internet Engineering Task Force. *The Session Initiation Protocol UPDATE Method*. J.
11508 Rosenberg. [RFC 3311](#), September 2002.
- 11509 [16] Internet Engineering Task Force. *Private Extensions to the Session Initiation Protocol
11510 (SIP) for Asserted Identity within Trusted Networks*. C. Jennings, J. Peterson, and M.
11511 Watson. [RFC 3325](#), November 2002.
- 11512 [17] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Extension for
11513 Instant Messaging*. B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, and D.
11514 Gurle. [RFC 3428](#), December 2002.
- 11515 [18] Internet Engineering Task Force. *The Reason Header Field for the Session Initiation
11516 Protocol (SIP)*. H. Schulzrinne, D. Oran, and G. Camarillo. [RFC 3326](#), December
11517 2002.
- 11518 [19] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) Refer Method*.
11519 R. Sparks. [RFC 3515](#), April 2003.
- 11520 [20] Internet Engineering Task Force. *Grouping of Media Lines in the Session Description
11521 Protocol (SDP)*. G. Camarillo and H. Schulzrinne. [RFC 5888](#), June 2010.
- 11522 [21] Internet Engineering Task Force. *An Extension to the Session Initiation Protocol
11523 (SIP) for Symmetric Response Routing*. J. Rosenberg and H. Schulzrinne. [RFC 3581](#),
11524 August 2003.
- 11525 [22] Internet Engineering Task Force. *Real-time Control Protocol (RTCP) attribute in
11526 Session Description Protocol (SDP)*. C. Huitema. [RFC 3605](#), October 2003.
- 11527 [23] Internet Engineering Task Force. *Indicating User Agent Capabilities in the Session
11528 Initiation Protocol (SIP)*. J. Rosenberg, H. Schulzrinne, and P. Kyzivat. [RFC 3840](#),
11529 August 2004.
- 11530 [24] Internet Engineering Task Force. *Caller Preferences for the Session Initiation
11531 Protocol (SIP)*. J. Rosenberg, H. Schulzrinne, and P. Kyzivat. [RFC 3841](#), August 2004.
- 11532 [25] Internet Engineering Task Force. *A Presence Event Package for the Session Initiation
11533 Protocol (SIP)*. J. Rosenberg. [RFC 3856](#), August 2004.

[MM/DD/YYYY]

Page 471 of 675



- 11534 [26] Internet Engineering Task Force. *A Watcher Information Event Template-Package for*
11535 *the Session Initiation Protocol (SIP)* J. Rosenberg. [RFC 3857](#), August 2004.
11536 [27] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) "Replaces"*
11537 *Header*. R. Mahy, B. Biggs, and R. Dean. [RFC 3891](#), September 2004.
11538 [28] Internet Engineering Task Force. *The Session Initiation Protocol (SIP) Referred-By*
11539 *Mechanism*. R. Sparks. [RFC 3892](#), September 2004.
11540 [29] Internet Engineering Task Force. *Using E.164 numbers with the Session Initiation*
11541 *Protocol (SIP)*. J. Peterson, H. Liu, J. Yu, and B. Campbell. [RFC 3824](#), June 2004.
11542 [30] Internet Engineering Task Force. *Early Media and Ringing Tone Generation in the*
11543 *Session Initiation Protocol (SIP)*. G. Camarillo and H. Schulzrinne. [RFC 3960](#),
11544 December 2004.
11545 [31] Internet Engineering Task Force. *Presence Information Data Format (PIDF)*. H.
11546 Sugano, S. Fujimoto, G. Klyne, A. Bateman, and J. Peterson. [RFC 3863](#), August
11547 2004.
11548 [32] Internet Engineering Task Force. *Session Timers in the Session Initiation Protocol*
11549 *(SIP)*. S. Donovan and J. Rosenberg. [RFC 4028](#), April 2005.
11550 [33] Internet Engineering Task Force. *Internet Media Type message/sipfrag*. R. Sparks.
11551 [RFC 3420](#), November 2002.
11552 [34] Internet Engineering Task Force. *Basic Network Media Services with SIP*. J. Berger,
11553 Ed., J. Van Dyke, and A. Spitzer. [RFC 4240](#), December 2005.
11554 [35] Internet Engineering Task Force. *An Extension to the Session Initiation Protocol*
11555 *(SIP) for Request History Information*. M. Barnes, F. Audet, S. Schubert, J. van
11556 Elburg, and C. Holmberg. [RFC 7044](#), February 2014.
11557 [36] Internet Engineering Task Force. *Actions Addressing Identified Issues with the*
11558 *Session Initiation Protocol's (SIP) Non-INVITE Transaction*. R. Sparks. [RFC 4320](#),
11559 January 2006.
11560 [37] Internet Engineering Task Force. *Communications Resource Priority for the Session*
11561 *Initiation Protocol (SIP)*. H. Schulzrinne, and J. Polk. [RFC 4412](#), February 2006.
11562 [38] Internet Engineering Task Force. *Conveying Feature Tags with the Session Initiation*
11563 *Protocol (SIP) REFER Method*. O. Levin, and A. Johnston. [RFC 4508](#), May 2006.
11564 [39] Internet Engineering Task Force. *Session Initiation Protocol Call Control -*
11565 *Conferencing for User Agents*. A. Johnston and O. Levin. [RFC 4579](#), August 2006.
11566 [40] Internet Engineering Task Force. *A Session Initiation Protocol (SIP) Event Package*
11567 *for Conference State*. R. Rosenberg, H. Schulzrinne, and O. Levin. [RFC 4575](#), August
11568 2006.
11569 [41] Internet Engineering Task Force. *Obtaining and Using Globally Routable User Agent*
11570 *(UA) URIs (GRUU) in the Session Initiation Protocol (SIP)*. J. Rosenberg, Internet
11571 Engineering Task Force, [RFC 5627](#), October 2009.

[MM/DD/YYYY]

Page 472 of 675



- 11572 [42] Internet Engineering Task Force. *Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)*. C. Jennings, Ed., R. Mahy, Ed., and F. Audet, Ed.. [RFC 5626](#), October 2009.
- 11573 [43] Internet Engineering Task Force. *Session Initiation Protocol Package for Voice Quality Reporting*. A. Pendleton, A. Clark, A. Johnston, and H. Sinnreich. [RFC 6035](#), November 2010.
- 11574 [44] Internet Engineering Task Force. *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*. A. Keranen, C. Holmberg, and J. Rosenberg. [RFC 8445](#), July 2018.
- 11575 [45] Internet Engineering Task Force. *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*. H. Schulzrinne. [RFC 5031](#), January 2008.
- 11576 [46] Internet Engineering Task Force. *Best Current Practice for Communications Services in support of Emergency Calling*. B. Rosen and J. Polk. [RFC 6881](#), March 2013.
- 11577 [47] Internet Engineering Task Force. *Location-to-URL Mapping Architecture and Framework*. H. Schulzrinne. [RFC 5582](#), September 2009.
- 11578 [48] Internet Engineering Task Force. *LoST: A Location-to-Service Translation Protocol*. T. Hardie, A. Newton, H. Schulzrinne, and H. Tschofenig. [RFC 5222](#), August 2008.
- 11579 [49] 3rd Generation Partnership Project. *IP Multimedia Subsystem (IMS) emergency sessions*. Curt Wong. [3GPP TS 23.167](#), January 22, 2015.
- 11580 [50] Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions. *Enhanced Wireless 9-1-1 Phase 2*. Washington, DC: ATIS. [J-STD-036-C-2](#). Washington, DC: ATIS, June 2017.
- 11581 [51] Organization for the Advancement of Structured Information Standards (OASIS). *Universal Description, Discovery, and Integration (UDDI) Version 3.0*. L. Clement, A. Hately, C. von Riegen, T. Rogers. [UDDI V3.0](#), October 19, 2004.
- 11582 [52] Internet Engineering Task Force. *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*. J. Winterbottom, M. Thomson, and H. Tschofenig. [RFC 5491](#), March 2009.
- 11583 [53] Internet Engineering Task Force. *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*. M. Thomson and J. Winterbottom. [RFC 5139](#), March 2009.
- 11584 [54] Internet Engineering Task Force. *Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance*. R. Marshall. [RFC 5808](#), May 2010.
- 11585 [55] Internet Engineering Task Force. *A Location Dereferencing Protocol Using HTTP-Enabled Location Delivery (HELD)*. J. Winterbottom, H. Tschofenig, H. Schulzrinne, and M. Thomson. [RFC 6753](#), October 2012.

- 11610 [56] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Overload Control*. V.
11611 Gurbani, V. Hilt, and H. Schulzrinne. [RFC 7339](#), September 2014.
- 11612 [57] Internet Engineering Task Force. *The Transport Layer Security (TLS) Protocol Version*
11613 1.1. T. Dierks and E. Rescola. [RFC 4346](#), April 2006.
- 11614 [58] Organization for the Advancement of Structured Information Standards (OASIS).
11615 *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)*
11616 V2.0. S. Cantor, J. Kemp, R. Philpott, and E. Maler. [saml-core-2.0-os](#), March 15,
11617 2005.
- 11618 [59] Internet Engineering Task Force. *Internet X.509 Public Key Infrastructure Certificate*
11619 *Policy and Certification Practices Framework*. S. Chokani, W. Ford, R. Sabett, C.
11620 Merrill, and S. Wu. [RFC 3647](#), November 2003.
- 11621 [60] Internet Engineering Task Force. *Authenticated Identity Management in the Session*
11622 *Initiation Protocol (SIP)*. J. Peterson, C. Jennings, E. Rescorla, and C. Wendt. [RFC](#)
11623 [8224](#), February 2018.
- 11624 [61] Organization for the Advancement of Structured Information Standards (OASIS).
11625 *eXtensible Access Control Markup Language (XACML) Version 2.0*. [XACML 2.0](#),
11626 February 1, 2005.
- 11627 [62] National Institute of Standards and Technology. *Secure Hash Standard, Federal*
11628 *Information Processing Standards Publication 180-4*. [FIPS-PUB-180-4](#), August 2015.
- 11629 [63] National Institute of Standards and Technology. *Advanced Encryption Standard,*
11630 *Federal Information Processing Standards Publication 197*. [FIPS-PUB-197](#), November
11631 26, 2001.
- 11632 [64] Internet Engineering Task Force. *Simple Network Management Protocol, Version 3*
11633 (*SNMPv3*). J. Case, R. Mundy, D. Partain, and B. Stewart. [RFC 3410](#), December 2002
11634 through [RFC 3418](#), December 2002.
- 11635 [65] Internet Engineering Task Force. *RTP Control Protocol Extended Reports (RTCP XR)*.
11636 T. Friedman, Ed., R. Caceres, Ed., and A. Clark, Ed. [RFC 3611](#), November 2003.
- 11637 [66] Organization for the Advancement of Structured Information Standards. *Common*
11638 *Alerting Protocol V1.0*. A. Botterell. [oasis-200402-cap-core-1.0](#), March 2004.
- 11639 [67] National Institute of Standards and Technology. *Security Requirements for*
11640 *Cryptographic Modules, Federal Information Processing Standards Publication 140-2*.
11641 [FIPS-PUB-140-3](#), March 22, 2019.
- 11642 [68] Internet Engineering Task Force. *An INVITE-Initiated Dialog Event Package for the*
11643 *Session Initiation Protocol (SIP)*. J. Rosenberg, H. Schulzrinne, and R. Mahy. [RFC](#)
11644 [4235](#), November 2005.
- 11645 [69] GML 3.1.1 PIDF-LO Shape Application Schema for Use by the Internet Engineering
11646 Task Force (IETF), M. Thomson and C. Reed, Candidate OpenGIS Implementation
11647 Specification [06-142r1](#), Version 1.0, April 2007.

- 11648 [70] National Emergency Number Association. *Functional and Interface Standards for*
11649 *Next Generation 9-1-1 Version 1.0 (i3)*. [NENA 08-002](#). Arlington, VA: NENA,
11650 approved December 18, 2007.
- 11651 [71] National Emergency Number Association. *Technical Information Document*
11652 *Network/System Access Security*. [NENA 04-503](#). Arlington, VA: NENA, approved
11653 December 1, 2005.
- 11654 [72] Internet Engineering Task Force. *Filtering Location Notifications in the Session*
11655 *Initiation Protocol (SIP)*. R. Mahy, B. Rosen, and H. Tschofenig. [RFC 6447](#), January
11656 2012.
- 11657 [73] National Emergency Number Association. *NG9-1-1 Additional Data*. [NENA-STA-](#)
11658 [012.2-2017](#). Arlington, VA: NENA, approved December 21, 2017.
- 11659 [74] Internet Engineering Task Force. *Domain Names – Concepts And Facilities*. , P.
11660 Mockapetris. [RFC 1034](#), November 1987.
- 11661 [75] Internet Engineering Task Force. *A DNS RR for specifying the location of services*
11662 (*DNS SRV*). A. Gulbrandsen, P. Vixie, and L. Esibov. [RFC 2782](#), February 2000.
- 11663 [76] SIPforum. *IP PBX / Service Provider Interoperability*. C. Sibley, C. Gatch. [SIPconnect](#)
11664 [Technical Recommendation V1.0](#), January 23, 2008.
- 11665 [77] National Emergency Number Association. *Next Generation United States Civic*
11666 *Location Data Exchange Format (CLDXF)*. [NENA-STA-004.1-2014](#), Arlington, VA:
11667 NENA, approved March 23, 2014.
- 11668 [78] Organization for the Advancement of Structured Information Standards. *Emergency*
11669 *Data Exchange Language Distribution Element (EDXL-DE) 1.0*. M. Raymond, S.
11670 Webb, and P. Aymond. [OASIS EDXL-DE v1.0](#), May 1, 2006.
- 11671 [79] Internet Engineering Task Force. *Synchronizing Service Boundaries and <mapping>*
11672 *Elements Based on the Location-to-Service Translation (LoST) Protocol*. H.
11673 Schulzrinne and H. Tschofenig. [RFC 6739](#), October 2012.
- 11674 [80] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Event Notification*
11675 *Extension for Notification Rate Control*. A. Niemi, K. Kiss, and S. Loreto. [RFC 6446](#),
11676 January 2012.
- 11677 [81] Internet Engineering Task Force. *Design Considerations for Session Initiation*
11678 *Protocol (SIP) Overload Control*. V. Hilt, E. Noel, C. Shen, and A. Abdelai. [RFC 6357](#),
11679 August 2011.
- 11680 [82] World Wide Web Consortium (W3C). *XML Schema Part 2: Datatypes Second Edition*.
11681 P. Biron and A. Malhotra. <http://www.w3.org/TR/xmlschema-2/>, October 28, 2004.
- 11682 [83] Internet Engineering Task Force. *Session Traversal Utilities for NAT (STUN)*, J.
11683 Rosenberg, R. Mahy, P. Matthews, and D. Wing. [RFC 5389](#), October 2008.
- 11684 [84] Internet Engineering Task Force. *Framework for Real-Time Text over IP Using the*
11685 *Session Initiation Protocol (SIP)*. A. van Wijk and G. Gybels. [RFC 5194](#), June 2008.

- 11686 [85] Internet Engineering Task Force. *RTP Payload for Text Conversation*. G. Hellstrom
11687 and P. Jones. [RFC 4103](#), June 2005.
- 11688 [86] Internet Engineering Task Force. *Framework for Transcoding with the Session*
11689 *Initiation Protocol (SIP)*. G. Camarillo. [RFC 5369](#), October 2008.
- 11690 [87] Internet Engineering Task Force. *Indication of Message Composition for Instant*
11691 *Messaging*. H. Schulzrinne. [RFC 3994](#), January 2005.
- 11692 [88] Internet Engineering Task Force. *The Message Session Relay Protocol (MSRP)*. B.
11693 Campbell, Ed., R. Mahy, Ed., and C. Jennings, Ed. [RFC 4975](#), September 2007.
- 11694 [89] Internet Engineering Task Force. *Relay Extensions for the Message Session Relay*
11695 *Protocol (MSRP)*. C. Jennings, R. Mahy, A.B. Roach, Internet Engineering Task Force,
11696 [RFC 4976](#), September 2007.
- 11697 [90] Internet Engineering Task Force. *Multipurpose Internet Mail Extensions (MIME) Part*
11698 *Two: Media Types*. N. Freed and N. Borenstein. [RFC 2046](#), November 1996.
- 11699 [91] Alliance for Telecommunications Industry Solutions. *Signalling System Number 7*
11700 (*SS7 – Operator Services Network Capabilities*). [ATIS-1000666.1999 \(S2019\)](#).
11701 Washington, DC: ATIS, February 11, 1999.
- 11702 [92] Internet Engineering Task Force. *An Extensible Markup Language (XML)-Based*
11703 *Format for Event Notification Filters*. H. Khatabil, E. Leppanen, M. Lonnfors, and J.
11704 Costa-Requena. [RFC 4661](#), September 2006.
- 11705 [93] Open Geospatial Consortium. *OGC Web Feature Service 2.0 Interface Standard –*
11706 *With Corrigendum Version 2.0.2*. P. Vretanos. [OGC09-025r2](#), July 10, 2014.
- 11707 [94] Open Geospatial Consortium. *OWS 7 Engineering Report – Geosynchronization*
11708 *service*. P. Vretanos, , [OGC 10-069r2](#), January 12, 2011.
- 11709 [95] Internet Engineering Task Force. *The Atom Syndication Format*. M. Nottingham and
11710 R. Sayre. [RFC 4287](#), December 2005.
- 11711 [96] Internet Engineering Task Force. *The ATOM Publishing Protocol*. J. Gregorio, Ed., and
11712 B. de hOra, Ed. [RFC 5023](#), October 2007.
- 11713 [97] World Wide Web Consortium. *Voice Extensible Markup Language (VoiceXML) Version*
11714 *2.0*. S. McGlashan, D. Burnett, J. Carter, P. Danielsen, J. Ferrans, A. Hunt, B. Lucas,
11715 B. Porter, K. Rehor, and S. Tryphonas. [REC-voicexml20-20040316](#), 16 March 2004.
- 11716 [98] Internet Engineering Task Force. *Real-time Streaming Protocol Version 2.0*. H.
11717 Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, and M. Stiemerling, Ed., [RFC 7826](#),
11718 December 2016.
- 11719 [99] Internet Engineering Task Force. *The Session Description Protocol (SDP) Label*
11720 *Attribute*. O. Levin and G. Camarillo, RFC 4574, August 2006.
- 11721 [100] Internet Engineering Task Force. *An Extension to the Session Description Protocol*
11722 *(SDP) and Real-time Transport Protocol (RTP) for Media Loopback*. H. Kaplan, K.
11723 Hedayat, N. Venna, P. Jones, and N. Stratton. RFC 6849, February 2013.

[MM/DD/YYYY]

Page 476 of 675



- 11724 [101] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service*
11725 *Option 3 for Wideband Spread Spectrum Digital Systems.* [C.S0014-A V1.0](#), April
11726 2004; and also Internet Engineering Task Force. *RTP Payload Format for Enhanced*
11727 *Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV).* A. Li. [RFC 3558](#),
11728 July 2003.
- 11729 [102] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service*
11730 *Option 3 and 68 for Wideband Spread Spectrum Digital Systems.* [C.S0014-B V1.0](#),
11731 May 2006; and also Internet Engineering Task Force. *Enhancements to RTP Payload*
11732 *Formats for EVRC Family Codecs.* Q. Xie and R. Kapoor. [RFC 4788](#), January 2007.
- 11733 [103] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service*
11734 *Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems.* [C.S0014-C](#)
11735 [V1.0](#), January 2007; and also Internet Engineering Task Force. *RTP Payload Format*
11736 *for the Enhanced Variable Rate Wideband Codec (EVRC-WB) and the Media Subtype*
11737 *Updates for EVRC-B Codec.* H. Desineni and Q. Xie. [RFC 5188](#), February 2008.
- 11738 [104] 3rd Generation Partnership Project 2. *Enhanced Variable Rate Codec, Speech Service*
11739 *Options 3, 68, 70, and 73 for Wideband Spread Spectrum Digital Systems.*
11740 [C.S0014-D V1.0](#), May 2009; and also Internet Engineering Task Force. *RTP payload*
11741 *format for Enhanced Variable Rate Narrowband-Wideband Codec (EVRC-NW).* R.
11742 Aggarwal, K. Kompella, T. Nadeau, and G. Swallow. [RFC 6884](#), June 2010.
- 11743 [105] National Emergency Number Association. "Funding 9-1-1 Into the Next Generation:
11744 An Overview of NG9-1-1 Funding Model Options for Consideration". [NG Funding](#)
11745 [Report](#). Arlington, VA: NENA, March 2007.
- 11746 [106] National Emergency Number Association. "Next Generation 9-1-1 Transition Policy
11747 Implementation Handbook: A Guide for Identifying and Implementing Policies to
11748 Enable NG9-1-1". [NG911 Transition Policy Handbook](#). Arlington, VA: NENA, March
11749 2010.
- 11750 [107] Internet Engineering Task Force. *Additional Data related to an Emergency Call.* R.
11751 Gellens, B. Rosen, H. Tschofenig, R. Marshall, and J. Winterbottom. [RFC 7852](#), July
11752 2016.
- 11753 [108] Internet Engineering Task Force. *Geolocation Policy: A Document Format for*
11754 *Expressing Privacy Preferences for Location Information.* H. Schulzrinne, H.
11755 Tschofenig, J. Cuellar, J. Polk, J. Morris, and M. Thomson. [RFC 6772](#), January 2013.
- 11756 [109] Internet Engineering Task Force. *Common Policy: A Document Format for Expressing*
11757 *Privacy Preferences..* H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, J.
11758 Rosenberg. [RFC 4745, February 2007](#).
- 11759 [110] National Institute of Standards and Technology. *Guide to Storage Encryption*
11760 *Technologies for End User Devices.* K. Scarfone, M. Souppaya, and M. Sexton. [NIST](#)
11761 [Special Publication 800-111](#), November 2007.

[MM/DD/YYYY]

Page 477 of 675



- 11762 [111] National Emergency Number Association. *Emergency Incident Data Object (EIDO)*.
11763 [NENA-STA-021.1-201X](#). Arlington, VA: NENA (forthcoming).
- 11764 [112] Internet Engineering Task Force. *URN Syntax*. R. Moats. [RFC 2141, <date>](#).
- 11765 [113] Internet Engineering Task Force. *xCard: vCard XML Representation*. S. Perreault.
[RFC 6351](#), May 1997.
- 11766 [114] National Emergency Number Association *Legacy Selective Router Gateway Technical Standard*. NENA-STA-034.1-202x. Arlington, VA: NENA, (forthcoming).
- 11767 [115] Internet Engineering Task Force. *Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)*. J. Winterbottom, M. Thomson,
R. Barnes, B. Rosen, and R. George. [RFC 6848](#), January 2013.
- 11768 [116] Internet Engineering Task Force. *Session Recording Protocol*. L. Portman, H. Lum,
Ed., C. Eckel, A. Johnston, and A. Hutton. [RFC 7866](#), May 2016.
- 11769 [117] Internet Engineering Task Force. *Session Initiation Protocol (SIP) Recording Metadata*. R. Mohan, P. Ravindran, and P. Kyzivat. [RFC 7865](#), May 2016.
- 11770 [118] Internet Engineering Task Force. *DNS Security Introduction and Requirements*. R.
Arends, R. Austein, M. Larson, D. Massey, and S. Rose. [RFC 4035](#), March 2005.
- 11771 [119] Internet Engineering Task Force. *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*. R. Mahy, P. Matthews, and
J. Rosenberg. [RFC 5766](#), April 2010.
- 11772 [120] International Telecommunications Union. *The international public telecommunication numbering plan*. [Recommendation E.164 \(11/10\)](#), November 18, 2010.
- 11773 [121] Internet Engineering Task Force. *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)*. S. Wenger, U. Chandra, M. Westerlund, and B.
Burman. [RFC 5104](#), February 2008.
- 11774 [122] Internet Engineering Task Force. *XML Schema for Media Control*. O. Levin, R. Even,
and P. Hagendorf. [RFC 5168](#), March 2008.
- 11775 [123] Internet Engineering Task Force. *Multi-party Chat Using the Message Session Relay Protocol (MSRP)*. A. Niemi, M. Garcia-Martin, and G. Sandbakken. [RFC 7701](#),
December 2015.
- 11776 [124] Internet Engineering Task Force. *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*. J. Ott, S. Wenger, N. Sato, C.
Burmeister, and J. Rey. [RFC 4585](#), July 2006.
- 11777 [125] Internet Engineering Task Force. *Call Processing Language (CPL): A Language for User Control of Internet Telephony Services*. J. Lennox, X. Wu, and H. Schulzrinne.
[RFC 3880](#), October 2004.
- 11778 [126] Internet Engineering Task Force. *Uniform Resource Identifier (URI): Generic Syntax*.
T. Berners-Lee, R. Fielding and L. Masinter. [RFC 3986](#), January 2005.

- 11799 [127] Organization for the Advancement of Structured Information Standards (OASIS).
11800 *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.* [saml-](#)
11801 [bindings-2.0-os](#), March 15, 2005.
11802 [128] Organization for the Advancement of Structured Information Standards (OASIS).
11803 *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* [saml-](#)
11804 [profiles-2.0-os](#), March 15, 2005.
11805 [129] Organization for the Advancement of Structured Information Standards (OASIS).
11806 *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0.* [saml-](#)
11807 [metadata-2.0-os](#), March 15, 2005.
11808 [130] Alliance for Telecommunications Industry Solutions. *Interworking between Session*
11809 *Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part.*
11810 [ATIS 1000679.2015](#). Washington, DC: ATIS, April 14, 2015.
11811 [131] Internet Engineering Task Force. *Discovering Location-to-Service Translation (LoST)*
11812 *Servers Using the Dynamic Host Configuration Protocol (DHCP).* H. Schulzrinne, J.
11813 Polk, and H. Tschofenig. [RFC 5223](#), August 2008.
11814 [132] Internet Engineering Task Force. *Content-ID and Message-ID Uniform Resource*
11815 *Locators.* E. Levinson. [RFC 2392](#), August 1998.
11816 [133] Internet Engineering Task Force. *Simple Mail Transfer Protocol.* J. Klensin. [RFC 5321](#),
11817 October 2008.
11818 [134] Internet Engineering Task Force. *An Architecture for Differentiated Services.* S.
11819 Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss. [RFC 2475](#), December
11820 1998.
11821 [135] Internet Engineering Task Force. *Date and Time on the Internet: Timestamps.* G.
11822 Klyne and C. Newman. [RFC 3339](#), July 2002.
11823 [136] Alliance For Telecommunications Industry Solutions. *ECS – Connection and Ring*
11824 *Back Addendum [Supplement to ATIS-1000628.2000 (R2010)], ATIS-*
11825 [1000678.a.2001\(R2015\)](#). Washington, DC: ATIS, August 2002.
11826 [137] Cable Television Laboratories, Inc. *Residential SIP Telephony Feature Specification.*
11827 [PKT-SP-RSTF-C01-140314](#), March 14, 2014.
11828 [138] Cable Television Laboratories, Inc. *CMS to CMS Signaling Specification.* [PKT-SP-](#)
11829 [CMSS1.5-I07-120412](#), April 12, 2012.
11830 [139] Internet Engineering Task Force. *Integrated Services Digital Network (ISDN) User*
11831 *Part (ISUP) to Session Initiation Protocol (SIP) Mapping.* G. Camarillo, A. B. Roach, J.
11832 Peterson, and L. Ong. [RFC 3398](#), December 2002.
11833 [140] Internet Engineering Task Force. *Definition of Events for Channel-Oriented*
11834 *Telephony Signalling.* H. Schulzrinne and T. Taylor. [RFC 5244](#), June 2008.
11835 [141] Internet Engineering Task Force. *Public Safety Answering Point (PSAP) Callback.* H.
11836 Schulzrinne, H. Tschofenig, C. Holmberg, and M. Patel. [RFC 7090](#), April 2014.

- 11837 [142] Internet Engineering Task Force. *RTP Payload for DTMF Digits, Telephony Tones, and*
11838 *Telephony Signals.* H. Schulzrinne and T. Taylor. [RFC 4733](#), December 2006.
- 11839 [143] Telcordia Technologies. *Telcordia Technologies Specification of Signalling System*
11840 *Number 7.* [GR-246-CORE](#), December 2005.
- 11841 [144] International Telecommunications Union. *The Directory: Public-key and attribute*
11842 *certificate frameworks.* [Recommendation X.509 \(10/2019\)](#), October 14, 2019.
- 11843 [145] Internet Engineering Task Force. *Representation of Uncertainty and Confidence in*
11844 *the Presence Information Data Format Location Object (PIDF-LO).* M. Thomson and
11845 J. Winterbottom. [RFC 7459](#), February 2015.
- 11846 [146] [Internet Engineering](#) Task Force. *Dynamic Extensions to the Presence Information*
11847 *Data Format Location Object (PIDF-LO).* H. Schulzrinne, V. Singh, H. Tschofenig, and
11848 M. Thomson. [RFC 5962](#), September 2010.
- 11849 [147] Internet Engineering Task Force. *Dynamic Host Configuration Protocol.* R. Droms.
11850 [RFC 2131](#), March 1997.
- 11851 [148] World Wide Web Consortium (W3C). *SOAP Version 1.2 Part 1: Messaging Framework*
11852 *(Second Edition).* M. Gugin, M. Hadley, N. Mendelsohn, J-J. Moreau, H. F. Nielsen, A.
11853 Karmarkar, and Y. Lafon. [TR/2007/REC-soap12-part1-20070427](#), April 27, 2007.
- 11854 [149] Internet Engineering Task Force. *Session Initiation Protocol (SIP) INFO Method and*
11855 *Package Framework.* C. Holmberg, E. Burger, and H. Kaplan. [RFC 6086](#), January
11856 2011.
- 11857 [150] Internet Engineering Task Force. *The tel URI for Telephone Numbers.* H.
11858 Schulzrinne. [RFC 3966](#), December 2004.
- 11859 [151] Alliance For Telecommunications Industry Solutions. *ATIS Standard for*
11860 *Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination*
11861 *and ESInet/Legacy Selective Router Termination.* [ATIS-0700015.v004](#). Washington,
11862 DC: ATIS, July 2018.
- 11863 [152] Association of Public-Safety Communications Officials (APCO) and Central Station
11864 Alarm Association (CSAA). *Alarm Monitoring Company to Public Safety Answering*
11865 *Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol*
11866 *(ASAP),* [APCO/CSAA ANS 2.101.2-2014](#), August 5, 2014.
- 11867 [153] Internet Engineering Task Force. *HTTP over TLS.* E. Rescorla. [RFC 2818](#), May 2000.
- 11868 [154] Internet Engineering Task Force. *Domain-Based Application Service Location Using*
11869 *URIs and the Dynamic Delegation Discovery Service (DDDS).* L. Daigle. [RFC 4848](#),
11870 April 2007.
- 11871 [155] Internet Engineering Task Force. *Discovering the Local Location Information Server*
11872 *(LIS).* M. Thomson and J. Winterbottom. [RFC 5986](#), September 2010.
- 11873 [156] Internet Engineering Task Force. *A Session Initiation Protocol (SIP) Event Package*
11874 *for Key Press Stimulus (KPML).* E. Burger and M. Dolly. [RFC 4730](#), November 2006.

- 11875 [157] International Organization for Standardization (ISO). *Identification cards – Integrated*
11876 *circuit cards.* [ISO/IEC 7816 \(1-15\)](#). Geneva: ISO, 1999-2018.
- 11877 [158] Internet Engineering Task Force. *Public-Key Cryptography Standards (PKCS) #1:*
11878 *RSA Cryptography Specifications Version 2.2.* K. Moriarty, Ed., B. Kaliski, J. Jonsson,
11879 and A. Rusch. [RFC 8017](#), November 2016.
- 11880 [159] Telcordia Technologies. *CCS/SS7 Generic Requirements in Support of E9-1-1 Service.*
11881 [GR-2956-CORE](#), December 2002.
- 11882 [160] Telcordia Technologies. *LSSGR: Switching System Generic Requirements for Call*
11883 *Control Using the Integrated Services Digital Network User Part (ISDNUP).* [GR-317-](#)
11884 [CORE](#), November 2007.
- 11885 [161] Internet Engineering Task Force. *Representing Trunk Groups in tel/sip Uniform*
11886 *Resource Identifiers (URIs).* V. Gurbani and C. Jennings. [RFC 4904](#), June 2007.
- 11887 [162] Internet Engineering Task Force. *Hypertext Transfer Protocol (HTTP/1.1): Message*
11888 *Syntax and Routing.* R. Fielding, Ed. and J. Reschke, Ed. [RFC 7230](#), June 2014.
- 11889 [163] National Emergency Number Association. *NENA Standard for the implementation of*
11890 *Enhanced MF Signaling, E9-1-1 Tandem to PSAP.* [NENA 03-002](#). Arlington, VA:
11891 NENA, January 17, 2007.
- 11892 [164] National Emergency Number Association. *NENA E9-1-1 PSAP Equipment Standards.*
11893 [NENA-STA-027.3-2018 \(originally 04-001\)](#). Arlington, VA: NENA, July 2, 2018.
- 11894 [165] National Emergency Number Association. *NENA ALI Query Service Standard.* [NENA](#)
11895 [04-005](#), Arlington, VA: NENA, November 21, 2006.
- 11896 [166] Internet Engineering Task Force. *Framework for Establishing a Secure Real-time*
11897 *Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security*
11898 *(DTLS).* J. Fischl, H. Tschofenig, and E. Rescorla. [RFC 5763](#), May 2010.
- 11899 [167] Internet Engineering Task Force. *Datagram Transport Layer Security (DTLS)*
11900 *Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP).* D.
11901 McGrew and E. Rescorla. [RFC 5764](#), May 2010
- 11902 [168] Internet Engineering Task Force. *Next-Generation Vehicle-Initiated Emergency Calls.*
11903 R. Gellens, B. Rosen, and H. Tschofenig. [RFC 8148](#), May, 2017.
- 11904 [169] Association of Public-Safety Communications Officials. *Vehicular Emergency Data Set*
11905 *(VEDS) Recommendation Version 3.0.* [VEDS 3.0](#). Daytona Beach: Advanced
11906 Automatic Crash Notification (AACN) Joint APCO/NENA Data Standardization
11907 Working Group, July 2012.
- 11908 [170] Internet Engineering Task Force. *Private Session Initiation Protocol (SIP) Proxy-to-*
11909 *Proxy Extensions for Supporting the PacketCable Distributed Call Signaling*
11910 *Architecture.* F. Andreasen, B. McKibben and B. Marshall. [RFC 5503](#), March 2009.
- 11911 [171] Internet Engineering Task Force. *JSON Web Signature (JWS).* M. Jones, J. Bradley,
11912 and N. Sakimura. [RFC 7515](#), May 2015.

- 11913 [172] Internet Engineering Task Force. *Real-time text media handling in multi-party*
11914 *conferences*. G. Hellstrom. Draft-hellstrom-[mmusic-multi-party-rtt-00](#), November 1,
11915 2019.
- 11916 [173] Internet Engineering Task Force. *Negotiating Human Language in Real-Time*
11917 *Communications*. R. Gellens. [RFC 8373](#), May 2018.
- 11918 [174] National Emergency Number Association. *TTY/TDD Communications Standard*
11919 *Operating Procedure Model Recommendation*. [NENA-STA-037.2-2018 \(originally 56-](#)
11920 [004\)](#). Arlington, VA: NENA, August 17, 2018.
- 11921 [175] Federal Communications Commission. *Proposed procedures for the TTY as a text*
11922 *terminal in legacy 9-1-1 PSAPs without IP connection*. [EAAC Report. Washington DC:](#)
11923 Emergency Access Advisory Committee (EAAC) TTY Transition Report, June 14,
11924 2013.
- 11925 [176] Internet Engineering Task Force. *Common Profile For Instant Messaging (CPIM)*. J.
11926 Peterson. [RFC 3860](#), August 2004.
- 11927 [177] Internet Engineering Task Force. *Common Presence and Instant Messaging (CPIM):*
11928 *Message Format*. G. Klyne and D. Atkins. [RFC 3862](#), August 2004.
- 11929 [178] Internet Engineering Task Force. *Validation of Locations Around a Planned Change*,
11930 B. Rosen. [draft-ecrit-lost-planned-changes](#) (expired), July 18, 2016.
- 11931 [179] Internet Assigned Numbers Authority (IANA). "Emergency Call Data Types."
11932 Accessed December 29, 2019. [IANA registry](#).
- 11933 [180] Internet Assigned Numbers Authority (IANA). "Language Subtag Registry." Accessed
11934 December 29, 2019. [IANA registry](#).
- 11935 [181] Internet Assigned Numbers Authority (IANA). "Media types." Accessed December 29,
11936 2019. [IANA Registry](#).
- 11937 [182] SIPforum. *SIP-PBX / Service Provider Interoperability*. A. Hutton and G. Salgueiro.
11938 SIPconnect 2.0 Technical Recommendation, Document Number: [TWG 11](#), 2016.
- 11939 [183] Telecommunications Industry Association. *A Frequency Shift Keyed Modem for Use*
11940 *on the Public Switched Telephone Network*. [TIA-825 Revision A](#). Englewood, CO:
11941 TIA, April 2003.
- 11942 [184] National Emergency Number Association. *NENA Standard for NG9-1-1 GIS Data*
11943 *Model*. [NENA-STA-006.1-2018](#). Arlington, VA: NENA, June 16, 2018.
- 11944 [185] National Emergency Number Association. *NENA Standard for the Conveyance of*
11945 *Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1)*
11946 *Systems and Applications*. NENA-STA-024.1-202X. Arlington, VA: NENA,
11947 (forthcoming)
- 11948 [186] Open Geospatial Consortium. *Open GIS Web Map Server Implementation*
11949 *Specification, Version 1.3.0*. J. de la Beaujardiere, Ed. [OGC 06-042](#). March 15, 2006.
- 11950 [187] Spatial Reference. "EPSG Projection 4326 – WGS 84." Last revised August 27, 2007.
11951 <http://spatialreference.org/ref/epsg/4326/>

[MM/DD/YYYY]

Page 482 of 675



- 11952 [188] Alliance For Telecommunications Industry Solutions. *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling.* [ATIS 0600414.1998 \(R2007\)](#) Washington, DC: ATIS, March 1, 1998.
- 11953 [189] Telcordia Technologies. *E911 Public Safety Answering Point: Interface Between 1/1AESS Switch and Customer Premise Equipment.* [GR-350-CORE](#), June 2003.
- 11954 [190] Telcordia Technologies. *Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface.* [GR-2953-CORE](#), March 1997.
- 11955 [191] Alliance for Telecommunication Industry Solutions. *Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification, Release 2.* [ATIS J-STD-110.v002](#). Washington, DC: ATIS, May 1, 2015.
- 11956 [192] Alliance for Telecommunication Industry Solutions. *Network to Customer Installation Interfaces – Enhanced 911 Analog Voicegrade PSAP Access Using Loop Reverse-Battery Signaling.* [ATIS-0900414.2012\(R2017\)](#). Washington, DC: ATIS, April 2012.
- 11957 [193] National Emergency Number Association. *NENA Standard for NG9-1-1 Additional Data.* [NENA STA-012.2.-2017 \(originally 71-001\)](#). Arlington, VA: NENA, 12/21/2019.
- 11958 [194] National Emergency Number Association. *NENA Registry System Standard,* [NENA-STA-008.2-2014 \(originally 70-001\)](#). Arlington, VA: NENA, October 6, 2014.
- 11959 [195] Internet Engineering Task Force. *Uniform Resource Name (URN) Namespace for the National Emergency Number Association (NENA).* B. Rosen. [RFC 6061](#), January 2011.
- 11960 [196] Internet Engineering Task Force. *A Recommendation for Ipv6 Address Text Representation.* S. Kawamura and M. Kawashima. [RFC 5952](#), August 2010.
- 11961 [197] Internet Engineering Task Force. *Hypertext Transfer Protocol Version 2 (HTTP/2).* M. Belshe, R. Peon, and M. Thomson, Ed. [RFC 7540](#), May 2015.
- 11962 [198] Open Mobile Alliance. *Mobile Location Protocol 3.2 Approved Version 3.2.* [OMA-TS-MLP-V3_2-20110719-A](#), July 19, 2011.
- 11963 [199] Internet Engineering Task Force. *The Transport Layer Security (TLS) Protocol Version 1.2.* T. Dierks and E. Rescorla. [RFC 5246](#), August 2008.
- 11964 [200] Internet Engineering Task Force. *Transport Layer Security (TLS) Protocol Version 1.3.* E. Rescorla. [RFC 8446](#), August 2018.
- 11965 [201] Internet Engineering Task Force. *Location Source Parameter for the SIP Geolocation Header Field.* J. Winterbottom, R. Jesske, B. Chatras, and A. Hutton. [RFC 8787](#). May 2020.
- 11966 [202] Internet Engineering Task Force. *Next-Generation Pan-European eCall.* R. Gellens and H. Tschofenig. [RFC 8147](#), May 2017.
- 11967 [203] Internet Engineering Task Force. *PASSporT: Personal Assertion Token.* C. Wendt and J. Peterson. [RFC 8225](#), February 2018.

[MM/DD/YYYY]

Page 483 of 675



- 11990 [204] 3rd Generation Partnership Project. *Codec for Enhanced Voice Services (EVS)* J. Gibbs. [3GPP TS 26.441](#), June 2018.
- 11991 [205] 3rd Generation Partnership Project. *Mandatory speech CODEC speech processing functions; AMR speech Codec; General Description*. S. Bruhn. [3GPP TS 26.071](#), June 2018.
- 11992 [206] 3rd Generation Partnership Project. *Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; ANSI-C code*. S. Bruhn. [3GPP TS 26.204](#), December 2018.
- 11993 [207] Internet Engineering Task Force. *A Privacy Mechanism for the Session Initiation Protocol (SIP)*. J. Peterson. [RFC 3323](#), November 2002.
- 11994 [208] Internet Engineering Task Force. *P-Charge-Info: A Private Header Field (P-Header) Extension to the Session Initiation Protocol (SIP)*, D. York and T. Asversen. [RFC 8496](#), October 2018.
- 11995 [209] Internet Engineering Task Force. *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP*. R. Jesske, K. Drage, and C. Holmberg. et. al., [RFC 7315](#), July 2014.
- 11996 [210] Alliance for Telecommunications Industry Solutions and the SIP Forum. *Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)*. [ATIS-1000074-E](#). Washington, DC: ATIS, February 1, 2019.
- 11997 [211] Alliance for Telecommunications Industry Solutions and the SIP Forum. *Errata to ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, Joint Alliance for Telecommunications Industry Solutions*. [ATIS-1000080-E](#). Washington, DC: ATIS, approved February 27, 2019.
- 11998 [212] Internet Engineering Task Force. *Definition of the Opus Audio Codec*. JM. Valin, K. Voss, and T. Terriberry. [RFC 6716](#), September 2012.
- 11999 [213] Internet Engineering Task Force. *The Use of AES-192 and AES-256 in Secure RTP*. D. McGrew. [RFC 6188](#), March 2011.
- 12000 [214] Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner. [RFC 2119](#), March 1997.
- 12001 [215] Internet Engineering Task Force. *jCard: The JSON Format for vCard*. P. Kewisch. [RFC 7095](#), January 2014.
- 12002 [216] Internet Engfineering Task Force. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. D. Mills, J. Marin, J. Burbank, and W. Kasch. [RFC 5905](#), June 2010.
- 12003 [217] Internet Engineering Task Force. *Connection Reuse in the Session Initiation Protocol (SIP)*. V. Gurbani, R. Mahy, and B Tate. [RFC 5923](#), June 2010.

[MM/DD/YYYY]

Page 484 of 675



- 12027 [218] Internet Engineering Task Force. *Definition of the Differentiated Services Field (DS*
12028 *Field) in the IPv4 and IPv6 Headers.* K. Nichols, S. Blake, F. Baker, and D. Black. [RFC](#)
12029 [2474](#), December 1998.
- 12030 [219] Internet Engineering Task Force. *RTP-mixer formatting of multi-party Real-time text.*
12031 G. Hellström. [draft-ietf-avtcore-multi-party-rtt-mix](#).
- 12032 [220] Internet Engineering Task Force. *Serving Stale Data to Improve DNS Resiliency.* D.
12033 Lawrence and W. Kumari, [draft-ietf-dnsop-serve-stale-00](#). October 10, 2017.
- 12034 [221] Internet Engineering Task Force. *JSON Web Algorithms (JWA).* M. Jones, [RFC 7518](#).
12035 May, 2015.
- 12036 [222] Internet Assigned Numbers Authority (IANA). *Hypertext Transfer Protocol (HTTP)*
12037 *Status Code Registry.* [https://www.iana.org/assignments/http-status-codes/http-](https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml)
12038 [status-codes.xhtml](#), last updated 21 September 2018.
- 12039 [223] Internet Engineering Task Force. *Hypertext Transfer Protocol (HTTP/1.1): Semantics*
12040 *and Content.* R. Fielding, Ed. and J. Reschke, Ed. [RFC 7231](#), June 2014.
- 12041 [224] Internet Engineering Task Force. *The LoST-Validation S-NAPTR Application Service*
12042 *Tag.* R. Gellens and B. Rosen. [RFC 8917](#), October 2020.
- 12043 [225] Internet Engineering Task Force. *Non-interactive Emergency Calls.* B. Rosen, H.
12044 Schulzrinne, H. Tschofenig, and R. Gellens, [RFC 8876](#). September 2020.
- 12045 [226] 3rd Generation Partnership Project. *IP multimedia call control based on Session*
12046 *Initiation Protocol (SIP), Stage 3 (Release 17).* 3GPP. [3GPP TS 24.229](#), September
12047 25, 2020.
- 12048 [227] Internet Engineering Task Force. *Edwards-Curve Digital Signature Algorithm*
12049 *(EdDSA).* S. Josefsson and I. Liusvaara. [RFC 8032](#), January 2017.
- 12050 [228] Internet Engineering Task Force. *CFRG Elliptic Curve Diffie-Hellman (ECDH) and*
12051 *Signatures in JSON Object Signing and Encryption (JOSE).* I. Liusvaara. RFC 8032,
12052 January 2017.
- 12053 [229] Internet Engineering Task Force. *FYI on Questions and Answers – Answers to*
12054 *Commonly Asked "New Internet User" Questions.* R. Plzak, A. Wells, and A. Krol.
12055 [RFC 2664](#), August 1999.
- 12056 [230] National Emergency Number Association. *NENA Standard for the Implementation of*
12057 *the Wireless Emergency Service Protocol E2,* [NENA-STA-018.2 \(originally 05-001\)](#).
12058 Arlington, VA: NENA (forthcoming).
- 12059 [231] National Emergency Number Association. *NENA Security for Next-Generation 9-1-1*
12060 *Standard (NG-SEC),* [NENA 71-001](#). Arlington, VA: NENA, February 6, 2010.
- 12061 [232] National Emergency Number Association. "NENA Registry System". NRS
12062 Administrator. Updated September 30, 2020.
12063 http://technet.nena.org/nrs/registry/_registries.xml.

- 12064 [233] Internet Engineering Task Force. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. T. Mrugalski, M. Sidoleski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon and T. Winters. [RFC 8415](#), November 2018.
- 12065 [234] Internet Engineering Task Force. *Path MTU Discovery for IP version 6*. J. McCann, S. Deering, J. Mogul, and R. Hinden, Ed. [RFC 8201](#), July 2017.
- 12066 [235] Internet Engineering Task Force. *Internet Control Message Protocol (ICMPv6 for the Internet Protocol Version 6 (IPv6) Specification*. A. Conta, S. Deering, and M. Gupta, Ed. [RFC 4443](#), March 2006.
- 12067
- 12068
- 12069
- 12070
- 12071
- 12072

DRAFT

[MM/DD/YYYY]

Page 486 of 675



12073 **Appendix A - Mapping Between NG9-1-1 and Legacy ALI Data**
12074 **Structures (Informative)**

12075 The following tables illustrate approximately equivalent legacy data elements and
12076 PIDF-LO/Additional Data Elements. Exact mapping of fields between legacy formats and NG
12077 formats is complex because local field usage in legacy systems varies widely, while field
12078 usage in NG9-1-1 is standardized and uniform. The LNG must map legacy elements to SIP
12079 header fields, PIDF-LO parameters, or Additional Data Elements (NENA 02-010 Field Name
12080 maps to PIDF-LO and/or Additional Data) for use within the NG9-1-1 system. The LPG
12081 must map SIP header fields, PIDF-LO parameters, or Additional Data Elements to legacy
12082 elements (PIDF-LO and/or Additional Data map to NENA 02-010 Field Name) for display in
12083 legacy PSAPs. The format of Table A-12-1 that is used in the "Standard ALI Query Best
12084 Practices" may be found on NENA.org.

12085 **Note:** A future version of this document will further clarify how conversion between legacy
12086 formats and NG9-1-1 formats is accomplished.

NENA AQS Element	NG9-1-1 Mapping
<i>Call Info</i>	
CallBackNum	SIP INVITE/P-Asserted-Identity (P-A-I) ⁸² SIP INVITE/P-Preferred-Identity (P-P-I) for Non Service Initiated calls
CallingPartyNum (ANI)	SIP INVITE/P-Asserted-Identity (P-A-I) ⁷⁰
ClassOfService	Included in Additional Data and PIDF-LO. See Table A-12-2
TypeOfService	See Table A-12-3
SourceOfService	N/A
MainTelNum	EmergencyCallData.SubscriberInfo/SubscriberData/vcard/tel[n]/uri=tel : URI with MainTelNum expressed as a global number (i.e. starting with +1) AND EmergencyCallData:SubscriberInfo/ SubscriberData /vcard/tel[n]/parameters/type/text=main-number
CustomerName	EmergencyCallData:SubscriberInfo/ SubscriberData /vcard/fn/text= Full name of the customer
CustomerCode	N/A
AttentionIndicator	N/A
SpecialMessage	N/A

⁸² CBN and CPN are assumed to be mutually exclusive. For Legacy to i3, both map to P-A-I. For i3 to Legacy, map P-A-I to CPN.

NENA AQS Element	NG9-1-1 Mapping
AlsoRingsAtAddress	N/A
<i>Location Info: StreetAddress</i>	
HouseNum	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/HNO
HouseNumSuffix	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/HNS
PrefixDirectional	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PRD
StreetName	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/RD
StreetSuffix	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/STS
PostDirectional	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/POD
TextualAddress	N/A
MSAGCommunity	[Mapped via MCS] pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A3
PostalCommunity	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PCN
StateProvince	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A1
CountyID	[Mapped via MCS] pidflo:presence/tuple/status/geopriv/location-info/civicAddress/A2
Country	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/country
TARCode	[Mapped via MCS]
PostalZipCode	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/PC
Building	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/BLD
Floor	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/FLR
	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/UNIT
UnitNum	The UnitNum and UnitType are combined in a PIDF-LO Unit with a separator. Examples include "Apartment 6", "Silver Suite", and "Gate 5". A Unit Num without a Unit Type or vice versa (for example "Penthouse") can also occur.
UnitType	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/UNIT The UnitNum and UnitType are combined in a PIDF--LO Unit with a separator. Examples include "Apartment 6", "Silver Suite", and "Gate 5". A Unit Num without a Unit Type or vice versa (for example "Penthouse") can also occur.
LocationDescription	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC
LandmarkAddress	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LMK

NENA AQS Element	NG9-1-1 Mapping
<i>Location Info: Geo Location</i>	
Latitude	pidflo:presence/tuple/status/geopriv/location-info/Circle/gml:pos [latitude part] OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [latitude part]
Longitude	pidflo:presence/tuple/status/geopriv/location-info/Circle/gml:pos [longitude part] OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [longitude part]
Elevation	pidflo:presence/tuple/status/geopriv/location-info/Sphere/gml:pos [altitude part]
Datum	Datum must always be WGS84 (EPSG4326/EPSG4979). Entities receiving locations with any other datum must convert the locations. The GML object (point, circle, polygon, etc.) in a PIDF-LO carries the datum, but the PIDF-LO and NENA Standard restrict to WGS84 only.
Heading	pidflo:presence/tuple/status/geopriv/location-info/Dynamic/heading (RFC 5692) [146]
Speed (in KPH MPH)	pidflo:presence/tuple/status/geopriv10:/location-info/Dynamic/speed
PositionSource	See Table A-12-4 and Table A-12-5
Uncertainty	pidflo:presence/tuple/status/geopriv/location-info/Circle/radius OR pidflo:presence/tuple/status/geopriv/location-info/Sphere/radius uom="urn:ogc:def:uom:EPSG::9001"
Confidence	pidflo:presence/tuple/status/geopriv/location-info/confidence (RFC 7459) [145]
DateStamp Represents the time of the location fix	pidflo:presence/tuple/timestamp Represents the time the PIDF-LO status changed
LocationDescription	If this data field is encountered in the legacy-to-NG9-1-1 mapping, the ensued PIDF-LO would have to have a civic tuple added containing pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC
<i>Location Info:Cell Site</i>	
CellID	From SIP P-Access-Network-Info if passed (carrier-specific format)
SectorID	From SIP P-Access-Network-Info if passed (carrier-specific format)
LocationDescription	pidflo:presence/tuple/status/geopriv/location-info/civicAddress/LOC

NENA AQS Element	NG9-1-1 Mapping
<i>Location Info</i>	
Comment	EmergencyCallData.Comment/Comment xml:lang= free text and associated language used
<i>Agencies:Police</i>	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.police If derivable from the name, append with the appropriate value from the registry (Section 10.6)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
<i>Agencies:Fire</i>	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.fire If derivable from the name, append with the appropriate value from the registry (Section 10.8)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
<i>Agencies:EMS</i>	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.ems If derivable from the name, append with the appropriate value from the registry (Section 10.9)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
<i>Agencies:OtherAgencies</i>	From ECRF
Name	LoST:findServiceResponse/mapping/displayName AND LoST:findServiceResponse/mapping/service=urn:emergency:service:responder.agency Replace "agency" with appropriate value from the registry (10.5)
TN	LoST:findServiceResponse/mapping/uri=tel: URI with TN expressed as a global number (i.e. starting with +1)
<i>Agencies</i>	
AdditionalInfo	N/A

NENA AQS Element	NG9-1-1 Mapping
ESN	Mapped from PIDF-LO via MCS
SourceInfo: DataProvider	
DataProviderID	EmergencyCallData.ProviderInfo/ProviderID
TN	EmergencyCallData.ProviderInfo/ContactURI in the form of a tel: URI expressed as a global number (i.e. starting with +1)
Name	EmergencyCallData.ProviderInfo/DataProviderString
	Type: EmergencyCallData.ProviderInfo/TypeOfProvider
SourceInfo: AccessProvider	Map when type is EmergencyCallData.ProviderInfo/TypeOfProvider=Access Network Provider
AccessProviderID	EmergencyCallData.ProviderInfo/ProviderID
TN	EmergencyCallData.ProviderInfo/ContactURI in the form of a tel: URI expressed as a global number (i.e. starting with +1)
Name	EmergencyCallData.ProviderInfo/DataProviderString
SourceInfo	
ALIUpdateGMT	N/A
ALIRetrieveGMT	N/A
GeneralUses	Vendor specific mapping
NetworkInfo	
PSAPALIHost	N/A
ResponseALIHost	N/A
PSAPID	N/A
PSAPName	N/A
RouterID	N/A
Exchange	N/A
CLLI	N/A

12087

12088

Table A-12-1 Data Element Mapping

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
1	Residence	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed

[MM/DD/YYYY]

Page 491 of 675



Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
2	Business	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
3	Residence PBX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-local and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
4	Business PBX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-local and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
5	Centrex	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=MLTS-hosted and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
6	Coin 1 way out	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=coin;one-way and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
7	Coin 2 way	pidflo:presence/ tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
8	Wireless Phase 0	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility =Mobile
9	Residence OPX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS;OPX and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
0	Business OPX	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=POTS;OPX and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
A	Customer owned Coin	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=Coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Fixed
B	Not Available	N/A

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
C	VoIP Residence	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ and EmergencyCallData.ServiceInfo/ServiceEnvironment=Residence and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown ⁸⁴
D	VoIP Business	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown ⁸⁴
E	VoIP Coin or Pay Phone	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ ;coin and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown ⁸⁴
F	VoIP Wireless	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ ;wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
J	VoIP Nomadic	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ and EmergencyCallData.ServiceInfo/ServiceMobility=Nomadic

⁸³ If the type of VoIP provider is known, and the VoIP provider is also the Access Infrastructure Provider (AIP) then use “digital”, otherwise use “OTT”. If the VoIP service is not known, use “digital” for all VoIP types except “J”, “VoIP Nomadic”.

⁸⁴ If the type of service mobility is known, use the correct value, otherwise “Unknown”.

Legacy CoS Code	Legacy Value	NG9-1-1 Data Structure
K	VoIP Enterprise	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ and EmergencyCallData.ServiceInfo/ServiceEnvironment=Business and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown ⁸⁴
G	Wireless Phase I	pidflo:presence/tuple/status/geopriv/method=Cell and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
H	Wireless Phase II	pidflo:presence/tuple/status/geopriv/method= (See Table A-12-4 and Table A-12-5 LTY to i3 Mapping) and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
I	Wireless Phase II returning Phase I	pidflo:presence/tuple/status/geopriv/method=Cell and EmergencyCallData.ServiceInfo/ServiceType=wireless and EmergencyCallData.ServiceInfo/ServiceMobility=Mobile
V	Voice Over IP	pidflo:presence/tuple/status/geopriv/method=Manual and EmergencyCallData.ServiceInfo/ServiceType=OTT or digital ⁸³ and EmergencyCallData.ServiceInfo/ServiceMobility=Unknown ⁸⁴

12089

12090

12091

Table A-12-2 Class of Service Mapping

TYS Codes	TYS Values	NG9-1-1 Data Structure
0	Not FX nor Non-Published	Normal SIP header field use
1	FX in 911 serving area	treat as TYS=0
2	FX outside 911 serving area	treat as TYS=0
3	Non-Published	Privacy Header per RFC 3323 [207]

[MM/DD/YYYY]

Page 495 of 675



TYS Codes	TYS Values	NG9-1-1 Data Structure
4	Non-Published FX in 911 serving area	treat as TYS=3
5	Non-Published FX outside 911 serving area	treat as TYS=3
6	Local Ported Number (LNP)	N/A
7	Interim Ported Number	N/A
8	PSALI Published	treat as TYS=0
9	PSALI Non-Published	treat as TYS=3

12092

Table A-12-3 Type of Service Mapping

12093 Clarifications on Table A-12-3: Legacy TYS values map to NG9-1-1 values as shown in the
12094 Table. For NG9-1-1 to Legacy TYS mapping, the absence of privacy indication maps to
12095 TYS=0 and the use of privacy maps to TYS=3.

12096

Value	Name	PIDF-LO Mapping
0	unknown	Method not included in PIDF-LO
1	networkUnspecified	Method not included in PIDF-LO
2	networkAOA	pidflo:presence/tuple/status/geopriv/method=AOA
3	networkTOA	pidflo:presence/tuple/status/geopriv/method=networkTOA
4	networkTDOA	pidflo:presence/tuple/status/geopriv/method=networkTDOA
5	networkRFFingerprinting	pidflo:presence/tuple/status/geopriv/method=networkRFFingerprinting
6	networkCellSector	pidflo:presence/tuple/status/geopriv/method=Cell
7	networkCellSectorwithTiming	pidflo:presence/tuple/status/geopriv/method=TA
16	handsetUnspecified	Method not included in PIDF-LO
17	handsetGPS	pidflo:presence/tuple/status/geopriv/method=GPS
18	handsetAGPS	pidflo:presence/tuple/status/geopriv/method=Device-Assisted_A-GPS
19	handsetEOTD	pidflo:presence/tuple/status/geopriv/method=Device-Assisted_EOTD
20	handsetAFLT	pidflo:presence/tuple/status/geopriv/method=Handset_AFLT
21	handsetEFLT	pidflo:presence/tuple/status/geopriv/method=Handset_EFLT

[MM/DD/YYYY]

Page 496 of 675



Value	Name	PIDF-LO Mapping
22	handsetGNSS	pidflo:presence/tuple/status/geopriv/method=GNSS
23	handsetAGNSS	pidflo:presence/tuple/status/geopriv/method=A-GNSS
24	handsetOTDOA	pidflo:presence/tuple/status/geopriv/method=OTDOA
25	handsetTBS	pidflo:presence/tuple/status/geopriv/method=MBS
26	handsetWi-Fi	pidflo:presence/tuple/status/geopriv/method=Handset_WiFi ⁸⁵
27	handsetBluetooth	pidflo:presence/tuple/status/geopriv/method=Handset_BLE ⁸⁵
32	hybridUnspecified	Method not included in PIDF-LO
33	hybridAGPS_AFLT	pidflo:presence/tuple/status/geopriv/method=hybridAGPS_AFLT
34	hybridCellSector_AFLT	pidflo:presence/tuple/status/geopriv/method=hybridCellSector_AFLT ⁸⁵
35	hybridNetworkTDOA_AOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AOA
36	hybridNetworkTDOA_AGPS	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS
37	hybridTDOA_AGPS_AOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS_AOA
38	hybridAGPS_OTDOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_AGPS
39	hybridAGNSS_OTDOA	pidflo:presence/tuple/status/geopriv/method=hybridTDOA_A-GNSS ⁸⁵
40	hybridDeviceBased	pidflo:presence/tuple/status/geopriv/method=DBH
41	hybridAGPS_RFPatternMatch	pidflo:presence/tuple/status/geopriv/method=hybridRFPatternMatch_AGPS ⁸⁵
42	hybridAGPS_Wi-Fi	pidflo:presence/tuple/status/geopriv/method=hybridWiFi_AGPS ⁸⁵
48	cosUnspecified	Method not included in PIDF-LO
49	cosWRLS	pidflo:presence/tuple/status/geopriv/method=Cell Some local variations exist where phase 0 (Manual) is appropriate

⁸⁵ Submit method to IANA Method Token Registry.

Value	Name	PIDF-LO Mapping
50	cosWPH1	pidflo:presence/tuple/status/geopriv/method=Cell
51	cosWPH2	Method not included in PIDF-LO
52	cosTEXT	Method not included in PIDF-LO
53	cosFIXD	Method not included in PIDF-LO
54	cosRESD	Method not included in PIDF-LO
55	cosWCVC	Method not included in PIDF-LO
56	cosWDL1	Method not included in PIDF-LO
57	cosWDL2	Method not included in PIDF-LO

12097

Table A-12-4 LNG Mapping for Position Source – E2 to PIDF-LO

12098

Note on Table A-12-4: Mappings have been added in this version for newly designated position sources as found in the NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2, NENA-STA-018.2 (originally 05-001) [230].

12100

Token	PIDF-LO Mapping
CELL	pidflo:presence/tuple/status/geopriv/method=Cell
OTDOA	pidflo:presence/tuple/status/geopriv/method=OTDOA
GPS	pidflo:presence/tuple/status/geopriv/method=GPS
A-GPS	pidflo:presence/tuple/status/geopriv/method=A-GPS
GNSS	pidflo:presence/tuple/status/geopriv/method=GNSS
A-GNSS	pidflo:presence/tuple/status/geopriv/method=A-GNSS
E-OTD	pidflo:presence/tuple/status/geopriv/method=Device-Assisted_EOTD
U-TDOA	pidflo:presence/tuple/status/geopriv/method=UTDOA
AFLT	pidflo:presence/tuple/status/geopriv/method=Handset_AFLT
EFLT	pidflo:presence/tuple/status/geopriv/method=Handset_EFLT
E-CID	pidflo:presence/tuple/status/geopriv/method=E-CID
UNKNOWN	Method not included in PIDF-LO
OTHER	Method not included in PIDF-LO

12101

Table A-12-5 LNG Mapping for Position Method – MLP to PIDF-LO

12102

12103

12104

[MM/DD/YYYY]

Page 498 of 675



12105 **Appendix B – SI Provisioning Data Model (Normative)**

12106 The model defined in the Appendix represents the data to be incorporated in an XML
12107 schema that defines the SI. It may not represent data actually stored in the GIS system
12108 but it represents the data that is required by the ECRF, the LVF, the Mapping Data Service
12109 (MDS), the Geospatial Conversion Service and the MSAG Conversion Service (MCS) to
12110 perform their functions adequately and consistently. This data format is aligned with the
12111 NG GIS Data format [184] in that it is possible to convert from the format described in NG
12112 GIS to this format, or vice versa, algorithmically, without manual intervention. This format
12113 uses "related tables" where data such as the name of a street appears once in a
12114 CompleteStreetName table, the StreetSegment table has an index into the
12115 CompleteStreetName table and the Centerline table has an index into the StreetSegment
12116 table for each road segment.

12117 Attribute names and descriptions are drawn from CLDXF [77] when appropriate. Any
12118 difference between the definition of fields other than right/left and similar variances
12119 between this model and CLDXF are resolved in favor of the CLDXF definition. When
12120 provisioning data for an ECRF and LVF through the SI, a 9-1-1 Authority (or 9-1-1 Authority
12121 designee) MUST only include GIS data for their geographic area of responsibility and MUST
12122 ensure the data includes coverage for the entire extent of that area.

12123 The "Use M/C/O" column contains the following values:

- 12124 • "M" = Mandatory, a value MUST be provided.
- 12125 • "C" = Conditional, a value MUST be provided if the listed condition is met, otherwise
12126 optional.
- 12127 • "O" = Optional, a value MAY be provided.

12128 Since the SI uses XML data structures, elements that are Mandatory have "minoccurs=1",
12129 while elements that are Conditional or Optional have "minoccurs=0".

12130 The "Type" column contains the following values:

- 12131 • A: Represents upper/lower case alphabetic characters only, plus the space character
12132 (ASCII decimal code 32).
- 12133 • N: Represents non-negative integers (whole numbers only).
- 12134 • AN: Represents upper/lower alphabetic characters plus non-negative integers (i.e.,
12135 alphanumeric characters)
- 12136 • P: Printable ASCII characters (decimal codes 32 to 126).
- 12137 • E: UTF-8 restricted to character sets designated by the 9-1-1 Authority, but not
12138 including pictographic characters
- 12139 • U: Represents characters allowed in a URI (see RFC 3986) [126].
- 12140 • D: Represents a Date field. Represented as a Timestamp as defined in Section 2.3.

12141 • C: Represents a complex data object.

12142 B.1 Centerlines

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that supplies the data, and is the agency that receives a Discrepancy Report (DR) should a discrepancy be discovered.
Data Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique ID	M	P	Unique ID for each Road Segment, with domain of agency included. The IDs MUST not be re-used when a road is split or deleted. Example: GHC123@houston.eoc.tx
Country Left	M	A	The name of a country on the left side of where the road is located, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital letters as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
Country Right	M	A	The name of a country on the right side of where the road is located, represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital letters as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State Left	M	A	The name of a state, province, or equivalent on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
State Right	M	A	The name of a state, province, or equivalent on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX

[MM/DD/YYYY]

Page 500 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
County Left ¹	C	P	The name of county or county-equivalent on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. Must be provided where there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris
County Right ¹	C	P	The name of county or county-equivalent on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. Must be provided where there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris
AdditionalCodeLeft	C	P	A code that specifies the geographic area on the left side of where the road is located. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
AdditionalCodeRight	C	P	A code that specifies the geographic area on the right side of where the road is located. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality Left	M	E	The name of the incorporated municipality or other general-purpose local governmental unit (if any) on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Incorporated Municipality Right	M	E	The name of the incorporated municipality or other general-purpose local governmental unit (if any) on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community Right	C	E	The name of an unincorporated community, on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139 [53]). MUST be provided if Incorporated Municipality Right contains "Unincorporated".
Unincorporated Community Left	C	E	The name of an unincorporated community, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53]). MUST be provided if Incorporated Municipality Left contains "Unincorporated".
Neighborhood Community Right	O	E	The name of an unincorporated neighborhood, subdivision, or area, on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Neighborhood Community Left	O	E	The name of an unincorporated neighborhood, subdivision, or area, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Street Segment	M	C	StreetSegment.
Alias Street Segment	O	C	StreetSegment aliases. MAY occur more than once.
Road Class	M	A	Road classes as specified in MAF/TIGER Feature Classification Codes (MTFCC) Attachment D, Series S. Examples: Primary, Secondary, Local, Ramp, Service, Vehicular Trail, Walkway, Alley, Private, Parking Lot, Trail, Other.

[MM/DD/YYYY]

Page 502 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
One-way	M	A	<p>One-way road classification</p> <ul style="list-style-type: none"> • B or blank – travel in both directions • FT – One-way from FROM node to TO node (in direction of arc); • TF – One way from TO node to FROM Node (opposite direction of arc)
Speed Limit	O	N	Normal Posted Speed in MPH if country is US or KPH if country is Canada
Speed Limit Unit	C	A	MPH or KPH. MUST be provided if Speed Limit is provided.
Postal Community Name Left	C	A	A city name for the postal code of an address, as determined by the postal authority, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent. (PCN in RFC 5139 [53]). MUST be populated if a Postal Code is assigned.
Postal Community Name Right	C	A	A city name for the postal code of an address, as determined by the postal authority on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (PCN in RFC 5139 [53]). MUST be populated if a Postal Code is assigned.
Postal Code Left ²	C	A	Postal Code, on the left side of where the road is located, as specified in CLDXF or its Canadian equivalent (PC in RFC 5139 [53]). MUST be populated if a Postal Code is assigned. Does not include ZIP+4 code.
Postal Code Right ²	C	A	Postal Code on the right side of where the road is located, as specified in CLDXF or its Canadian equivalent (PC in RFC 5139 [53]). MUST be populated if a Postal Code is assigned. Does not include ZIP+4 code.
MSAG Left	C	C	Unique ID of corresponding entry associated with the Left side of the street in MSAG table. Provided for E9-1-1 and if needed for transition.

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
MSAG Right	C	C	Unique ID of corresponding entry associated with the Left side of the street in MSAG table. Provided for E9-1-1 and if needed for transition.

12143 **B.2 Street/Address Structures**

12144 **B.2.1 CompleteStreetName**

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Street Name Pre Modifier	O	E	A street pre-modifier as specified in CLDXF or its Canadian equivalent. (PRM in RFC 5139 [53]). Examples: Alternate, Business, Bypass, Extended, Historic, Loop, Old, Private, Public, Spur, etc.
Street Name Pre Directional	O	A	A street name pre-directional as specified in CLDXF or its Canadian equivalent. (PRD in RFC 5139 [53])
Street Name Pre Type	O	E	A street name pre-type as specified in CLDXF or its Canadian equivalent. (STP in RFC 6848 [115])
Street Name Pre Type Separator	O	E	A preposition or prepositional phrase between the Street Name Pre Type and the Street Name as specified in CLDXF or its Canadian equivalent. Example: "of the" in "Boulevard of the Allies".
Street Name	M	E	The street name as specified in CLDXF or its Canadian equivalent. (RD in RFC 5139 [53])
Street Name Post Type	O	E	The street name post type as specified in CLDXF or its Canadian equivalent. (STS in RFC 5139 [53])
Street Name Post Directional	O	A	The street name post directional as specified in CLDXF or its Canadian equivalent. (POD in RFC 5139 [53])

[MM/DD/YYYY]

Page 504 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Street Name Post Modifier	O	E	The street name post modifier as specified in CLDXF or its Canadian equivalent. (POM in RFC 5139 [53]) Examples: Access, Alternate, Business, Bypass, Connector, Extended, Extension, Loop, Private, Public, Scenic, Spur, Ramp, Underpass, Overpass.

12145

12146 B.2.2 CompleteAddressNumber

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Address Number Prefix	O	P	The address number prefix as specified in CLDXF or its Canadian equivalent. (HNP in RFC 6848 [115])
Address Number	M	N	The Address Number as specified in CLDXF or its Canadian equivalent. (HNO in RFC 5139 [53])
Address Number Suffix	O	P	The Address Number Suffix as specified in CLDXF or its Canadian equivalent.

12147 B.2.3 StreetSegment

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Street Name	M	C	CompleteStreetName.
Left Address Number Prefix	O	P	An Address Number Prefix as specified in CLDXF or its Canadian equivalent, applying to all address numbers on the left side of the road in the segment.
Left From Address Number	M	N	The address number (as specified in CLDXF or its Canadian equivalent) on the Left side of the road, which corresponds to the left side of the "FROM Node" of the arc segment. It is quite possible that this address is higher than the left "TO Node". Example: 399

[MM/DD/YYYY]

Page 505 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Left To Address Number	M	N	The address number (as specified in CLDXF or its Canadian equivalent) on the Left side of the road, which corresponds to the left side of the "TO Node" of the arc segment. It is quite possible that this address is lower than the left "From Address". Example: 199
Parity Left	M	A	A single character code that explicitly defines the allowable addresses on the Left side of the road. Valid values include "O", "E", "B", "Z" for odd, even, both, or zero range, respectively.
Left Address Number Suffix	O	P	An Address Number Suffix, as specified in CLDXF or its Canadian equivalent, applying to all address numbers on the left side of the road in a segment.
Validation Left	O	A	TRUE if any Address Number in the range is valid for the left side of the road. FALSE if Address Number must occur in another layer (e.g., Site/Structure) to be valid. If not present, true is assumed.
Right Address Number Prefix	O	P	Like Left Address Number Prefix, but applying to the right side of the road.
Right From Address Number	M	N	Like Left From Address, but applying to the right side of the road.
Right To Address Number	M	N	Like Left To Address, but applying to the right side of the road.
Parity Right	M	A	Like Parity Left, but applying to the right side of the road.
Right Address Number Suffix	O	P	Like Left Address Number Suffix, but applying to the right side of the road.
Validation Right	O	A	Like Validation Left, but applying to the right side of the road.

12148 B.2.4 CompleteAddress

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Street Name	M	C	CompleteStreetName.

[MM/DD/YYYY]

Page 506 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Complete Address Number	C	C	CompleteAddressNumber. If Milepost is provided, Complete Address Number is optional, otherwise it is required.
Milepost	O	P	Milepost as specified in CLDXF or its Canadian equivalent (MP in RFC 6848) [115]

12149

B.3 Site/Structure

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID, (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The 2--character abbreviation of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as described in CLDXF or its Canadian equivalent (A2 in RFC 5139 [53]). MUST be provided where there is a county or county equivalent. (A2 in RFC 5139 [53]) Example: Harris

[MM/DD/YYYY]

Page 507 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
AdditionalCode ¹	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent ³ . Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated" (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	C	E	The name of an unincorporated community, division, or area, as specified in CLDXF or its Canadian equivalent (A4 in RFC 5139 [53]). If Incorporated Municipality contains "Unincorporated", it MUST be provided, otherwise OPTIONAL.
Neighborhood Community	O	E	The name of an unincorporated neighborhood, subdivision, or area, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
Address	C	C	CompleteAddress. MUST be present unless Complete Landmark Name is populated.
Alias Address	O	C	CompleteAddress aliases. MAY occur more than once.
Postal Community Name	C	A	A city name for the postal code of an address, as determined by the postal authority, as specified in CLDXF or its Canadian equivalent. (PCN in RFC 5139 [53]). MUST be populated if there is an assigned postal code.
Postal Code ²	C	A	Postal code (PC in RFC 5139 [53]). MUST be populated if there is an assigned postal code. Does not contain the ZIP+4 code. Examples: 05421, G1R 1M9
Postal Code Extension	O	P	Contains the ZIP+4 code or equivalent.

[MM/DD/YYYY]

Page 508 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Building	O	E	The name of a building as specified in CLDXF or its Canadian equivalent. (BLD in RFC 5139 [53]) Examples: DuPont Hotel, Shiloh Church, Tower B
Floor	O	P	A floor, story, or level within a building as specified in CLDXF or its Canadian equivalent. (FLR in RFC 5139 [53])
Unit	O	P	A group or suite of rooms within a building that are under common ownership or tenancy, typically having a common primary entrance, as specified in CLDXF or its Canadian equivalent. (UNIT in RFC 5139 [53]) Examples: Apartment 101, Suite 233-A
Room	O	P	A single room within a building or unit as specified in CLDXF or its Canadian equivalent. (ROOM in RFC 5139 [53]) Examples: Bedroom, Exam Room 3, Ballroom
Seat	O	P	A place where a person might sit within a room as specified in CLDXF or its Canadian equivalent. (SEAT in RFC 5139 [53]) Examples: Seat 35A, Cubicle 1A213
Complete Landmark Name	O	E	The complete name by which a prominent feature is publicly known as specified in CLDXF or its Canadian equivalent. (LMK in RFC 5139 [53])
Landmark Name Part	C	E	A part of the name by which a prominent feature is publicly known as specified in CLDXF or its Canadian equivalent (LMKP the NENA extension to PIDF-LO). MUST be populated if Complete Street Name is not provided, otherwise OPTIONAL.
Additional Location Information	O	E	A part of a subaddress that is not a building, floor, unit, room, or seat as specified in CLDXF or its Canadian equivalent. (LOC in RFC 5139 [53])

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Place-Type	O	AN	Type of place as specified in CLDXF or its Canadian equivalent. (PLC in RFC 5139 [53]) Examples: office, store, school, residential
AdditionalDataURI	O	U	URI of Additional Data for this site/structure. MAY occur more than once.
MSAG	C	P	Unique ID of corresponding entry in MSAG table. Provided for E9-1-1 and if needed for transition.
MSAG Street Exception	O	P	Unique ID of corresponding entry in MSAG table

12150

B.4 State Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX

[MM/DD/YYYY]

Page 510 of 675



12151

B.5 County Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	M	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) Example: Harris

12152

B.6 Incorporated Municipality Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.

[MM/DD/YYYY]

Page 511 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]). MAY be omitted if the boundary straddles more than one county. Example: Harris
AdditionalCode ¹	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago

12153

B.7 Unincorporated Community Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.

[MM/DD/YYYY]

Page 512 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]). MAY be omitted if the boundary straddles more than one county. Example: Harris
AdditionalCode ¹	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned, but MAY be omitted if boundary straddles more than one Additional Code.
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	M	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])

[MM/DD/YYYY]

Page 513 of 675



12154

B.8 Neighborhood Community Boundary

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update as a Timestamp
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	M	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US
State	M	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	C	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) MAY be omitted if the boundary straddles more than one county. Example: Harris
AdditionalCode ¹	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned, but MAY be omitted if boundary straddles more than one Additional Code.

[MM/DD/YYYY]

Page 514 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Incorporated Municipality	M	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	O	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])
Neighborhood Community	M	E	The name of the Neighborhood, as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])

12155

12156 B.9 Service Boundary

12157 Most of the Country/State/Municipality fields are optional, since they are not needed, and
12158 boundaries may straddle more than one of those fields.

12159

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Country	O	A	The name of a country represented by its two-letter ISO 3166-1 English country alpha-2 code elements in capital ASCII letters, as specified in CLDXF or its Canadian equivalent. (country in RFC 5139 [53]) Example: US

[MM/DD/YYYY]

Page 515 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
State	O	A	The name of a state, province, or equivalent, as specified in CLDXF or its Canadian equivalent. (A1 in RFC 5139 [53]) Example: TX
County	O	P	The name of county or county-equivalent as specified in CLDXF or its Canadian equivalent. (A2 in RFC 5139 [53]) Example: Harris
AdditionalCode ¹	O	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties.
Incorporated Municipality	O	E	The name of the incorporated municipality or other general-purpose local governmental unit as specified in CLDXF or its Canadian equivalent. Populate a name of incorporated municipality if it exists, otherwise enter "Unincorporated". (A3 in RFC 5139 [53]) Example: Chicago
Unincorporated Community	O	E	The name of an unincorporated community, as specified in CLDXF or its Canadian equivalent. (A4 in RFC 5139 [53])
Neighborhood Community	O	E	Neighborhood or other informal designation for a part of a community as specified in CLDXF or its Canadian equivalent. (A5 in RFC 5139 [53])
AgencyId	M	U	Unique FQDN for the Service.
ServiceResponse	M	C	Service supplied for this boundary. MAY occur more than once.

12160 **B.9.1 Service Response**

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Service URI	M	U	URI for Routing. Example: sip:sos@psap.columbus.oh.us

[MM/DD/YYYY]

Page 516 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Service URN	M	U	The URN/URL for the Emergency Service or other Well-Known Service (e.g., "urn:service:sos" for a PSAP or "urn:service:sos.ambulance" for an ambulance service). Per RFC 5031 [45]
Service Number	O	P	The emergency services number appropriate for the location provided in the query. "911" is assumed if not provided.
Agency vCard URI	M	U	URI for the vCARD of contact information.
Display Name	M	P	Display Name of the Service. Example: Houston FD

12161 **B.10 MSAG**

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of the last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Prefix Directional	O	P	Leading street direction prefix.
Street Name	M	E	Street Name.
Street Suffix	O	E	Street Type.
Post Directional	O	P	Trailing street direction suffix.
MSAG Community Name	M	P	Service community name.
County ID	O	P	County Identifier.
AdditionalCode ¹	C	P	A code that specifies the geographic area. Used in Canada to hold a Standard Geographical Classification code, which differentiates two municipalities with the same name in a province that does not have counties. MUST be provided if assigned.
State/Province	M	P	State or Province.

[MM/DD/YYYY]

Page 517 of 675



ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
ESN	C	N	Emergency Service Number, MUST be provided if any LPGs or egress LSRGs exist in the ESInet or other legacy systems that require an ESN remain.

12162 **B.10.1 MSAG Street Number Exception**

ATTRIBUTE NAME	USE M/C/O	TYPE	DATA DESCRIPTION
Discrepancy Agency ID	M	U	Agency that last updated the record – Agency ID (e.g., the FQDN of the 9-1-1 Authority).
Date Updated	M	D	Date of last update, as a Timestamp.
Effective Date	O	D	Date the new layer information goes into effect, as a Timestamp.
Expiration Date	O	D	Date this feature is no longer effective, as a Timestamp.
Unique_ID	M	P	Unique ID for each record.
Street Number	M	P	Street Number as found in MSAG.
Street Number Suffix	O	P	Street Number Suffix as found in MSAG.
ESN	O	P	Emergency Service Number associated with this House Number, Street Name, and Community Name.

12163 ¹ In Canada, there may not be counties in some areas, but in a given province, there can be two municipalities with the same name. Where there is no county, and there is name collision in the Municipality or MSAG Community name, a code may be placed in this field to differentiate the instances.

12167 ² The USPS considers ZIP codes to be delivery points instead of areas. There may be differences between this depiction and actual ZIP code mailing address.

12169 ³ Used in legacy systems and in transition. Not used in a full i3 implementation.

12170 **Appendix C – Support for PSAP Call Control Features (Normative)**

12171 PSAP Call Control Features allow a Public Safety Answering Point (PSAP) to prevent a call
12172 from being taken down when an emergency caller attempts to disconnect, and also allow
12173 the PSAP attendant, after being signaled that the caller attempted to disconnect, to invite
12174 an emergency caller to rejoin a conversation by providing alerting to the caller. These
12175 features are currently offered as part of emergency services deployments in North America
12176 and around the world, and some jurisdictions even mandate the availability of some of
12177 these features.

12178 While support of PSAP Call Control Features is not a required component of all i3
12179 implementations, this Appendix describes the procedures necessary to support PSAP Call
12180 Control Features in those networks in which such capabilities are desired or required. This
12181 appendix assumes that PSAPs and originating networks know when they are operating in
12182 an environment in which PSAP Call Control Features are supported. The set of features that
12183 are referred to collectively as PSAP Call Control. Features consist of: Called Party Hold
12184 (CPH)⁸⁶, Enhanced Called Party Hold (ECPH), Switch-hook Status, and on/off-hook
12185 Ringback.

12186 Functional Elements defined in this document that are involved in emergency calls
12187 supporting PSAP Call Control Features MUST comply with the requirements set forth in this
12188 Appendix. This includes MANDATORY support of the SDP “a” attribute values “suspended”
12189 and media feature tag “urn:emergency:media-feature.psap-call-control” for Functional
12190 Elements on the call path and processing SDP in call scenarios in which these are used.

12191 **C.1 Assumptions Regarding Behavior in the Originating Network**

12192 This document does not place any specific requirements on originating networks, however
12193 the procedures in this Appendix are based on a set of assumptions regarding the signaling
12194 generated by a legacy or SIP-based originating network toward an i3 ESIet/NGCS in
12195 support of PSAP Call Control Features. The text in this section describes these assumptions
12196 so that the reader will better understand the procedures associated with i3 Functional
12197 Elements and PSAPs that are normatively described in subsequent sections of this
12198 Appendix.

86 Also referred as “Calling Party Hold”, “Bureau Hold”, “Network Hold”, “Connection Hold”, “Originator Hold”, “Caller Hold”, “Emergency Calling Service Call Hold”, and “Forced Hold”.

12199 **C.1.1 Assumed Behavior in a Legacy Originating Network**

12200 **C.1.1.1 SS7 Signaling from Originating End Office**

12201 If Called Party Hold/Switch-hook Status is supported in a legacy originating network that
12202 uses outgoing SS7-supported trunks from the originating end office for emergency calls, it
12203 is assumed that the originating network will signal the availability of the Called Party Hold
12204 feature by generating an SS7 Initial Address Message (IAM) that contains a Service
12205 Activation Parameter (SAP) with a Feature Code Indicator (FCI) set to "hold available", as
12206 described in ATIS-1000628.a.2001(2010) [136] and ATI_-1000666.1999 (2014) [91]. If
12207 connection hold is desired/required for the call, the originating network expects to receive
12208 a SAP parameter with an FCI set to "hold request" in an SS7 Address Complete Message
12209 (ACM) (or SS7 Facility [FAC] message if an ACM has already been received for that circuit).
12210 If Called Party Hold is active for an emergency call, and the emergency caller attempts to
12211 disconnect from the call, the legacy originating switch will generate an SS7 FAC message
12212 that contains a SAP with an FCI indicating "disconnect request". In response to this FAC
12213 message, the legacy originating switch will either receive periodic SS7 FAC messages that
12214 contain a SAP with an FCI set to "hold continuation request" (if the PSAP wishes to
12215 maintain the existing connection) or an SS7 Release (REL) message (if the PSAP wishes to
12216 release the connection).

12217 If the emergency caller goes off-hook after the "disconnect request" has been sent, and an
12218 SS7 REL has not yet been received, the legacy originating switch will generate an SS7 FAC
12219 message that contains a SAP with an FCI indicating "reconnect request".

12220 The procedures described above are also expected from originating networks supporting
12221 Enhanced Called Party Hold. Note that Enhanced Called Party Hold requires the addition of
12222 an ECPH timer⁸⁷ downstream from the originating network. When the ECPH timer expires
12223 prior to the call being answered at the PSAP, the legacy originating switch may receive an
12224 SS7 FAC message containing a SAP with an FCI indicating "hold release request".

12225 When the Ringback feature is invoked by the PSAP attendant on a held connection in an
12226 originating network that supports PSAP Call Control features and call delivery via SS7-
12227 controlled trunk groups, it is expected that the originating network will be capable of
12228 receiving and processing an SS7 FAC message that contains an FCI indicating "Ringback
12229 request" and will apply the appropriate treatment towards the caller depending on the call
12230 state (ringing for on-hook, or Receiver-Off-Hook [ROH], also known as "howler" tone, for

⁸⁷ The ECPH timer controls the time ECPH is active for a given 9-1-1 call. In legacy implementations, it is a configurable parameter typically set in the range of a few tens of seconds to a few minutes after call initiation.

12231 off-hook). In this scenario, the originating network is expected to supply audible ringing
12232 back towards the PSAP.

12233 **C.1.1.2 MF Signaling from Originating End Office**

12234 If Called Party Hold/Switch-hook Status is supported in a legacy originating network that
12235 uses outgoing MF trunk groups from the originating end office for emergency calls, then
12236 upon receiving an off-hook signal from the caller followed by the digits "911", the end
12237 office will seize an outgoing trunk to a Legacy Network Gateway (LNG). When the
12238 originating end office receives a wink back from the LNG, the end office will outpulse the
12239 called number (i.e., KP + 911 + ST), and will wait for an ANI request signal. Upon
12240 receiving the ANI request signal, the end office will outpulse the ANI sequence using CAMA
12241 (I + 7-digit ANI) or Feature Group D operator-type (II + 7/10-digit ANI) MF signaling.
12242 While the PSAP is being alerted, audible ringing will be delivered to the caller. When the
12243 PSAP answers the call, an answer ("off-hook") signal will be delivered to the originating
12244 end office.

12245 If an emergency caller subsequently goes on-hook, an on-hook signal will be sent forward
12246 by the originating switch. Feature-specific processing of the MF signals generated by the
12247 end office will be applied by downstream elements based on trunk group provisioning.
12248 Since Called Party Hold/Switch-hook Status is supported by the legacy originating switch,
12249 the connection to the LNG is expected to be maintained.

12250 If the caller subsequently goes off-hook, an off-hook signal will be sent forward, and the
12251 behavior of downstream elements will be determined based on provisioning associated with
12252 the outgoing MF trunk group.

12253 If the Ringback feature is invoked by the PSAP attendant on a held connection in an
12254 originating network that supports MF trunking out of the end office, it is expected that the
12255 originating network will pass the appropriate treatment, as applied by the downstream
12256 element (in this case the LNG), through towards the caller as follows: If an off-hook
12257 Ringback is invoked by a PSAP attendant on an established connection, the originating
12258 network is expected to pass the appropriate treatment (e.g., ROH/howler tone), as applied
12259 by the LNG, through to the caller. If the on-hook Ringback feature is invoked by the PSAP
12260 attendant on a held connection to an LNG associated with an emergency call that was
12261 delivered via an MF trunk group out of the end office, it is expected that normal ringing will
12262 be used to alert the caller to the Ringback attempt. As described in Section C.4.4.2, the PIF
12263 component of the LNG will also return a SIP 180 Ringing message to the NIF component in
12264 response to an incoming re-INVITE message containing an Alert-Info header field from the
12265 NIF component. Note that neither the originating network nor the LNG will provide audible
12266 ringing toward the PSAP in this case.

12267 **C.1.2 Assumed Behavior in a SIP-Based Originating Network**

12268 If a SIP-based originating network is operating in a jurisdiction in which Called Party
12269 Hold/Switch-hook Status is supported, this Appendix assumes that the SIP-based
12270 originating network will behave in one of the following ways:

- 12271 1. The SIP-based originating network follows the procedures defined in
12272 PKT-SP-RSTF-C01-140314 [137] and PKT-SP-CMSS1.5-I07-120412 [138]. According
12273 to Section 8.5.5.8 of PKT-SP-RSTF-C01-140314 [137], because only the PSAP knows
12274 if the network hold feature is in effect, the originating network must assume that
12275 network hold could be applied. Therefore the originating network processing of a
12276 disconnect request from the calling user will be different from normal disconnect
12277 processing if it occurs after the PSAP has answered the call. Specifically, upon
12278 receiving a disconnect request from the caller after the PSAP has answered the call,
12279 the originating network is expected to send a SIP re-INVITE containing an
12280 associated SDP with attribute "a= inactive" and a Priority header field set to
12281 "emergency", and set a Network Hold timer⁸⁸. If the user subsequently attempts to
12282 reconnect to the call, the originating network is expected to send a re-INVITE with
12283 an updated SDP offer and stop the Network Hold timer. If the originating network
12284 receives 200 OK responses to the re-INVITE messages, it will interpret these as
12285 indications of acceptance of the associated media offers.

12286 If the originating network supports Enhanced Called Party Hold, it is expected to set
12287 an ECPH timer at call setup time. Upon receiving a disconnect request from the
12288 caller before the PSAP has answered the call, the originating network will send a SIP
12289 UPDATE with an associated SDP "a" attribute set to "inactive" and a Priority header
12290 field set to "emergency". If the user subsequently attempts to reconnect to the call
12291 prior to a PSAP answer, the originating network is expected to send an UPDATE with
12292 an updated SDP offer. If the originating network receives 200 OK responses to the
12293 UPDATE messages, it will interpret these as indications of acceptance of the
12294 associated media offers. If the originating network receives the 200 OK response to
12295 the original INVITE, it will cancel the ECPH timer, if not expired. The originating
12296 network is expected to process received SIP BYE messages as specified in RFC
12297 3261. If the Network Hold timer expires before the user attempts to reconnect to
12298 the call, the originating network is expected to generate a SIP BYE message.
12299 Additionally, if the ECPH timer expires before the call is answered by the PSAP
12300 attendant, the originating network is expected to generate a SIP CANCEL message.

88 See Table 54 of RFC 3398 [139] for guidance on the Network Hold timer value.

- 12301 If the originating network receives a re-INVITE message that contains an Alert-Info
12302 header field (i.e., as a result of a Ringback request being initiated by the PSAP), the
12303 originating network is expected to apply the associated Ringback alerting treatment
12304 (i.e., regular ringing or receiver off-hook/howler tone, as identified in the ringing
12305 tone URI included in the Alert-Info header field) to the emergency caller. The
12306 originating network is also expected to return a SIP 180 Ringing message to/toward
12307 the i3 PSAP or Legacy PSAP Gateway (LPG). Note that the originating network
12308 should not provide audible ring to the PSAP.
- 12309 2. Alternatively, the SIP-based originating network may follow the procedures defined
12310 between the LNG-NIF and the NGCS in Sections C.3.1.1.2, C.3.1.2.2, C.4.4.1 and
12311 C.5.2.2. Additionally, because such originating networks may support nomadic
12312 devices, additional procedures are required to confirm whether the features can be
12313 supported end-to-end. This is accomplished by including the media feature tag
12314 "urn:emergency:media-feature.psap-call-control" in a Contact header field of the
12315 original SIP INVITE and any subsequent requests in-dialog. A PSAP or LPG
12316 supporting PSAP Call Control features will include the same media feature tag value
12317 in all responses within the dialog. If both parties have received the media feature
12318 tag, they must assume that PSAP Call Control features are in effect. From this point,
12319 the originating network processing of a disconnect request from the calling user will
12320 be different from normal disconnect processing if it occurs after the PSAP has
12321 answered the call. Specifically, upon receiving a disconnect request from the caller
12322 after the PSAP has answered the call, the originating network is expected to send a
12323 SIP re-INVITE containing an associated SDP with attribute "a=suspended" and set a
12324 Network Hold timer. If the user subsequently attempts to reconnect to the call, the
12325 originating network is expected to send a re-INVITE with an updated SDP offer with
12326 attribute "a=sendrecv" and stop the Network Hold timer. If the originating network
12327 receives 200 OK responses to the re-INVITE messages, it will interpret these as
12328 indications of acceptance of the associated media offers.
- 12329 If the originating network supports Enhanced Called Party Hold, it is expected to set
12330 an ECPH timer at call setup time. Upon receiving a disconnect request from the
12331 caller before the PSAP has answered the call, the originating network will send a SIP
12332 UPDATE with an associated SDP with attribute "a=suspended". If the disconnect
12333 occurs before the response to the original INVITE is received and if that response
12334 does not contain the media feature tag "urn:emergency:media-feature.psap-call-
12335 control", the originating network is expected to immediately send a SIP CANCEL and
12336 cancel the ECPH timer. If the disconnect occurs after a response to the original
12337 INVITE containing the media feature tag is received and the user subsequently
12338 attempts to reconnect to the call prior to PSAP answer, the originating network is
12339 expected to send an UPDATE with an updated SDP offer with attribute

- 12340 "a=sendrecv". If the originating network receives 200 OK responses to the initial
12341 INVITE and subsequent UPDATE messages, it will interpret these as indications of
12342 acceptance of the associated media offers and cancel the ECPH timer.
- 12343 The originating network is expected to process received SIP BYE messages as
12344 specified in RFC 3261. If the Network Hold timer expires before the user attempts to
12345 reconnect to the call, the originating network is expected to generate a SIP BYE
12346 message. Additionally, if the ECPH timer expires before the call is answered by the
12347 PSAP attendant, the originating network is expected to generate a SIP CANCEL
12348 message.
- 12349 If the originating network receives a re-INVITE message that contains an Alert-Info
12350 header field (i.e., as a result of a Ringback request being initiated by the PSAP), the
12351 originating network is expected to apply the associated Ringback alerting treatment
12352 (i.e., regular ringing or receiver off-hook/howler tone, as identified in the ringing
12353 tone URI included in the Alert-Info header field) to the emergency caller. If Ringback
12354 is signaled through the "P-DCS-OSPS:RING" header field⁸⁹, the originating network
12355 is expected to apply the appropriate Ringback alerting treatment based on its
12356 knowledge of the hook state of the calling device. The originating network is also
12357 expected to return a SIP 180 Ringing message to/toward the i3 PSAP or LPG. Note
12358 that the originating network should not provide audible ringing to the PSAP.
- 12359 3. The originating network does not support any Called Party Hold/Enhanced Called
12360 Party Hold/Switch-hook Status-specific call handling procedures. If a disconnect
12361 request is received from the caller, the UA generates a SIP BYE message (or SIP
12362 CANCEL if the 200 OK response has not been received), as specified in RFC 3261. It
12363 is expected to follow the procedures specified in RFC 6881 [46] for handling
12364 emergency call originations.

12365 **C.2 Bridging Considerations**

- 12366 A conference bridge in an i3 ESInet that supports the functionality described in Section 4.7
12367 (referred to in this Appendix as the "Bridge") MUST be aware of the status of PSAP Call
12368 Control support of all parties involved in a conference. The following sub-sections define
12369 the procedures required depending on the Bridging method implemented.
- 12370 If only the caller supports PSAP Call Control features and the PSAPs on the conference do
12371 not, the Bridge, upon receiving a switch-hook status change from the caller, MUST send a
12372 BYE message to the caller. The Bridge MUST also send a NOTIFY message to the

89 See Section C.4.1 for further details.

12373 subscribers to the conference noting the conference status of the caller by setting the
12374 <endpoint> element with a <status> sub-element set to “disconnected” and a
12375 <disconnection-method> sub-element set to “booted”, as per RFC 4575 [40].

12376 **C.2.1 SIP Ad Hoc Method**

12377 A Bridge that uses the “SIP Ad Hoc” method must be informed of the support of PSAP Call
12378 Control features by the conference participants. When invoking the Bridge, a Transfer-from
12379 PSAP supporting PSAP Call Control features MUST signal in the INVITE message (and any
12380 subsequent requests in-dialog) to the Bridge that it supports PSAP Call Control features by
12381 adding the media feature tag “urn:emergency:media-feature.psap-call-control” as part of a
12382 Contact header field value of the INVITE message. When adding the caller, the Bridge
12383 MUST add the media feature tag “urn:emergency:media-feature.psap-call-control” in the
12384 Contact header field of the INVITE message with Replaces. If the Caller supports PSAP Call
12385 Control Features, the Caller (or B2BUA⁹⁰) MUST add the media feature tag
12386 “urn:emergency:media-feature.psap-call-control” in all responses, provisional or final, to
12387 the INVITE and any subsequent requests in-dialog. When adding the Transfer-To PSAP,
12388 the Bridge MUST add the media feature tag “urn:emergency:media-feature.psap-call-
12389 control” in a Contact header field of the outgoing INVITE message, if the caller supports
12390 PSAP Call Control features. If it supports PSAP Call Control features, the Transfer-To PSAP
12391 MUST add the media feature tag “urn:emergency:media-feature.psap-call-control” in all
12392 responses, provisional or final, to the INVITE and any subsequent requests in-dialog. At
12393 this point, the Bridge and all parties participating on the conference are aware of PSAP Call
12394 Control support.

12395 **C.2.2 Route All Calls via a Conference-Aware UA Method**

12396 A Bridge that uses the “Route All Calls via a Conference-Aware UA” method MUST maintain
12397 state of PSAP Call Control features support, as learned through the signaling of the initial
12398 emergency call. If the calling device supports PSAP Call Control features, the Bridge MUST
12399 also learn support of PSAP Call Control features of any party added to the conference. The
12400 Bridge does so by adding the media feature tag “urn:emergency:media-feature.psap-call-
12401 control” as part of a Contact header field value of the INVITE messages (and any
12402 subsequent requests in-dialog) sent to parties by the Conference-Aware UA. Parties
12403 supporting PSAP Call Control features MUST add the media feature tag
12404 “urn:emergency:media-feature.psap-call-control” as part of a Contact header field value of

⁹⁰ A B2BUA which supports origination devices/services that do not support Replaces but do support Call Control Features will need to add the media feature tag on the response to INVITE/Replaces. How this is recognized is an implementation detail.

12405 all responses, provisional or final, to the INVITE message and any subsequent requests in-
12406 dialog.

12407 **C.3 Called Party Hold/Switch-Hook Status**

12408 **C.3.1 Procedures at the Legacy Network Gateway**

12409 **C.3.1.1 SS7 Signaling from Originating End Office**

12410 When a legacy originating switch receives an emergency call origination and determines
12411 that the Called Party Hold feature may be requested by an emergency services network,
12412 and the originating switch can support the Called Party Hold feature for the outgoing
12413 circuit, the SS7 Initial Address Message (IAM) delivered by the originating switch to the
12414 LNG MAY contain a Feature Code Indicator in the Service Activation Parameter (SAP) set to
12415 "hold available".

12416 **C.3.1.1.1 Procedures at the LNG-PIF Component**

12417 Upon receiving an IAM with a SAP, the PIF component of the LNG SHALL follow the
12418 procedures in Section 6.1.1.2.2 and 6.1.1.5, with the following modifications. If the PIF
12419 component receives an IAM that contains a SAP, it SHALL encapsulate the IAM in the
12420 INVITE sent to the NIF component, including the encapsulated message in the body of the
12421 INVITE following the procedures specified in Section 5.4.1.2 of ATIS-1000679.2015 [130].

12422 In addition, the PIF component SHALL be capable of receiving a 180 Ringing message from
12423 the NIF component that includes an encapsulated ACM message that contains a SAP
12424 parameter with a Feature Code Indicator set to "hold request" in the body. The PIF
12425 component SHALL generate an ACM, based on the received 180 Ringing message, and
12426 SHALL include a SAP parameter with Feature Code Indicator set to "hold request" in the
12427 outgoing ACM.

12428 The PIF component SHALL also be capable of receiving a 183 Session Progress message
12429 from the NIF component that includes an encapsulated ACM message that contains a SAP
12430 parameter with a Feature Code Indicator set to "hold request" in the body. The PIF
12431 component SHALL generate an ACM, based on the received 183 Session Progress message,
12432 and SHALL include a SAP parameter with Feature Code Indicator set to "hold request" in
12433 the outgoing ACM.

12434 If the PIF component subsequently receives an SS7 Facility (FAC) message associated with
12435 the incoming SS7-supported trunk group over which the emergency call origination was
12436 received, it SHALL encapsulate the FAC message in a SIP INFO (RFC 6086) [149] message,
12437 as described in Section 5.4.3 of ATIS-1000679.2015 [130] and send it to the NIF
12438 component. This may occur if an emergency call has been established, Called Party Hold is

12439 active on that call, and the switch-hook status of the emergency caller changes. If the
12440 emergency caller attempts to disconnect from the call (i.e., goes "on-hook"), the FAC
12441 message MUST contain a Feature Code Indicator in the SAP set to "disconnect request". If
12442 the emergency caller subsequently goes "off-hook", the PIF component SHALL receive an
12443 FAC that contains a Feature Code Indicator in the SAP set to "reconnect request".
12444 If the PIF component receives a SIP INFO containing an encapsulated FAC message from
12445 the NIF component, the PIF component SHALL generate an SS7 FAC message based on
12446 the encapsulated FAC message.
12447 If, at any time, the PIF component receives a SIP BYE message from NIF component, the
12448 PIF component SHALL process that SIP BYE message as described in Section 6.1.1.5. If, at
12449 any time, the PIF component receives an SS7 REL message from the legacy originating
12450 network, the PIF component SHALL generate a SIP BYE message and send it to the NIF
12451 component, as described in Section 6.1.1.2.2.

12452 **C.3.1.1.2 Procedures at the LNG-NIF Component**

12453 Upon receipt of an INVITE message from the PIF component containing an encapsulated
12454 IAM, the NIF component SHALL follow the procedures in Sections 6.1.2.1, 6.1.2.1.1, and
12455 6.1.2.2 with the following modifications. If, based on receipt of a media feature tag with
12456 the value "urn:emergency:media-feature.psap-call-control", the NIF component determines
12457 that the destination to which the call was delivered supports PSAP Call Control Features,
12458 then upon receipt of a 180 Ringing message from the NGCS (that does not contain an
12459 encapsulated ACM), the NIF component SHALL generate and send a 180 Ringing message
12460 to the PIF component with an encapsulated ACM in the body of that message. If, based on
12461 receipt of the media feature tag "urn:emergency:media-feature.psap-call-control", the NIF
12462 component determines that the destination to which the call was delivered supports PSAP
12463 Call Control Features and the NIF component receives a 183 Session Progress message
12464 from the NGCS (that does not contain an encapsulated ACM), the NIF component SHALL
12465 generate and send a 183 Session Progress message to the PIF component with an
12466 encapsulated ACM in the body of that message. In either case, the NIF component SHALL
12467 populate the encapsulated ACM following the procedures described in Section 6.1.1.5 and
12468 SHALL also include a SAP with a Feature Code Indicator set to "hold request" in the
12469 encapsulated ACM message.

12470 If the NIF component receives a 180 Ringing or 183 Session Progress message that
12471 contains an encapsulated ACM, the NIF component SHALL follow the procedures in Section
12472 7.2.1 or 7.2.2, respectively, of ATIS-1000679.2015 [130] for sending a 180 Ringing or 183
12473 Session Progress message to the PIF component.

12474 If the NIF component receives a SIP INFO message from the PIF component, associated
12475 with the same emergency call that contains an encapsulated FAC message with the Feature
12476 Code Indicator in the SAP set to "disconnect request," the NIF component SHALL generate
12477 a re-INVITE message that contains an SDP offer with an "a= suspended" attribute⁹¹. The
12478 re-INVITE message MUST reference the existing dialog so that the i3 PSAP (or LPG, in the
12479 case of a legacy PSAP) knows that it is to modify an existing session instead of establishing
12480 a new session. The re-INVITE message SHALL include the following information:

- 12481 • A Request-URI that contains the information provided in the Contact header field of
12482 the 200 OK message that was returned in response to the original INVITE message;
- 12483 • A To header field that contains the same information as the original INVITE message
(i.e., the digits "911");
- 12484 • A From header field that contains the same information as in the original INVITE
message;
- 12485 • A Via header field that is populated with the Element Identifier (see Section 2.1.3)
for the LPG;
- 12486 • A Route header field that contains the same information as in the original INVITE
(i.e., the ESRP URI obtained from the ECRF, which should be augmented with the
"lr" parameter to avoid Request-URI rewriting);
- 12487 • A Contact header field that contains the same information as in the original INVITE
message (i.e., a SIP URI associated with the LNG), including the media feature tag;
- 12488 • An SDP with an "a = suspended" attribute to identify that this is related to PSAP Call
Control Features.

12489 Upon receiving a 200 OK message from the i3 PSAP/LPG (via the NGCS), indicating that it
12490 accepts the change, the NIF component SHALL respond to the 200 OK by returning an ACK
12491 message toward the i3 PSAP/LPG. The NIF component SHALL also send a SIP INFO
12492 message to the PIF component that contains an encapsulated FAC message with the
12493 Feature Code Indicator in the SAP set to "hold continuation request" and will repeat this
12494 periodically (e.g., every minute or so) to maintain the connection in the legacy originating
12495 network.

91 Note that the use of a re-INVITE that contains an SDP offer indicating that the originator of the re-INVITE no longer wishes to receive media is consistent with the procedures described in Section 9.2 of IETF RFC 3398 [139]. The use of an "a=" attribute value of "suspended" in the SDP will allow the entity receiving the re-INVITE to associate the message with a disconnect request issued by an emergency caller that is subject to PSAP Call Control features.

12503 If the NIF component receives a SIP INFO message from the PIF component, associated
12504 with the same emergency call, that contains an encapsulated FAC message with the
12505 Feature Code Indicator in the SAP set to "reconnect request", the NIF component SHALL
12506 generate a re-INVITE message with a new SDP offer that contains an attribute of
12507 "a=sendrecv". The re-INVITE SHALL contain the same information listed above, except
12508 that the SDP will contain the new offer.
12509 Upon receiving a 200 OK message from the i3 PSAP/LPG indicating that it accepts the
12510 change, the NIF component SHALL respond to the 200 OK by returning an ACK message
12511 toward the i3 PSAP/LPG to acknowledge receipt of the SIP 200 response and to confirm the
12512 media has been reactivated.

12513 **C.3.1.2 MF Signaling from Originating End Office**

12514 **C.3.1.2.1 Procedures at the LNG-PIF Component**

12515 Upon receiving a trunk seizure (off-hook) from the originating end office, the PIF
12516 component of the LNG SHALL return a wink back to the end office. After receiving the
12517 called number sequence (i.e., KP + 911 + ST), the PIF component SHALL generate an ANI
12518 request signal and await the ANI sequence. If CAMA-type signaling is used on the MF trunk
12519 from the originating end office to the LNG, the PIF component of the LNG SHALL be
12520 capable of receiving and processing an ANI sequence that consists of "I + 7-digit ANI". If
12521 Feature Group D operator-type signaling is used on the MF trunk from the legacy end office
12522 to the PIF component of the LNG, the PIF component SHALL be capable of receiving and
12523 processing an ANI sequence consisting of "II + 7/10-digit ANI".

12524 The PIF component SHALL follow the procedures in Section 6.1.1.5 for generating a SIP
12525 INVITE message and sending it to the NIF component of the LNG.

12526 Also, as described in Section 6.1.1.5, the PIF component of the LNG SHALL be capable of
12527 receiving and processing a SIP 100 Trying message passed to it by the NIF component,
12528 acknowledging receipt of the INVITE that was previously generated by the PIF component.

12529 The PIF component of the LNG SHALL also be capable of receiving and processing a 180
12530 Ringing message and a 183 Session Progress message from the NIF component. Upon
12531 receiving a 180 Ringing message, the PIF component MUST apply audible ringing tone to
12532 the calling party.

12533 The PIF component of the LNG SHALL be capable of receiving and processing a 200 OK
12534 message, indicating that the call has been answered. Upon receiving the 200 OK message,
12535 the PIF SHALL generate an answer signal to the originating end office.

12536 If the PIF component receives an "on-hook" indication from the originating end office
12537 switch associated with an existing emergency call delivered over an MF trunk group, the

12538 PIF component SHALL use trunk group provisioning to determine its subsequent behavior.
12539 If the provisioning associated with the incoming MF trunk group indicates that Called Party
12540 Hold/Switch-hook Status is supported, the PIF component SHALL pass the on-
12541 hook/"unseize circuit" telephony event to the NIF component using the mechanisms
12542 defined in RFC 5244 [140] (or equivalent), and SHALL maintain the connection to the
12543 originating end office switch. If the emergency caller subsequently goes "off-hook", the PIF
12544 component SHALL pass the off-hook/"seizure" telephony event to the NIF component using
12545 the mechanisms defined in RFC 5244 [140] (or equivalent).

12546 If the provisioning associated with the incoming MF trunk group indicates that Called Party
12547 Hold/Switch-hook Status is not supported, and an on-hook signal is received from the
12548 originating end office associated with an existing emergency call delivered over an MF
12549 trunk group, the PIF component SHALL generate a SIP BYE message and send it to the NIF
12550 component, as described in Section 6.1.1.1.

12551 If, at any time, the PIF component receives a SIP BYE message from the NIF component,
12552 the PIF component SHALL process that SIP BYE message, return a 200 OK message to the
12553 NIF component, acknowledging receipt of the SIP BYE message, as described in Section
12554 6.1.1.5, and SHALL generate an on-hook signal toward the originating switch.

12555 **C.3.1.2.2 Procedures at the LNG-NIF Component**

12556 Upon receipt of an INVITE message from the PIF component, the NIF component SHALL
12557 follow the procedures in Sections 6.1.2.1, 6.1.2.1.1, and 6.1.2.2 for processing that INVITE
12558 message and sending an INVITE to the NGCS. Based on provisioning associated with the
12559 incoming trunk group parameters in the Contact header field of the INVITE message
12560 received from the PIF component, the NIF component SHALL determine whether PSAP Call
12561 Control Features are supported for this emergency call.

12562 As described in Section 6.1.2.2, the NIF component SHALL return a SIP 100 Trying
12563 message to the PIF after sending the SIP INVITE to the NGCS. The NIF component SHALL
12564 also be capable of receiving and processing a 180 Ringing or 183 Session Progress
12565 message from the NGCS in response to the SIP INVITE. The NIF component SHALL
12566 forward the 180 Ringing or 183 Session Progress message to the PIF component. In
12567 addition, the NIF component SHALL determine whether the destination to which the call
12568 was delivered supports PSAP Call Control Features based on the presence or absence of
12569 the "urn:emergency:media-feature.psap-call-control" media feature tag in a Contact header
12570 field of the received 180 Ringing or 183 Session Progress message.

12571 The NIF component SHALL also be capable of receiving and processing a 200 OK message
12572 from the NGCS. If the NIF component receives a 200 OK message from the NGCS, it SHALL
12573 send it to the PIF component. The NIF component SHALL be capable of receiving and

12574 processing an ACK message from the PIF component in response to the 200 OK message.
12575 The NIF component SHALL subsequently send an ACK message to the NGCS.

12576 If the NIF component subsequently receives an on-hook/"unseize circuit" event indication
12577 (encoded using RFC 5244 [140] mechanisms or equivalent) from the PIF component
12578 associated with the same emergency call (received over an MF trunk group that is
12579 provisioned to indicate support for Called Party Hold/Switch-hook Status), and the
12580 destination to which the call was delivered also supports PSAP Call Control Features, the
12581 NIF component SHALL generate a re-INVITE message with SDP that contains an "a=
12582 suspended" attribute, as specified in Section C.3.1.1.2, and forward the re-INVITE to the
12583 NGCS.

12584 If, subsequent to receiving an on-hook/unseize circuit event indication, the NIF component
12585 receives an off-hook/seize event indication (encoded using RFC 5244 [140] mechanisms or
12586 equivalent) from the PIF component associated with the same emergency call, and the
12587 destination to which the call was delivered also supports PSAP Call Control Features, the
12588 NIF component SHALL generate a re-INVITE message with a new SDP offer with an
12589 attribute of "a=sendrecv". As in Section C.3.1.1.2, the re-INVITE will contain the same
12590 information as the previous re-INVITE, except that the SDP will contain the new offer.

12591 In both cases, upon receiving a 200 OK message from the i3 PSAP/LPG (via the NGCS)
12592 indicating that it accepts the change, the NIF component MUST respond to the 200 OK by
12593 returning an ACK message toward the i3 PSAP/LPG confirming the media has been
12594 changed.

12595 If the NIF component receives an on-hook/unseize circuit event indication (encoded using
12596 RFC 5244 [140] mechanisms or equivalent) from the PIF component associated with an
12597 emergency call that was received over an MF trunk group that is provisioned to indicate
12598 support for Called Party Hold/Switch-hook Status, and the destination to which the call was
12599 delivered does not support PSAP Call Control Features, the NIF component SHALL send a
12600 BYE message to the NGCS and a BYE message to the PIF component.

12601 If, at any time, the NIF component receives a SIP BYE message from the NGCS, the NIF
12602 component SHALL process that SIP BYE message as described in Section 6.1.2.2. If, at any
12603 time, the NIF component receives a SIP BYE message from the PIF component, the NIF
12604 component SHALL process that SIP BYE message as described in Section 6.1.2.2.

12605 **C.3.2 Procedures at the ESRP**

12606 If the ESRP is stateful (i.e., has been identified in record routing), and is therefore in the
12607 path of the re-INVITE messages, the ESRP SHALL follow normal procedures, as described
12608 in RFC 3261 [10], for passing SIP re-INVITE messages and related responses (200 OK and

12609 ACK) associated with requests for Called Party Hold when the originating network and the
12610 PSAP support feature-specific signaling.

12611 The ESRP SHALL also follow normal procedures, as described in RFC 3261 [10], for passing
12612 SIP BYE messages and Contact header fields.

12613 **C.3.3 Procedures at the i3 PSAP**

12614 If an i3 PSAP is operating in a jurisdiction in which PSAP Call Control features are
12615 supported/required, it SHALL be capable of interpreting the presence of a media feature
12616 tag⁹² of "urn:emergency:media-feature.psap-call-control"⁹³ in a Contact header field of the
12617 original INVITE (and any subsequent requests in-dialog) as an indication from the
12618 originating network that it supports PSAP Call Control features. An i3 PSAP operating in a
12619 jurisdiction in which PSAP Call Control features are supported/required SHALL include a
12620 media feature tag of "urn:emergency:media-feature.psap-call-control" in a Contact header
12621 field of all responses (provisional or final) to that original INVITE and any subsequent
12622 requests in-dialog. If the i3 PSAP receives a media feature tag of "urn:emergency:media-
12623 feature.psap-call-control" to original INVITE messages and it is operating in a jurisdiction in
12624 which PSAP Call Control features are supported/required, the i3 PSAP MUST assume that
12625 PSAP Call Control features are in effect end-to-end. Additionally, it SHALL be capable of
12626 receiving and processing re-INVITE messages that contain new SDP offers with attribute
12627 "a= suspended" or "a=sendrecv", indicating that the re-INVITE is associated with PSAP Call
12628 Control Features. The i3 PSAP SHALL also associate re-INVITE messages that contain both
12629 a Priority header field of "emergency" and an SDP with attribute "a= inactive" or
12630 "a=sendrecv" as being associated with PSAP Call Control Features⁹⁴. The i3 PSAP SHALL
12631 use an appropriate mechanism for notifying the PSAP attendant of the change in status.⁹⁵
12632 (As noted above, today, this notification takes the form of a switch-hook status audible
12633 tone). In response to the change in switch-hook status, the PSAP attendant may initiate a
12634 Ringback request, using the procedures described in Section C.4.1.

92 The Media feature tag SIP framework is defined in RFC 3840 [23].

93 See Section 10.16 for registration in the NENA Registry System.

94 The combination of Priority = "emergency" and SDP with "a=inactive" will be sent by originating networks that follow the procedures defined in PKT-SP-RSTF-C01-140314 [137] and PKT-SP-CMSS1.5-I07-120412 [138] when a caller goes on-hook and PSAP Call Control Features are in effect. (See Section C.1.2) Note that the value of the "a=" attribute within the SDP associated with these re-INVITE messages could be changed from "inactive" to "suspended" or vice-versa by SBC functionality within the ingress BCF.

95 Details related to the mechanism used by the PSAP to notify the attendant of a change in caller status are outside the scope of this document.

12635 If an i3 PSAP is operating in a jurisdiction in which PSAP Call Control features are
12636 supported/required, and it receives a SIP BYE message from an ESRP associated with a
12637 premature disconnect, the i3 PSAP SHALL follow the procedures in RFC 3261 [10] for
12638 processing the BYE message, and MUST immediately notify the PSAP attendant of the
12639 change in status. In some circumstances, the i3 PSAP or call taker may initiate an
12640 immediate callback to the emergency caller. The callback initiated by the i3 PSAP SHALL
12641 follow the procedures specified in RFC 7090 [141] for marking the callback call by including
12642 a SIP Priority header field value of "psap-callback" in the INVITE message associated with
12643 the callback call.

12644 **C.3.4 Procedures at the Legacy PSAP Gateway**

12645 If the LPG is operating in an environment in which PSAP Call Control Features are
12646 supported, it MUST support the additional protocol and procedures described below.

12647 **C.3.4.1 Procedures at the LPG-NIF Component**

12648 The NIF component of the LPG SHALL be capable of interpreting the presence of a media
12649 feature tag of "urn:emergency:media-feature.psap-call-control" in a Contact header field of
12650 the original INVITE (and any subsequent requests in-dialog) as an indication from the
12651 originating network that it supports PSAP Call Control features. If, based on provisioning,
12652 the NIF component determines that the destination PSAP supports PSAP Call Control
12653 features, it SHALL include a media feature tag of "urn:emergency:media-feature.psap-call-
12654 control" in a Contact header field of all responses (provisional and final) to original INVITE
12655 messages and any subsequent requests in-dialog. From that point on, the NIF component
12656 of the LPG MUST assume that PSAP Call Control features are in effect end-to-end.

12657 The NIF component of the LPG SHALL follow the procedures described in Section 6.2.2,
12658 with the following clarifications. If the NIF component of an LPG receives a re-INVITE
12659 message from an NGCS, it SHALL forward that re-INVITE to the PIF component, including
12660 an Element Identifier associated with the LPG in a Via header field (see Section 2.1.3).

12661 If the NIF component subsequently receives a 200 OK message from the PIF component, it
12662 SHALL pass it to the NGCS, as described in Section C.3.1.1.2. Upon receiving an ACK from
12663 the NGCS, the NIF component SHALL forward the ACK to the PIF component.

12664 If an NIF component receives a BYE message from an NGCS, it SHALL follow the
12665 procedures specified in RFC 3261 [10] for processing that message (i.e., it will return a 200
12666 OK confirming receipt of the BYE message and terminating the session and the
12667 transaction,) however, before signaling the PIF component, the NIF component SHALL
12668 determine, based on provisioning, whether the PSAP supports PSAP Call Control Features.
12669 If the PSAP supports PSAP Call Control Features, the NIF component MUST generate a re-
12670 INVITE message containing an SDP with attribute "a = suspended" and send it to the PIF

12671 component, maintaining the connection to the PSAP. This will allow the legacy PSAP to be
12672 notified of the change in switch-hook status of the caller and allowing it to initiate Ringback
12673 if desired.

12674 If the NIF component receives a BYE message from the NGCS and the PSAP does not
12675 support PSAP Call Control Features, the NIF component SHALL send a BYE message to the
12676 PIF component.

12677 If the NIF component receives a BYE message from the PIF component, it SHALL follow
12678 standard RFC 3261 [10] procedures for processing the BYE and SHALL send a BYE to the
12679 NGCS.

12680 **C.3.4.2 Procedures at the LPG-PIF Component**

12681 In addition to the procedures specified in Section 6.2.1, the PIF component of the LPG
12682 SHALL be capable of receiving re-INVITE messages from the NIF component. Specifically,
12683 in the context of PSAP Call Control Features, the PIF component SHALL be capable of
12684 receiving and processing a re-INVITE message that is generated as a result of the
12685 procedures specified in Section C.3.4.1.

12686 Upon receipt of a re-INVITE message containing an SDP with attribute "a= suspended" or
12687 a re-INVITE message containing both a "Priority= emergency" header field and an SDP
12688 with attribute "a= inactive", the PIF component of the LPG SHALL apply audio alerting to
12689 the PSAP so that the attendant is notified of the on-hook status of the emergency caller.

12690 If the PIF component subsequently receives a re-INVITE message with a new SDP value
12691 (attribute "a= sendrecv" plus the "Priority: emergency" header field), it SHALL stop
12692 applying the on-hook status alerting, and re-establish the RTP to allow the conversation
12693 between the emergency caller and the attendant to resume.

12694 If a PIF component receives a disconnect indication from a legacy PSAP, the PIF
12695 component SHALL follow the procedures specified in Section 6.2.4.2.1 to identify the on-
12696 hook condition as a true disconnect, then it SHALL send a BYE message to the NIF
12697 component. If the PIF component receives a BYE message from the NIF component, it
12698 SHALL apply standard RFC 3261 [10] procedures for processing the BYE message and send
12699 an on-hook signal to the PSAP.

12700 **C.3.5 Procedures at the Bridge**

12701 It is possible that a caller hangs-up intentionally or unintentionally while connected to a
12702 Bridge. When PSAP Call Control features are in effect, the caller's hook status changes
12703 must be communicated to the other participants on the conference.

12704 The following sub-sections describe how changes in the caller's hook state are propagated
12705 by the Bridge and assumes that, at a minimum the transfer-from PSAP and the callers are
12706 connected to the Bridge (refer to the appropriate sub-sections of Section 4.7 depending on
12707 the bridging method used).

12708 **C.3.5.1 Using the SIP Ad-Hoc Method**

12709 Upon receiving a switch-hook status change from the caller through a re-INVITE, the
12710 Bridge will send a NOTIFY message to the PSAP(s) that subscribed to the conference,
12711 indicating the change in the subscription state. The NOTIFY message will contain a
12712 conference data structure with a <media> element containing a <status> sub-element
12713 indicating the SDP status of the caller as received in the re-INVITE message's SDP offer a-
12714 line as per RFC 4575 [40].

12715 **C.3.5.2 Using the Route All Calls via a Conference-Aware UA Method**

12716 The procedures are the same as for the SIP Ad Hoc method.

12717 **C.4 Ringback**

12718 The Ringback feature enables the PSAP attendant to invite back an emergency caller, or
12719 someone in the surrounding area, into the conversation, over an established connection.
12720 This feature has different behaviors depending on the state of the device (on-hook or off-
12721 hook). If a conversation between an emergency caller and a PSAP attendant is occurring
12722 but the emergency caller stops responding, it allows the attendant to request that the
12723 receiver off-hook tone (also known as howler tone) be temporarily played at the caller's
12724 device. As a complement to the Called Party Hold feature, the Ringback feature also allows
12725 the attendant to request that the emergency caller's device rings if it has gone on-hook.

12726 **C.4.1 Procedures at the PSAP**

12727 If an emergency call has been established, Called Party Hold is active on that call, and the
12728 emergency caller disconnects prematurely from the call, the PSAP may wish to re-invite the
12729 caller to the call by initiating a Ringback toward that caller to trigger normal ringing of the
12730 caller's device. Likewise, if Called Party Hold is active on an existing emergency call but
12731 conversation with the emergency call has ceased abruptly, the PSAP may attempt to re-
12732 invite the emergency caller or someone else in the area to re-establish communication by
12733 initiating a Ringback towards that caller to trigger the application of howler tone.

12734 In the case of a legacy PSAP, the attendant will typically trigger the Ringback by sending a
12735 switch-hook flash then dialing the Ringback access code (e.g., *99), resulting in DTMF
12736 signaling being sent to the LPG.

12737 In the case of an i3 PSAP, it is expected that, in response to an action taken by the
12738 attendant to request Ringback, the Ringback feature will be triggered by the PSAP UA
12739 issuing a re-INVITE with an Alert-Info header field⁹⁶ set to the appropriate audible ringing
12740 tone URI (typically, regular ringing, if the caller is considered on-hook, or ROH/howler
12741 tone, if the caller is considered off-hook) towards the emergency caller.
12742 Note that if an i3 PSAP receives a BYE associated with an emergency call (i.e., Called Party
12743 Hold is not active on the call), and the i3 PSAP wishes to re-establish contact with the
12744 emergency caller, the i3 PSAP MAY initiate a callback to that emergency caller. The callback
12745 initiated by the i3 PSAP SHALL follow the procedures specified in RFC 7090 [141] for
12746 marking the callback call by including a SIP Priority header field value of "psap-callback" in
12747 the INVITE message associated with the callback call.

12748 **C.4.2 Procedures at the Legacy PSAP Gateway**

12749 **C.4.2.1 Procedures at the LPG-PIF Component**

12750 Upon receiving a Ringback request from a legacy PSAP (in the form of a switch-hook flash
12751 and DTMF signaling generated by the attendant), the PIF component of the LPG SHALL
12752 follow the procedures defined in RFC 4733 [142] for passing DTMF signals to the NIF
12753 component of the LPG.

12754 If the PIF component subsequently receives a 183 Session Progress message or 180
12755 Ringing message from the NIF component (associated with an on-hook or off-hook
12756 Ringback request, as described in Section C.4.2.2) in response, it will apply audible ringing
12757 on the existing media path to the legacy PSAP.

12758 **C.4.2.2 Procedures at the LPG-NIF Component**

12759 Upon receiving DTMF information from the PIF component (using RFC 4733 [142]
12760 procedures), the NIF will interpret the DTMF information. If the NIF component determines
12761 that the DTMF information originated by the PSAP is a request for initiation of the Ringback
12762 feature, and Called Party Hold is active on the call, the NIF component SHALL generate a
12763 re-INVITE message toward the emergency caller. The re-INVITE message MUST contain an
12764 Alert-Info header field that indicates the type of alerting that should be provided. If the
12765 SDP currently associated with the call is "suspended" or "inactive" (i.e., the latest re-
12766 INVITE received by the NIF component contained an SDP with attribute "a=suspended" or

⁹⁶ Some deployments may use the P-DCS-OSPS header with a value of "RING" as defined in RFC 5503 [170] to signal Ringback. The specific method being used in one jurisdiction is determined through bilateral negotiations.

12767 an SDP attribute "a=inactive" with "Priority=emergency"), the ringing tone URI included in
12768 the Alert-Info header field SHALL be associated with regular ringing. If the SDP associated
12769 with the call has been updated in the most recently received re-INVITE message (i.e., SDP
12770 with attribute "a= sendrecv" with the "Priority: emergency" header field), the ringing tone
12771 URI in the Alert-Info header field will be associated with a receiver off-hook/howler tone to
12772 be played for a defined period.

12773 If the Alert-Info header field sent by the NIF in the re-INVITE message is associated with
12774 regular ringing (i.e., because the caller has gone on-hook), the NIF component SHALL be
12775 capable of receiving and processing a 183 Session Progress message or 180 Ringing
12776 message in response, indicating that the emergency caller is being alerted. The NIF
12777 component SHALL pass the 183 Session Progress/180 Ringing message to the PIF
12778 component.

12779 If the NIF component subsequently receives a 200 OK in response to the re-INVITE
12780 message it generated, the voice path SHALL be re-established between the emergency
12781 caller and the PSAP.

12782 If the NIF component receives DTMF information from the PIF component indicating that
12783 the PSAP is requesting initiation of the Ringback feature and the connection between the
12784 LPG and the emergency caller no longer exists (because the NIF component previously
12785 received a BYE or CANCEL from the NGCS associated with the emergency call), the NIF
12786 component SHALL initiate a callback request to/towards that caller. The callback initiated
12787 by the NIF component of the LPG SHALL follow the procedures specified in RFC 7090 [141]
12788 for marking the callback call by including a SIP Priority header field value of "psap-callback"
12789 in the INVITE message associated with the callback call.

12790 **C.4.3 Procedures at the ESRP**

12791 If the ESRP is stateful (i.e., has been identified in record routing), and is therefore in the
12792 path of the re-INVITE messages, the ESRP SHALL follow normal procedures, as described
12793 in RFC 3261 [10], for passing SIP re-INVITE messages and associated responses (200 OK
12794 and ACK).

12795 **C.4.4 Procedures at the Legacy Network Gateway**

12796 **C.4.4.1 Procedures at the LNG-NIF Component**

12797 The NIF component of the LNG SHALL be capable of receiving and processing a re-INVITE
12798 message that contains an Alert-Info header field. If the NIF component receives a re-
12799 INVITE message containing an Alert-Info header field associated with an emergency call
12800 that was delivered over an SS7 trunk group, the NIF component SHALL generate a SIP
12801 INFO message that includes an encapsulated SS7 FAC message with an SAP that contains

12802 a Feature Code Indicator set to “ringback request”, and pass it to the PIF component (see
12803 Table 9B/T1.113.3 of GR-246-CORE [143] for details regarding the coding of the SS7 FAC
12804 message).

12805 If the NIF component receives a re-INVITE message containing an Alert-Info header field
12806 associated with an emergency call that was delivered over an MF trunk group, the NIF
12807 component SHALL forward the re-INVITE message to the PIF component.

12808 **C.4.4.2 Procedures at the PIF Component**

12809 As described in Section C.3.1.1.1, the PIF component of the LNG SHALL be capable of
12810 receiving and processing a SIP INFO message from the NIF component. If the PIF
12811 component receives a SIP INFO containing an encapsulated FAC message from the NIF
12812 component, the PIF component SHALL generate an SS7 FAC message based on the
12813 encapsulated FAC message. In this scenario, a 180 Ringing Message SHOULD NOT be
12814 generated by the PIF component towards the NIF.

12815 If the PIF component receives a re-INVITE message containing an Alert-Info header field,
12816 the PIF component SHALL apply alerting toward the caller appropriate for the audible
12817 ringing tone URI provided in the Alert-Info header field, and SHALL return a SIP 180
12818 Ringing message to the NIF component.

12819 **C.4.5 Procedures at the Bridge**

12820 It is possible that a caller hangs-up intentionally or unintentionally when connected to a
12821 bridge, or a caller may become unresponsive. In such circumstances, a PSAP supporting
12822 PSAP Call Control features may want to initiate a Ringback through the Bridge.

12823 The following sub-sections describe how PSAP-originated Ringback requests are
12824 propagated by the Bridge.

12825 **C.4.5.1 Using the Ad Hoc Method**

12826 As defined in section C.4.1, PSAPs originate Ringback requests towards the caller using re-
12827 INVITE messages containing alerting information. However, when a Bridge is involved, the
12828 PSAP MUST use the REFER method to communicate with the caller via the Bridge. A PSAP
12829 that wishes to initiate a Ringback request through a Bridge MUST use the procedures
12830 defined in RFC 4579 [39] to propagate the Ringback request to the caller’s leg. The REFER
12831 message associated with a Ringback request SHALL have the Refer-to header field value
12832 set to the caller’s URI with a “method” parameter set to “INVITE” alongside the alerting
12833 information (i.e., either an Alert-Info or a P-DCS-OSPS header field passed as parameters).
12834 The Bridge uses the information in the REFER to initiate an INVITE message towards the

12835 caller with the alerting information. An example Refer-to header field construct would look
12836 like this:

12837 Refer-To:<sip:guy@vsp.com;method=INVITE?Alert-
12838 Info=http://localhost/howler.wav>

12839 And the corresponding INVITE from the Bridge towards the caller, like this:

12840 INVITE urn:service:sos SIP/2.0
12841 From: <sip:bridge@ngcs.com>;tag=547429769-1531467798707-
12842 To: sip:guy@vsp.com;tag=23859029fkwp42-g2486gf3w5
12843 Call-ID: jgigjsdksd faswdk-123412482tjf
12844 CSeq: 155978842 INVITE
12845 Contact: <sip:bridge@ngcs.com>
12846 Alert-Info: <http://localhost/howler.wav>
12847 Supported: 100rel
12848 Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
12849 Accept: application/sdp,multipart/mixed
12850 Max-Forwards: 67

12851 Upon receiving a final response from the caller, the Bridge MUST send a NOTIFY message
12852 to the conference subscribers with a "sipfrag" bodypart as per RFC 3420 [33]. Subscribers
12853 can use this information to initiate an audible and/or visual indication to a call-taker that
12854 the Ringback request was submitted.

12855 **C.4.5.2 Using the Route All Calls via a Conference-Aware UA Method**

12856 The procedures are the same as for the SIP Ad Hoc method.

12857 **C.5 Enhanced Called Party Hold**

12858 As a complement to the Called Party Hold feature, Enhanced Called Party Hold allows the
12859 media path to be established even though the PSAP attendant hasn't yet answered when
12860 the caller hangs up. Once the attendant picks up, regular connection hold capabilities
12861 apply. Therefore, if the caller picks up again, his/her conversation with the attendant will
12862 automatically resume.

12863 If a legacy originating network supports Enhanced Called Party Hold and the originating
12864 switch interconnects with the LNG via SS7 trunk groups, an ECPH timer MUST be
12865 supported at the LNG. The external signaling generated by the originating network
12866 SHOULD be the same as for Called Party Hold. The LNG SHALL follow the procedures
12867 described in Section C.5.1. The Called Party Hold procedures applicable to the ESRP, LPG,
12868 and i3 PSAP, as described in Section C.2 and its subsections, SHALL also apply for
12869 Enhanced Called Party Hold when the originating switch interconnects with the LNG via
12870 SS7-controlled trunks.

12871 If the legacy originating network supports Enhanced Called Party Hold and the originating
12872 switch interconnects with the LNG via MF trunk groups, an ECPH timer MUST be supported

[MM/DD/YYYY]

Page 539 of 675



12873 at the LNG and the LNG SHALL follow the procedures described in Section C.5.2. The
12874 procedures at the ESRP, LPG, and i3 PSAP will be the same as for Enhanced Called Party
12875 Hold where SS7 trunks are used between the originating switch and the LNG.

12876 Note that if a VoIP originating network does not support feature-specific signaling
12877 associated with PSAP Call Control Features and the caller disconnects before the PSAP
12878 attendant answers the call, a SIP CANCEL MAY be sent by the originating network. The
12879 CANCEL message SHALL be processed as specified in RFC 3261 [10] by all elements in the
12880 call path. As described in Section 4.2.1.9, if a call arrives at the ESRP but a CANCEL is
12881 received prior to any response message being received from an i3 PSAP (or LPG), such that
12882 the ESRP is unsure as to whether or not the INVITE message was ever received by the
12883 PSAP, the ESRP MUST notify the i3 PSAP (or LPG) using the AbandonedCall event.

12884 **C.5.1 Procedures at the LNG for Calls Received over SS7 Trunk Groups**

12885 **C.5.1.1 Procedures at the LNG-PIF Component**

12886 When an originating switch supports Enhanced Called Party Hold and interconnects with
12887 the LNG using SS7-supported trunks, the PIF component of the LNG SHALL follow the
12888 procedures specified in Section C.3.1.1.1.

12889 **C.5.1.2 Procedures at the LNG-NIF Component**

12890 When an originating switch supports Enhanced Called Party Hold and interconnects with
12891 the LNG using SS7-controlled trunks, the NIF component of the LNG SHALL follow the
12892 procedures specified in Section C.3.1.1.2, with the following clarifications.

12893 Upon receiving the original INVITE from the PIF, the NIF component SHALL determine,
12894 based on provisioning associated with the incoming trunk group from the originating
12895 switch, whether Enhanced Called Party Hold is supported. If supported, the NIF component
12896 MUST initiate an ECPH timer which indicates the maximum length of time that Enhanced
12897 Called Party Hold will be active. This timer should be provisionable. If ECPH is not
12898 supported, the ECPH timer MUST NOT be initiated for that call.

12899 If the NIF subsequently receives an INFO message from the PIF component that contains
12900 an encapsulated FAC message with the Feature Code Indicator in the SAP set to
12901 "disconnect request" after a 1XX provisional response has been received but prior to
12902 receiving the 200 OK response to the original INVITE associated with the emergency call,
12903 and Enhanced Called Party Hold is supported, the NIF component SHALL generate an
12904 UPDATE message that contains an SDP offer with an "a=suspended" attribute. If the INFO
12905 message from the PIF component is received before receiving a response (provisional or
12906 final) from the NGCS, the NIF component SHALL send a CANCEL message to the NGCS and

12907 an INFO message containing an encapsulated FAC with a SAP FCI of "hold release request"
12908 to the PIF component.

12909 If the NIF component receives a 200 OK message from the NGCS prior to the expiration of
12910 the ECPH timer, the NIF component SHALL cancel the timer and generate a SIP re-INVITE
12911 message containing an SDP with an "a= suspended" attribute, as specified in Section
12912 C.3.1.1.2. Regular Called Party Hold procedures SHALL apply from this point on.

12913 If, based on provisioning associated with the incoming trunk group, the NIF determines
12914 that Enhanced Called Party Hold is supported, but the NIF component does not receive a
12915 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF SHALL
12916 send a CANCEL message to the NGCS and an INFO message containing an encapsulated
12917 FAC with an SAP FCI of "hold release request" to the PIF component.

12918 Upon receiving the SIP INFO message with the SAP set to "disconnect request" from the
12919 PIF component where Enhanced Called Party Hold is not supported for the incoming trunk
12920 group, the NIF component SHALL send a CANCEL message to the NGCS and an INFO
12921 message containing an encapsulated FAC with an SAP FCI of "hold release request" to the
12922 PIF component.

12923 **C.5.2 Procedures at the LNG for Calls Received over MF Trunk Groups**

12924 **C.5.2.1 Procedures at the LNG-PIF Component**

12925 When an originating switch supports Enhanced Called Party Hold and interconnects with
12926 the LNG using MF trunks, the PIF component of the LNG SHALL follow the procedures
12927 specified in Section C.3.1.2.1, with the following clarification. If the originating switch
12928 supports Enhanced Called Party Hold, and the caller disconnects before the emergency call
12929 is answered by the PSAP, the PIF component will receive an on-hook signal from the
12930 originating switch. The PIF component SHALL use trunk group provisioning to determine its
12931 subsequent behavior. If the provisioning associated with the incoming MF trunk group
12932 indicates that Enhanced Called Party Hold is supported, the PIF component SHALL pass the
12933 on-hook/unseize circuit telephony event to the NIF component using the mechanisms
12934 specified in RFC 5244 [140] (or equivalent).

12935 If the emergency caller subsequently goes off-hook, the PIF component SHALL pass the
12936 off-hook/seizure telephony event to the NIF component using the mechanisms specified in
12937 RFC 5244 [140] (or equivalent).

12938 If the provisioning associated with the incoming MF trunk group indicates that Enhanced
12939 Called Party Hold is not supported, upon receiving an on-hook signal from the originating
12940 switch, the PIF component SHALL send a CANCEL message to the NIF component, and
12941 SHALL be capable of receiving and processing a 200 OK in response.

12942 **C.5.2.2 Procedures at the LNG-NIF Component**

12943 When an originating switch supports Enhanced Called Party Hold and interconnects with
12944 the LNG using MF trunks, the NIF component of the LNG SHALL follow the procedures
12945 specified in Section C.3.1.2.2, with the following exceptions and clarifications.

12946 Upon receiving the original INVITE from the PIF, the NIF component SHALL determine,
12947 based on provisioning associated with the incoming trunk group from the originating
12948 switch, whether Enhanced Called Party Hold is supported. If supported, the NIF component
12949 MUST initiate an ECPH timer which indicates the maximum length of time that Enhanced
12950 Called Party Hold will be active. This timer should be provisionable. If not supported on the
12951 incoming trunk group, the ECPH timer MUST NOT be initiated for that call.

12952 If the NIF subsequently receives an on-hook/unseize circuit event indication from the PIF
12953 component (encoded using RFC 5244 [140] mechanisms or equivalent) after receiving a
12954 1XX provisional response, but prior to receiving the 200 OK response to the original INVITE
12955 associated with the emergency call, and Enhanced Called Party Hold is supported, the NIF
12956 component SHALL generate an UPDATE message that contains an SDP offer with an
12957 "a=suspended" attribute. If the on-hook/unseize circuit event indication from the PIF
12958 component (encoded using RFC 5244 [140] mechanisms or equivalent) is received before
12959 receiving a response (provisional or final) from the NGCS, the NIF component SHALL send
12960 a 487 Request Terminated response message associated to the original INVITE to the PIF
12961 component and a CANCEL to the NGCS.

12962 If Enhanced Called Party Hold is supported on the incoming MF trunk group and the NIF
12963 component receives a 200 OK message from the NGCS prior to the expiration of the ECPH
12964 timer, it SHALL cancel the timer and generate a SIP re-INVITE message containing an SDP
12965 with an "a= suspended" attribute, as specified in Section C.3.1.2.2. Regular Called Party
12966 Hold procedures SHALL apply from this point on.

12967 If Enhanced Called Party Hold is supported on the incoming MF trunk group and the NIF
12968 component does not receive a 200 OK message from the NGCS prior to the expiration of
12969 the ECPH timer, the NIF SHALL send a 487 Request Terminated response message
12970 associated to the original INVITE to the PIF component, and a CANCEL to the NGCS.

12971 If, based on provisioning associated with the incoming trunk group, the NIF determines
12972 that Enhanced Called Party Hold is supported, but the NIF component does not receive a
12973 200 OK message from the NGCS prior to the expiration of the ECPH timer, the NIF SHALL
12974 send a CANCEL message to the NGCS and a 487 Request Terminated response message
12975 associated to the original INVITE to the PIF component.

12976 Upon receiving the on-hook/unseize circuit indication from the PIF component, where
12977 Enhanced Called Party Hold is not supported for the incoming trunk group, the NIF

12978 component SHALL send a CANCEL message to the NGCS and a 487 Request Terminated
12979 response message associated to the original INVITE to the PIF component.

12980 **C.5.3 Procedures at the Bridge**

12981 It is possible that a caller hangs-up intentionally or unintentionally while being connected
12982 to a bridge.

12983 The following sub-sections describe how a premature disconnect before call answer is
12984 propagated by the Bridge.

12985 **C.5.3.1 Using the SIP Ad Hoc Method**

12986 Given that ECPH is invoked prior to the establishment of an emergency call and that the
12987 SIP Ad Hoc Bridge is only invoked to establish a conference, which happens after initial call
12988 answer, it is impossible to encounter ECPH in the SIP Ad Hoc bridging scenario.

12989 **C.5.3.2 Using the Route All Calls via a Conference-Aware UA Method**

12990 Upon receiving a re-INVITE with updated switch-hook status prior to the issuance of the
12991 200 OK message establishing the original emergency call session with the PSAP, the Bridge
12992 using the Conference-Aware UA method SHALL propagate the re-INVITE to the PSAP.
12993 Normal procedures for Called Party Hold/Switch-hook status defined in section C.3 ensue.

12994 **Appendix D – Example Call Flows (informative)**

12995 This section provides example end-to-end i3 call flows. The first example, in Section D.1,
12996 describes a call flow in which all data is provided by value. The second example call flow, in
12997 which data is provided by reference, is presented in Section D.2. Other example calls flows
12998 may be added in future revisions of this document.

12999 **D.1 Data by Value SIP End-to-End Example Call Flow**

13000 The following assumptions and considerations have been taken in creating this example
13001 call flow:

- 13002 • SIP end-to-end call;
- 13003 • AIP and VSP are not vertically integrated;
- 13004 • The Calling Device is nomadic;
- 13005 • The Calling Device is identifiable and authenticable by the LIS to reside within its
13006 administrative domain;
- 13007 • The location format is Civic;
- 13008 • The provisioned location is LVF-valid in the LIS;
- 13009 • The Calling UA is location-capable;
- 13010 • The Calling UA is LoST-capable;
- 13011 • The Calling UA has the VSP Call Server configured as its outbound proxy (by adding
13012 a Route header field pointing to the VSP CS in dialog-initiating requests⁹⁷);
- 13013 • The VSP CS is a proxy;
- 13014 • Two ESInets scenario: the originating ESInet is a state/province ESInet, the
13015 terminating ESInet is a regional ESInet;
- 13016 • All data is provided by-value;
- 13017 • The LIS only supports HELD as a Location Configuration Protocol (LCP);
- 13018 • The Policy Store is external to the ESRP but within its ESInet;
- 13019 • At call time, ESRPs have already collected the Origination and Termination Policies
13020 for Queue Names they manage (enumeratePolicyRequest and response flows not
13021 shown);
- 13022 • BCFs outside ESInets are not shown;
- 13023 • All SIP Proxies are transaction stateful;
- 13024 • Egress BCFs do not anchor media;

97 Most devices don't include a Route header field with the URI of their configured outbound proxy. Rather, they just send every call to that proxy. We elected to show the header to remain strictly compliant with RFC 3261.

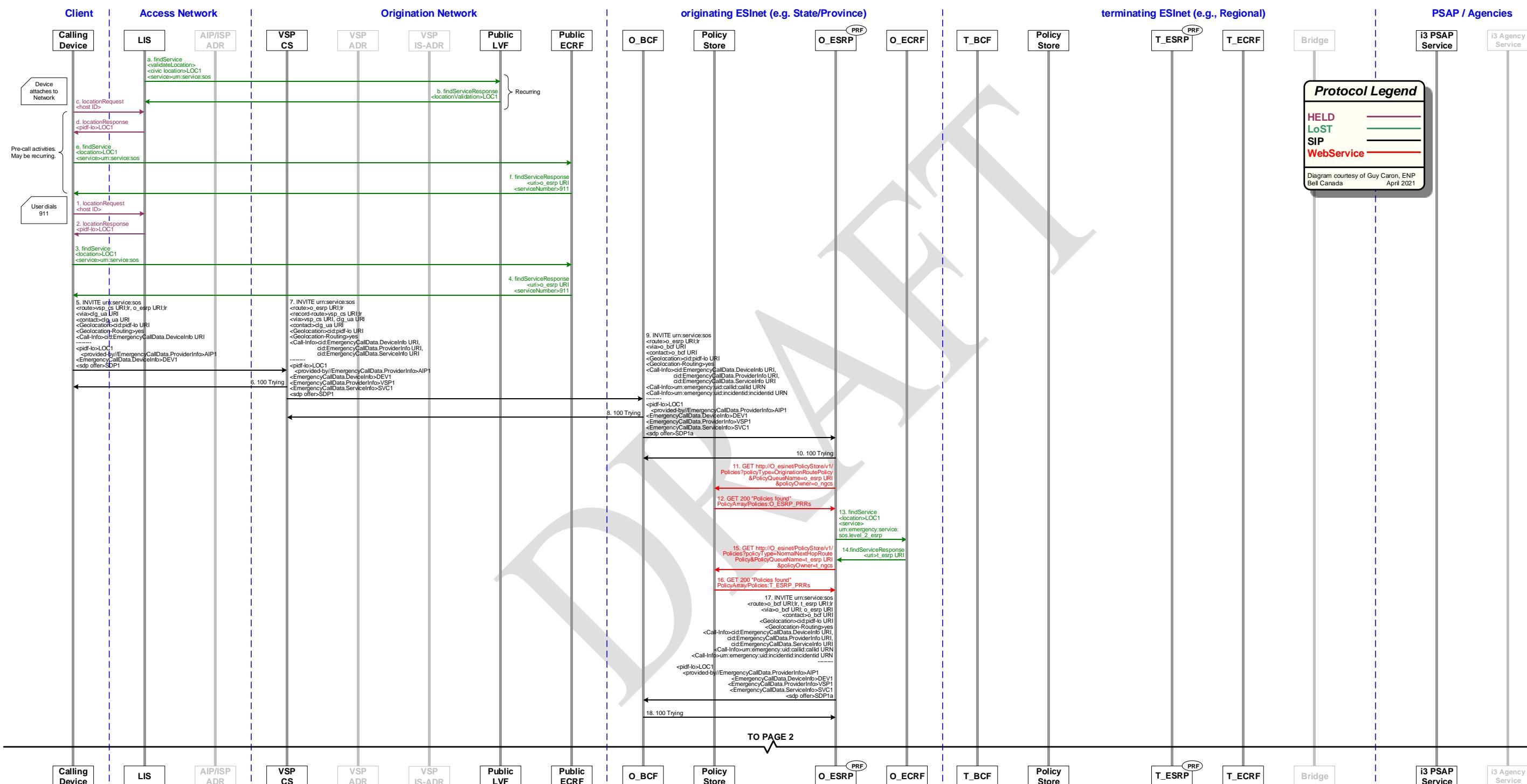
- 13025 • Ingress and egress BCFs are assumed to be the same server (shown as a single
13026 element);
13027 • ESRPs that route calls exiting the local ESInet will send such calls to a BCF facing
13028 the desired next hop (by adding a Route header field pointing to the BCF in dialog-
13029 initiating requests);
13030 • ECRFs return the authoritative answer, either directly or by recursion (not shown);
13031 • All queues are in Normal State;
13032 • PSAP and Agency are served by the same terminating (regional) ESInet;
13033 • All elements within the ESInets have valid credentials traceable back to the PCA;
13034 • External DNS resolution of ESRP URIs is the BCF IP address;
13035 • Internal DNS resolution of internal ESRP URIs is the ESRP IP address;
13036 • Provisioning, Registration, Authentication, Authorization, SIP
13037 Subscription/Notification, Logging, Recording, and Discovery flows have been
13038 omitted for simplicity;
13039 • DNS, DHCP, and NTP flows have been omitted for simplicity;
13040 • TCP with TLS is used for all transactions although not explicitly expressed (e.g., http
13041 vs https).

[MM/DD/YYYY]

Page 545 of 675



13042

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 1

13043

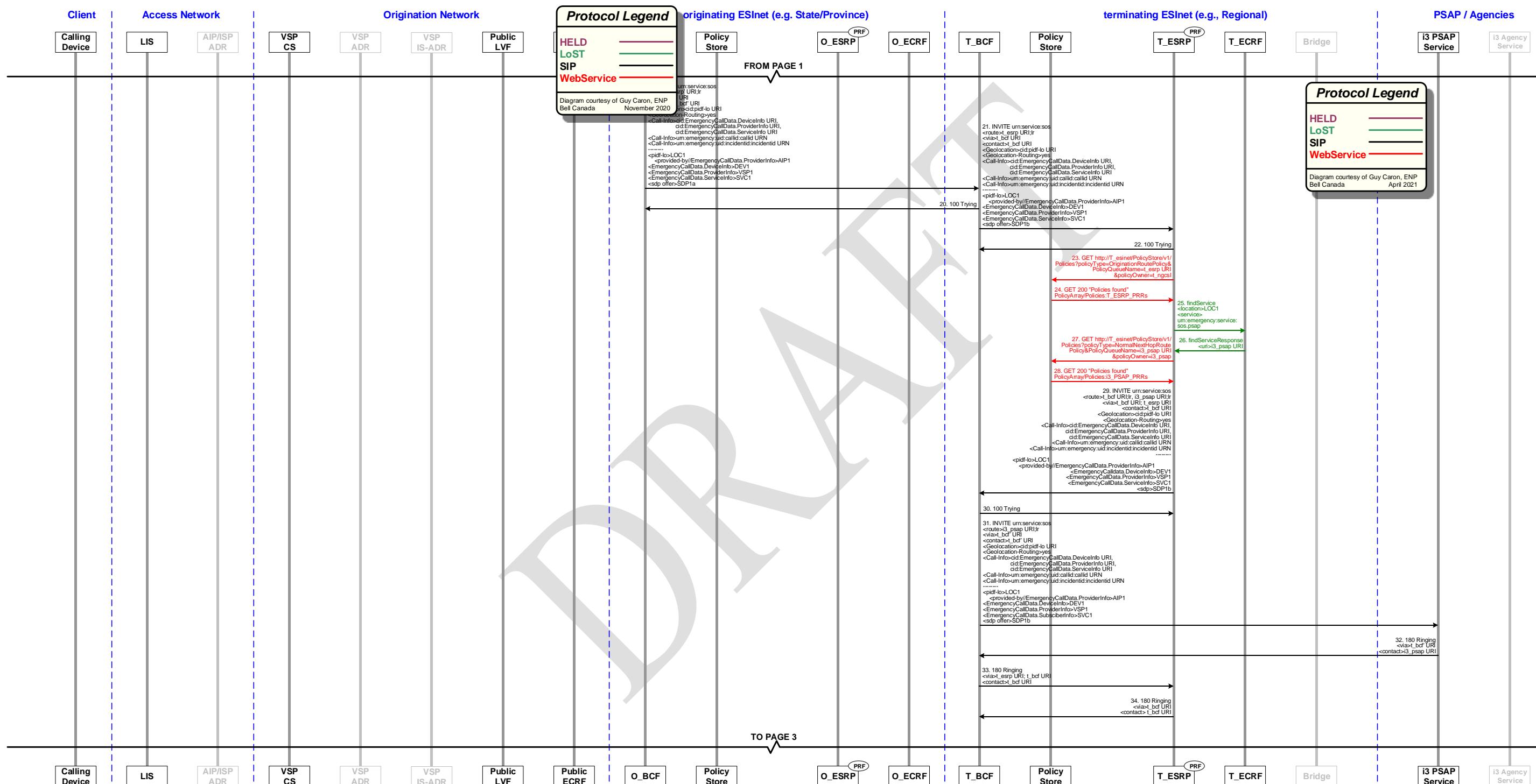
[MM/DD/YYYY]

Page 546 of 675



13044

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 2



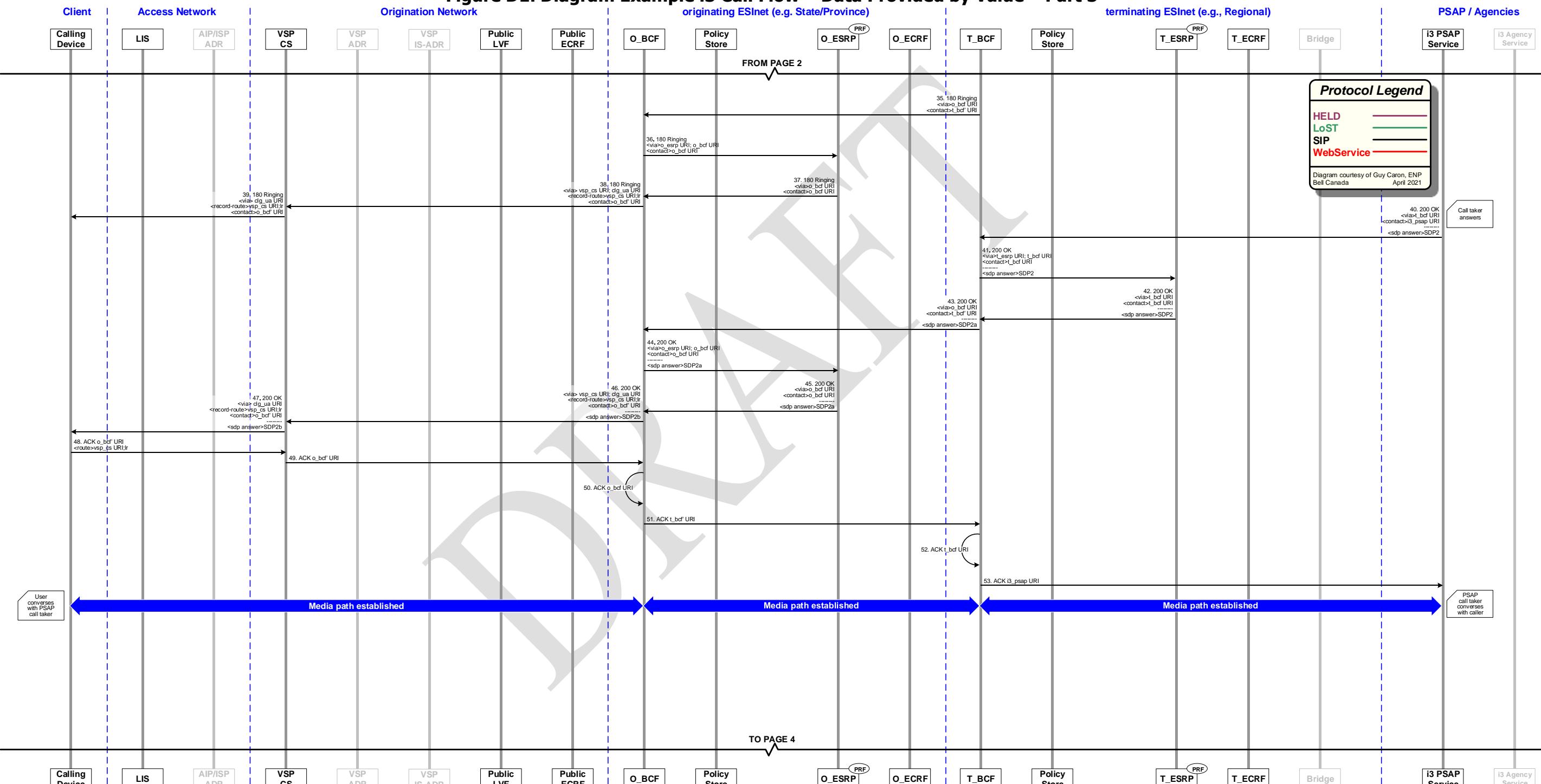
[MM/DD/YYYY]

Page 547 of 675



13046
13047

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 3



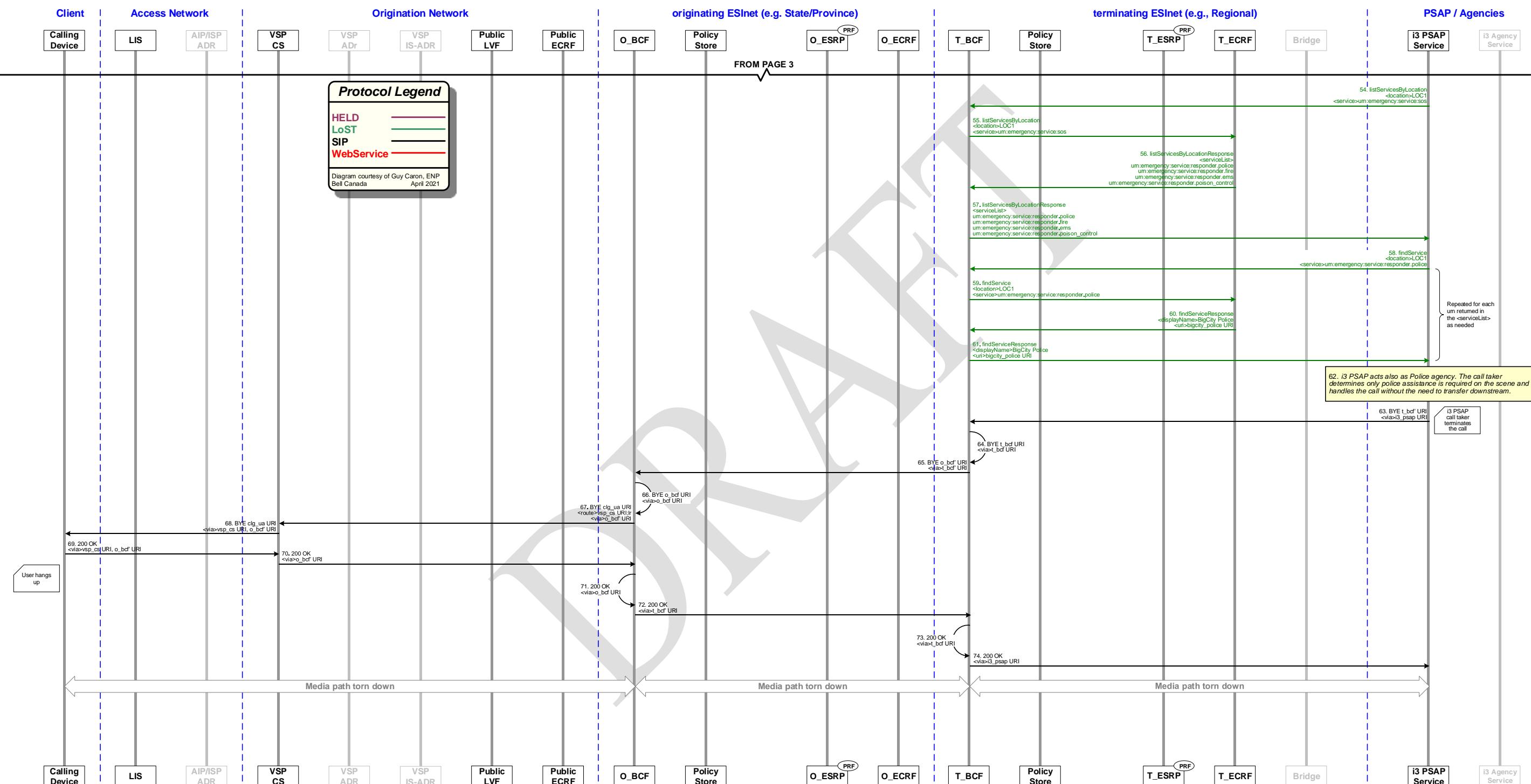
13048

[MM/DD/YYYY]

Page 548 of 675



13049

Figure D1. Diagram Example i3 Call Flow – Data Provided by Value – Part 4

13050

[MM/DD/YYYY]

Page 549 of 675



13051 **D.1.1 Step-by-Step Description**

13052 **D.1.1.1 Boot Up Activities (Steps Not Shown)**

13053 The LIS is statically provisioned with the URL of the Public LVF for its serving footprint. The
13054 LIS in the broadband access network has been provisioned with a record associating the
13055 location "LOC1" (which is LVF-valid) to the identifier "Host ID" of the Calling Device. The
13056 LIS exposes an external HELD interface to the network used by the Calling Device.

13057 The nomadic Calling Device is physically connected to a broadband access network at
13058 location "LOC1".

13059 The Calling Device boots up, attaches to the access network (i.e., it gets a service IP
13060 address and DNS server IP addresses), discovers its serving LIS and serving Public ECRF.

13061 The SIP UA part of the Calling Device registers with its VSP (step not shown). This step
13062 may be recurring based on the settings of the UA. The VSP CS authenticates the Calling
13063 UA.

13064 **D.1.1.2 Pre-Call Activities**

13065 a. The LIS queries the public LVF with a LoST findService location validation request
13066 for the civic address "LOC1" and the service URN "urn:service.sos".

13067 b. The Public LVF processes the validation request and returns a LoST
13068 findServiceResponse to the LIS showing "LOC1" as LVF-valid.

13069 *Steps a. and b. are recurring periodically to ensure any changes in GIS information are
13070 reflected in the LIS.*

13071 c. The Calling Device supports HELD and DHCP as Location Configuration Protocols but
13072 only the HELD request will successfully provide a location since the discovered LIS
13073 supports HELD as the LCP. The HELD locationRequest contains the Calling Device
13074 "host ID" and appropriate credentials.

13075 d. The LIS authenticates the Calling Device (step not shown), processes the request
13076 and responds with a HELD locationResponse containing a PIDF-LO representation of
13077 civic address "LOC1", including the element <provided-by> populated with the
13078 access provider ID "AIP1".

13079 e. Using civic location "LOC1" and service URN "urn:service.sos", the Calling Device
13080 initiates a LoST findService request to the Public ECRF previously discovered. The
13081 Public ECRF does not require authentication so no credentials are provided.

13082 f. The Public ECRF processes the request without authentication and responds with a
13083 LoST findServiceResponse containing among other things the destination URI for

13084 emergency calling <uri> "o_esrp URI" and the emergency number
13085 <serviceNumber> "911" for this area.

13086 *Steps c. to f. may recur. The rate of recurrency will be influenced by many factors*
13087 *associated with the device and the network to which it is attached. For example, the*
13088 *device may be configured to initiate a HELD locationRequest every time it is powered*
13089 *up and every 30 minutes thereafter. The same is true of the LoST findService request.*

13090 **D.1.1.3 Call-Related Activities**

1. The user is confronted with an emergency situation and uses the Calling Device to dial the emergency number he is accustomed to (in this example, 911). The Calling Device recognizes the dial string "911" as the emergency service number in the area of location "LOC1" (by comparing it to what was previously discovered in Step e), enters into "emergency calling mode", and following the advice in RFC 6881, adapts its behavior accordingly (for example, disabling certain features) and gets an updated location by querying the LIS using HELD. The HELD locationRequest contains the Calling Device "host ID" and appropriate credentials
2. The LIS authenticates the Calling Device (step not shown), processes the request, and responds with a HELD locationResponse containing a PIDF-LO representation of civic address "LOC1", including the element <provided-by> populated with the access provider ID "AIP1".
3. Using civic location "LOC1" and service URN "urn:service.sos", the Calling Device initiates a LoST findService request again to the Public ECRF previously discovered. The Public ECRF does not require authentication so no credentials are provided.
4. The Public ECRF processes the request without authentication and responds with a LoST findServiceResponse containing, among other things, the destination URI for emergency calling <uri> "o_esrp URI", and the emergency number <serviceNumber> "911" for this area.
5. The Calling SIP UA sends an INVITE with the Request-URI set to "urn:service.sos", a Route header field set to the VSP CS (outbound proxy) with the "lr" parameter, another Route header field set to the value received in the LoST response of Step 2 ("o_esrp URI") augmented with the "lr" parameter, a Contact header field for itself ("clg_ua URI"), and a Geolocation header field with a cid URI pointing to the PIDF-LO document embedded in the body, along with its SDP offer "SDP1". It also includes a Call-Info header field with a purpose parameter set to "EmergencyCallData.DeviceInfo" and a cid URI pointing to Additional Data about itself in the body <EmergencyCallData.DeviceInfo> "DEV1". It also includes a Call-Info header field with a purpose parameter set to "EmergencyCallData.ProviderInfo" and a cid URI pointing to Additional Data about itself in the body

- 13121 <EmergencyCallData.ProviderInfo>. Both additional data body blocks contain a
13122 <DataProviderReference> element set to the same value.
- 13123 6. The VSP CS receives the INVITE, authenticates the Calling UA (steps not shown), and
13124 replies with a provisional 100 Trying SIP response to the Calling UA.
- 13125 7. The VSP CS recognizes the Request-URI in the INVITE set to "urn:service:sos" to be
13126 an emergency call and invokes special logic to process this message. In the forwarded
13127 INVITE, it removes the first Route header field referring to itself and adds Via and
13128 Record-Route header fields pointing to itself ("vsp_cs URI"). It also adds Call-Info
13129 header field values, each with a purpose parameter beginning with
13130 "EmergencyCallData" and cid URIs pointing to the appropriate data element in the
13131 body. It then includes the related data elements in the body, namely
13132 <EmergencyCallData.ProviderInfo> "VSP1" (additional data about the originating
13133 network or service provider), and <EmergencyCallData.SubscriberInfo> "SUB1"
13134 (additional data about the subscriber). The SDP offer "SDP1" remains since the VSP
13135 CS does not anchor media. The VSP CS performs a DNS lookup on the URI found in
13136 the Route header field ("o_esrp URI") of the incoming INVITE. The DNS resolution of
13137 this URI in the originating network returns the O_BCF IP address(es). The INVITE is
13138 forwarded there.
- 13139 8. The O_BCF receives the INVITE, inspects the message for malicious content (step not
13140 shown), and replies with a provisional 100 Trying SIP response to the VSP CS. In
13141 some cases the O_BCF authenticates the VSP CS (e.g., if there is a relationship with
13142 the VSP).
- 13143 9. The O_BCF behaves as a full B2BUA, performs topology hiding, anchors media, and
13144 acts as the UAS for the ingress dialog. On the egress side, acting as a UAC, it creates
13145 a new transaction for the egress dialog by sending an INVITE populated with a Route
13146 header field set to "o_esrp URI;lr", Via, and Contact header fields pointing to itself
13147 ("o_bcf URI"), and an SDP offer "SDP1a". It generates Call and Incident tracking
13148 identifiers and adds them to Call-Info header fields with purpose parameters of
13149 "emergency-CallId" and "emergency-IncidentId" respectively. It also copies the Call-
13150 Info, Geolocation header field, and Geoloaction-Routing fields found in the incoming
13151 INVITE, as well as the other elements found in the body. The O_BCF then performs a
13152 DNS lookup on the URI found in the Route header field ("o_esrp URI") of the INVITE.
13153 The DNS resolution of this URI in the originating (state) ESInet returns the O_ESRP IP
13154 address(es). The INVITE is forwarded there. The O_BCF maintains independently the
13155 state of the ingress and egress dialog-initiating transactions as well as the association
13156 between them.
- 13157 10. The O_ESRP receives the INVITE on the call queue associated with "o_esrp URI",
13158 authenticates the O_BCF (steps not shown), and responds with a provisional 100
13159 Trying SIP message to the O_BCF. It deletes the top Route header field referring to it.

- 13160 11. The O_ESRP is statically provisioned with the address of its Policy Store. It formulates
13161 a RetrievePolicy through an HTTP GET request to O_esinet/PolicyStore/v1/Policies
13162 (with parameters <policyType> as "OriginationRoutePolicy", "policyQueueName" as
13163 "o_esrpURI", which is the URI of the queue the call was received on and
13164 "policyOwner" as "p_ngcs", which is the Agency Identifier of the agency responsible
13165 for O_ESRP) to retrieve the originating route policies associated with it. Credentials are
13166 also provided.
- 13167 12. The "O_esinet" Policy Store is provisioned with all the policies associated with its
13168 serving clients (step not shown). It receives the RetrievePolicy HTTP GET request,
13169 authenticates the O_ESRP, then dips into its database to find a record associated with
13170 the provided parameters. It returns the result in an HTTP response message with the
13171 origination route policy set for queue "o_esrp URI" in a PolicyArray object.
- 13172 13. The O_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules
13173 in the policy received and applies them to the incoming INVITE (step not shown). The
13174 origination policy contains the highest priority rule specifying a
13175 LoSTServiceURNCondition object which, when executed, results in a LoST query to its
13176 serving O_ECRF. The O_ESRP is provisioned with the address of the O_ECRF. It
13177 launches a LoST findService request with the following parameters: <location>
13178 "LOC1" as found in the body of the INVITE, <service>
13179 "urn:emergency:service:sos.level_2_esrp" as found in the originating policy.
13180 Credentials are also provided.
- 13181 14. The O_ECRF authenticates the O_ESRP, processes the request for "LOC1" and
13182 "urn:emergency:service:sos.level_2_esrp", and returns a LoST findService Response
13183 with the URI of the next hop ("t_esrp URI") to the O_ESRP.
- 13184 15. The O_ESRP receives the LoST response since the ECRF query was successful, it
13185 stores the URI received in the Normal-NextHop variable and then executes the actions
13186 associated to the rule containing the "LoSTServiceURNCondition" object. One of the
13187 actions contains an "InvokePolicyAction" actionType with "policyType" set to
13188 "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated
13189 with "t_esrp URI". As such, it formulates a RetrievePolicy HTTP GET request to
13190 O_esinet/PolicyStore/v1/Policies (with parameters "policyType" as
13191 "NormalNexthopRoutePolicy" and "policyQueueName" as "t_esrp URI", which is the
13192 URI stored in the Normal-NextHop variable and "policyOwner" as "t_ngcs", which is
13193 the Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination
13194 policy associated with it. Credentials are also provided.
- 13195 16. The Policy Store receives the RetrievePolicy HTTP GET request, authenticates the
13196 O_ESRP, then dips into its database to find a record associated with the provided
13197 parameters. It returns the result in a response message with the route policy for
13198 queue "t_esrp URI" in a PolicyArray object.

[MM/DD/YYYY]

Page 553 of 675

- 13199 17. The O_ESRP invokes its internal PRF that processes the rules within the policy
13200 received to determine where to send the INVITE. The route policy has a Route action
13201 that forwards the call to the normalNextHop that, in this case, is the T_ESRP. The
13202 O_ESRP adds a Route header field set to "t_esrp URI;lr" and adds a Via header field
13203 pointing to itself ("o_esrp URI"). Following its provisioned behavior for all calls exiting
13204 the local ESInet, the O_ESRP then adds a front value in the topmost Route header
13205 field pointing to its desired next hop "o_bcf URI;lr", performs a DNS lookup on it, and
13206 sends the INVITE to the O_BCF IP address.
- 13207 18. The O_BCF receives the INVITE, inspects the message for malicious content,
13208 authenticates the O_ESRP (steps not shown), and replies with a provisional 100 Trying
13209 SIP response to the O_ESRP.
- 13210 19. The O_BCF behaves as a full B2BUA⁹⁸ and terminates the ingress dialog. On the
13211 egress side, it creates a new dialog by sending an INVITE populated with a Route
13212 header field set to "t_esrp' URI;lr", Via and Contact header fields pointing to itself
13213 ("o_bcf' URI"), and copies the Call-Info, Geolocation and Geolocation-Routing header
13214 fields, and the elements found in the body of the incoming INVITE, including the SDP
13215 offer "SDP1a". The O_BCF then performs a DNS lookup on the URI found in the Route
13216 header field ("t_esrp' URI") of the INVITE. The DNS resolution of this URI in the
13217 originating ESInet returns the T_BCF IP address(es). The INVITE is forwarded there.
13218 The O_BCF maintains independently the state of the ingress and egress dialogs as well
13219 as the association between the two dialogs.
- 13220 20. The T_BCF receives the INVITE, inspects the message for malicious content,
13221 authenticates the O_BCF (steps not shown), and responds with a provisional 100
13222 Trying SIP message to the O_BCF.
- 13223 21. The T_BCF behaves as a full B2BUA⁹⁸, anchors media, and acts as the UAS for the
13224 ingress dialog. On the egress side, acting as a UAC, it creates a new transaction for
13225 the egress dialog by sending an INVITE populated with a Route header field set to
13226 "t_esrp URI;lr", Via and Contact header fields pointing to itself ("t_bcf URI"), and an
13227 SDP offer "SDP1b". It also copies the Call-Info, Geolocation and Geolocation-Routing
13228 header fields, and other elements found in the body of the incoming INVITE. The
13229 T_BCF then performs a DNS lookup on the URI found in the Route header field
13230 ("t_esrp URI") of the INVITE. The DNS resolution of this URI in the terminating
13231 (regional) ESInet returns the T_ESRP IP address(es). The INVITE is forwarded there.
13232 The T_BCF maintains independently the state of the ingress and egress dialog-
13233 initiating transactions as well as the association between them.

⁹⁸ Topology hiding may occur between ESInets, but consideration should be given to not doing so in support of improved ability to diagnose problems.

- 13234 22. The T_ESRP receives the INVITE on the call queue associated with "t_esrp URI",
13235 authenticates the T_BCF (steps not shown), and responds with a provisional 100
13236 Trying SIP message to the T_BCF. It deletes the top Route header field referring to it.
- 13237 23. The T_ESRP is statically provisioned with the address of its Policy Store. It formulates
13238 a RetrievePolicy through an HTTP GET request to T_esinet/PolicyStore/v1/Policies
13239 (with parameters "policyType" as "OriginationRoutePolicy", "policyQueueName" as
13240 "t_esrp URI", which is the URI of the queue the call was received on and
13241 "policyOwner" as "t_ngcs", which is the Agency Identifier of the agency responsible for
13242 T_ESRP) to retrieve the origination route policy set associated with it. Credentials are
13243 also provided.
- 13244 24. The "T_esinet" Policy Store is provisioned with all the policies associated with its
13245 serving clients (step not shown). It receives the RetrievePolicy HTTP GET request,
13246 authenticates the T_ESRP, then queries its database to find a record associated with
13247 the provided parameters. It returns the result in a response message with the
13248 origination route policy set for queue "t_esrp URI" in a PolicyArray object.
- 13249 25. The T_ESRP invokes its internal Policy Routing Function (PRF) that processes the rules
13250 in the policy received and applies them to the incoming INVITE (step not shown). The
13251 origination policy contains the highest priority rule specifying a
13252 LoSTServiceURNCondition object which, when executed, results in a LoST query to its
13253 serving T_ECRF. The T_ESRP is provisioned with the address of the T_ECRF. It
13254 launches a LoST findService request with the following parameters: <location>
13255 "LOC1" as found in the body of the INVITE, <service>
13256 "urn:emergency:service:sos.psap" as found in the originating policy. Credentials are
13257 also provided.
- 13258 26. The T_ECRF authenticates the T_ESRP, processes the request for "LOC1" and
13259 "urn:emergency:service:sos.psap", and returns a LoST findServiceResponse with the
13260 URI of the next hop ("i3_psap URI") to the T_ESRP.
- 13261 27. The T_ESRP receives the LoST response and since the ECRF query was successful, it
13262 stores the URI received in the NormalNextHop variable and then executes the actions
13263 associated to the rule containing the "LoSTServiceURNCondition" object. One of the
13264 actions contains an "InvokePolicyAction" actionType with "policyType" set to
13265 "NormalNexthopRoutePolicy" thus it determines it requires the route policy associated
13266 with "i3_psap URI". As such, it formulates a RetrievePolicy HTTP GET request to
13267 T_esinet/PolicyStore/v1/Policies (with parameters "policyType" as
13268 "NormalNexthopRoutePolicy" and "policyQueueName" as "i3_psap URI", which is the
13269 URI stored in the NormalNextHop variable and "policyOwner" as "i3_psap", which is
13270 the Agency Identifier of the agency responsible for i3_PSAP) to retrieve the origination
13271 route policy set associated with it.. Credentials are also provided.

[MM/DD/YYYY]

Page 555 of 675

- 13272 28. The Policy Store receives the RetrievePolicy HTTP GET request,, authenticates the
13273 T_ESRP, then queries its database to find a record associated with the provided
13274 parameters. It returns the result in a response message with the route policy for
13275 queue "i3_psap URI" in a PolicyArray object.
- 13276 29. The T_ESRP invokes its internal PRF that processes the rules within the policy received
13277 to determine where to send the INVITE. The route policy has a Route action that
13278 forwards the call to the normalNextHop that, in this case, is the i3_PSAP. The T_ESRP
13279 adds a Route header field set to "i3_psap URI;lr" and adds a Via header field pointing
13280 to itself ("t_esrp URI"). Following its provisioned behavior for all calls exiting the local
13281 ESInet, the T_ESRP then adds front value in the topmost Route header field pointing
13282 to its desired next hop "t_bcf URI;lr", performs a DNS lookup on it, and sends the
13283 INVITE to the T_BCF IP address.
- 13284 30. The T_BCF receives the INVITE, inspects the message for malicious content,
13285 authenticates the T_ESRP (steps not shown), and replies with a provisional 100 Trying
13286 SIP response to the T_ESRP.
- 13287 31. The T_BCF behaves as a full B2BUA⁹⁸ and terminates the ingress dialog. On the egress
13288 side, it creates a new dialog by sending an INVITE populated with a Route header
13289 field set to "i3_psap URI;lr", a Via header field pointing to itself ("t_bcf' URI"), and
13290 copies the Call-Info, Geolocation and Geolocation-Routing header fields, and the
13291 elements found in the body of the incoming INVITE, including the SDP offer "SDP1b".
13292 The T_BCF then performs a DNS lookup on the URI found in the Route header field
13293 ("i3_psap URI") of the INVITE. The DNS resolution of this URI in the regional
13294 (terminating) ESInet returns the i3_PSAP IP address(es). The INVITE is forwarded
13295 there. The T_BCF maintains independently the state of the ingress and egress dialogs
13296 as well as the association between the two dialogs.
- 13297 32. The i3_PSAP receives the INVITE, authenticates the T_BCF (steps not shown),
13298 presents the call on its normal call queue for the next available agent to answer, and
13299 replies with a provisional 180 Ringing⁹⁹ SIP response to the URI found in the top Via
13300 header field ("t_bcf' URI").
- 13301 33. The T_BCF receives the provisional 180 Ringing message on the egress transaction
13302 and creates a reciprocal response on the ingress transaction using the Via header
13303 fields of the associated ingress INVITE pointing to the T_ESRP.
- 13304 34. The T_ESRP receives the provisional 180 Ringing message, removes the Via header
13305 field referring to it, and forwards the response to the URI in the next Via header field,
13306 in this case, the T_BCF.

⁹⁹ The 180 Ringing message may be preceded by a 100 Trying message.

- 13307 35. The T_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_BCF.
- 13310 36. The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.
- 13313 37. The O_ESRP receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.
- 13316 38. The O_BCF receives the provisional 180 Ringing message on the egress dialog and creates a reciprocal response on the ingress dialog using the Via header fields of the associated ingress INVITE pointing to the VSP CS. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. It provides a different value in the Contact header field ("o_bcf' URI").
- 13321 39. The VSP CS receives the provisional 180 Ringing message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.
- 13324 *The Calling UA receives the provisional 180 Ringing SIP response, authenticates the VSP CS (steps not shown), processes the response, and generates a ring back tone towards the hearing medium (speaker phone, handset, headset, etc.) to alert the user that the call has reached its destination.*
- 13328 *Some ringing cycles later, the i3 PSAP call taker answers the call.*
- 13329 40. The i3 PSAP returns a final 200 OK SIP response to the URI found in the Via header field ("t_bcf' URI") with its SDP answer set to "SDP2".
- 13331 41. The T_BCF receives the final 200 OK message on the egress transaction, marking the establishment of the egress dialog. It creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the T_ESRP.
- 13335 42. The T_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the T_BCF.
- 13338 43. The T_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_BCF. Because it anchors media on ingress, the SDP answer is now "SDP2a". It also provides a different value in the Contact header field ("t_bcf' URI").

- 13343 44. The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the O_ESRP.
- 13346 45. The O_ESRP receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the O_BCF.
- 13349 46. The O_BCF receives the final 200 OK message on the egress transaction and creates a reciprocal response on the ingress transaction using the Via header fields of the associated ingress INVITE pointing to the VSP CS. The O_BCF also reinstates the Record-Route header field previously received in the INVITE. Because it anchors media on ingress, the SDP answer is now "SDP2b". It also provides a different value in the Contact header field ("o_bcf' URI").
- 13355 47. The VSP CS receives the final 200 OK message, removes the Via header field referring to it, and forwards the response to the URI in the next Via header field, in this case, the Calling UA.
- 13358 48. The Calling UA receives the final 200 OK response, builds its route-set with the information received in the Record-Route ("vsp_cs URI"). After accepting the session media offer, it then creates an ACK request with Route header fields set to the values of its route-set. It sets the Request-URI to the value of the Contact header field ("o_bcf' URI") and sends the ACK to the top Route header field, in this case, the VSP CS.
- 13364 49. The VSP CS removes the Route header field referring to it and forwards the ACK using the Request-URI ("o_bcf' URI").
- 13366 50. The O_BCF behaves as a full B2BUA⁹⁸. On the egress side, it sends an ACK populated with a Request-URI set to "o_bcf URI" found in the Contact header field of the associated 200 OK response (step 44).
- 13369 51. The O_BCF behaves as a full B2BUA⁹⁸ and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "t_bcf' URI" found in the Contact header field of the associated 200 OK response (Step 43).
- 13373 52. The T_BCF behaves as a full B2BUA⁹⁸ and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "t_bcf URI" found in the Contact header field of the associated 200 OK response (Step 41).
- 13377 53. The T_BCF behaves as a full B2BUA⁹⁸, performs topology hiding, and terminates the ingress dialog. On the egress side, it uses the previously opened egress dialog and sends an ACK populated with a Request-URI set to "i3_psap URI" found in the Contact header field of the associated 200 OK response (Step 40).

- 13381 *Media path is established between the Calling UA and the i3 PSAP with anchoring*
13382 *points at the BCFs (SBC part). Conversation between the call taker and the caller*
13383 *commences.*
- 13384 54. The i3 PSAP has built-in logic to gather agency information in preparation of a
13385 potential transfer to downstream agencies. The i3 PSAP is provisioned with its serving
13386 ECRF (T_ECRF), however the T_ECRF is only reachable by a static route through the
13387 T_BCF (firewall part). The i3 PSAP sends a LoST listServicesByLocation request using
13388 "LOC1" received in the INVITE against the top-level service URN
13389 "urn:emergency:service:sos". Credentials are also provided.
- 13390 55. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the
13391 source and destination IP addresses, inspects the message for malicious content, and
13392 lets the message go through to the T_ECRF.
- 13393 56. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST request,
13394 dips in its database for "LOC1", and formulates a LoST listServicesByLocationResponse
13395 populated with the services available for "LOC1"
13396 ("urn:emergency:service:responder.police", "urn:emergency:service:responder.fire",
13397 "urn:emergency:service:responder.ems", and
13398 "urn:emergency:service:responder.poison_control") back to the i3 PSAP through the
13399 T_BCF.
- 13400 57. The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the
13401 source and destination IP addresses, inspects the message for malicious content, and
13402 lets the message go through to the i3 PSAP.
- 13403 58. With the list of available services in hand, the i3 PSAP proactively launches a LoST
13404 findServiceRequest to the T_ECRF for each of the services available. As above, the
13405 requests are sent to the T_BCF (firewall part). In this example, only the
13406 "urn:emergency:service:responder.police" service URN is shown.
- 13407 59. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the
13408 source and destination IP addresses, inspects the message for malicious content, and
13409 lets the message go through to the T_ECRF.
- 13410 60. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST
13411 requests, dips in its database for "LOC1" and the service URN provided in the requests
13412 (in this example, "urn:emergency:service:responder.police"), and formulates LoST
13413 findServiceResponse messages populated with the URI of the requested service along
13414 with the display name of the agency (a.k.a., English Language Translation) back to the
13415 i3 PSAP through the T_BCF.
- 13416 61. The T_BCF (firewall part) receives the LoST response from the T_ECRF, examines the
13417 source and destination IP addresses, inspects the message for malicious content, and
13418 lets the message go through to the i3 PSAP.

- 13419 62. The i3 PSAP acts also as the police agency. The call taker determines only police
13420 assistance is required on the scene and handles the call without the need to transfer
13421 downstream.
- 13422 *Once all the information has been gathered and the caller is comforted that first*
13423 *responders are on their way, the call taker terminates the call (hangs up).*
- 13424 63.-68. Upon detecting the hang-up signal, the i3 PSAP sends a SIP BYE request towards
13425 the Calling UA. Each UAS and B2BUA uses its route-set and Contact header fields
13426 previously populated for its dialog(s) to populate the Route header fields and
13427 Request-URIs. The BYE request is propagated on the path, each element applying the
13428 routing logic gathered from the associated dialog until it reaches the Calling UA.
- 13429 69.-74. The Calling UA receives the BYE request and starts the tear down procedures. It
13430 then sends a final 200 OK response that gets propagated on the reverse path towards
13431 the i3 PSAP terminating the dialog and the session.
- 13432 *The media is torn down end-to-end. This emergency call is over.*

13433 **D.2 Location by Reference / Cellular / HELD Example Call Flow**

13434 The following assumptions and considerations apply to this example call flow:

- 13435 • SIP end-to-end call (e.g., on a 4G VoLTE IMS-based network);
- 13436 • AIP, and VSP are the same entity (an IMS cellular provider);
- 13437 • The Calling Device is mobile (an IMS cellular device);
- 13438 • The cellular provider does not offer a public LIS;
- 13439 • i3-required LIS functionality is provided by a Location Retrieval Function (LRF);
- 13440 • The LRF (as the LIS) supports location references using HELD deref (the “pull”
13441 model);
- 13442 • The location for dispatch format is geospatial;
- 13443 • The Calling UA uses the P-CSCF as its outbound proxy by sending all requests to it;
- 13444 • The Calling Device and originating network provide Additional Data by value100;
- 13445 • The Policy Store is external to the ESRP but within its ESInet;
- 13446 • At call time, ESRPs have already collected the Origination and Termination Policies
13447 for Queue Names they manage (enumeratePolicy request and response flows not
13448 shown);
- 13449 • The originating network’s BCF (the IMS cellular provider, an IBCF) is not shown;
- 13450 • All SIP Proxies are transaction stateful;
- 13451 • Egress BCFs do not anchor media;

¹⁰⁰ It is recommended to provide Additional Data by-reference to avoid overloading the SIP INVITE. The by-value method is used here to simplify the data flow.

- ESRPs that route calls exiting the local ESInet will send such calls to a BCF facing the desired next hop (by adding a Route header field pointing to the BCF in dialog-initiating requests) (not shown);
- ECRFs return the authoritative answer, either directly or by recursion (not shown);
- All queues are in Normal State;
- PSAP and Agency are served by the same terminating (regional) ESInet;
- All elements within the ESInets have valid credentials traceable to the PCA;
- External DNS resolution of ESRP URIs returns one or more IP addresses for a BCF;
- Internal DNS resolution of internal ESRP URIs returns one or more IP addresses for an ESRP;
- DNS, DHCP, and NTP flows have been omitted for simplicity;
- TCP with TLS is used for all transactions, although not explicitly expressed (e.g., http vs https).
- The cell site to which the Calling Device is connected has an associated location (for routing), in this call flow termed “LOC-AS”; dereference of the location reference for routing returns this location.
- Prior to availability of position determination results, dereference of the location reference returns the location of the cell site to which the Calling Device is connected (in cellular terminology, a Phase I location); in this call flow termed “LOC-P1”.
- An updated location estimate for the Calling Device is available after position determination (e.g., control plane or SUPL) procedures (in cellular terminology, a Phase II location); in this call flow termed “LOC-P2”.
- The call-related steps in D.1 are shown; unchanged steps retain their number and additionally have “(changed)” prepended; steps that differ have a letter appended (e.g., a modified Step 1 is denoted as “1a”); additional steps have a sub-number appended (e.g., “1.1” and “1.2” denote two steps inserted after Step 1).
- The bootup and pre-call steps are entirely different since the cellular network in the example does not provide a public LIS nor use a public ECRF nor an LVF (because dispatch locations are geospatial rather than civic), and the Calling Device does not obtain its own location, nor a location reference, nor does it query a LIS or ECRF.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 1

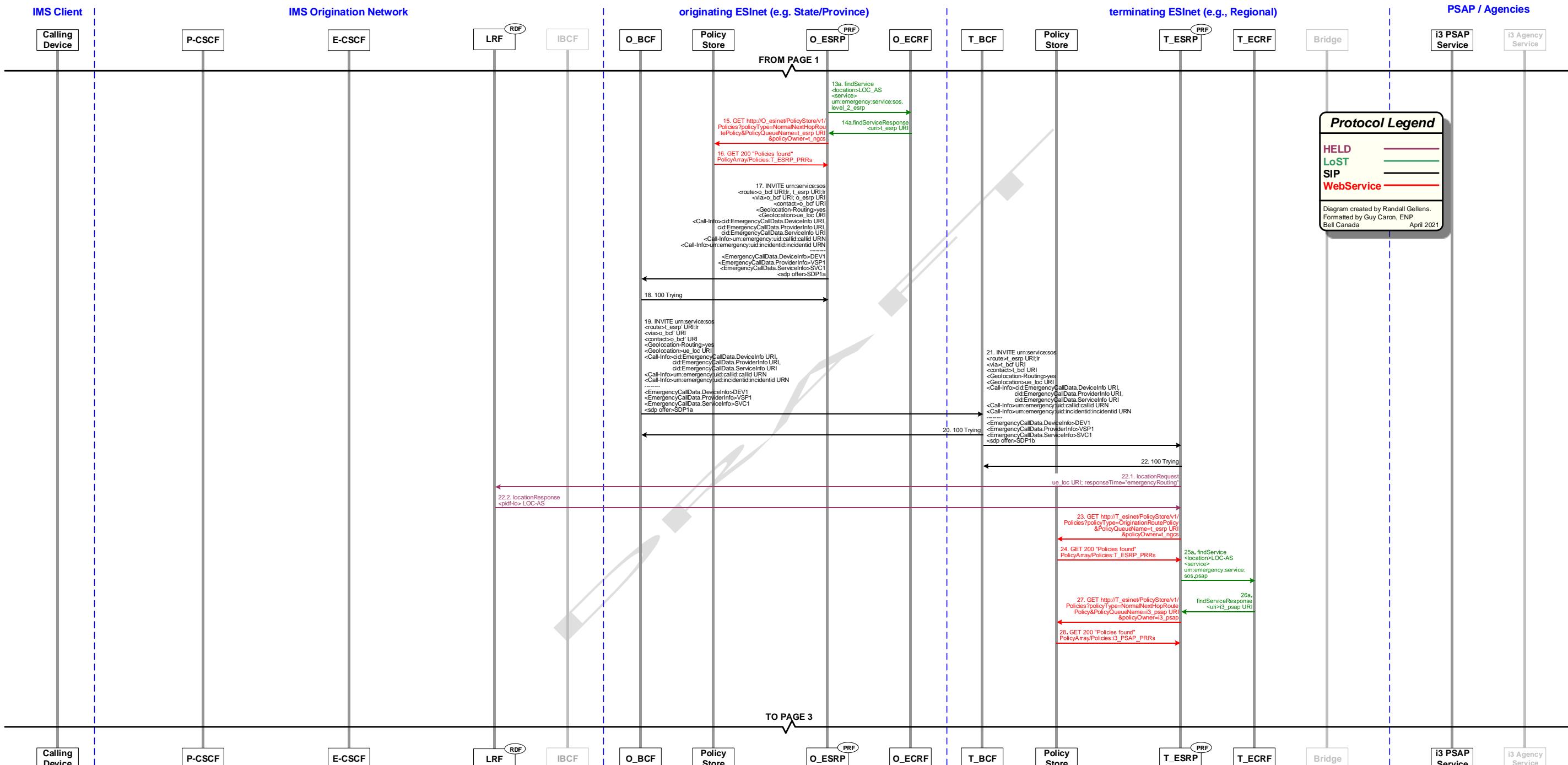


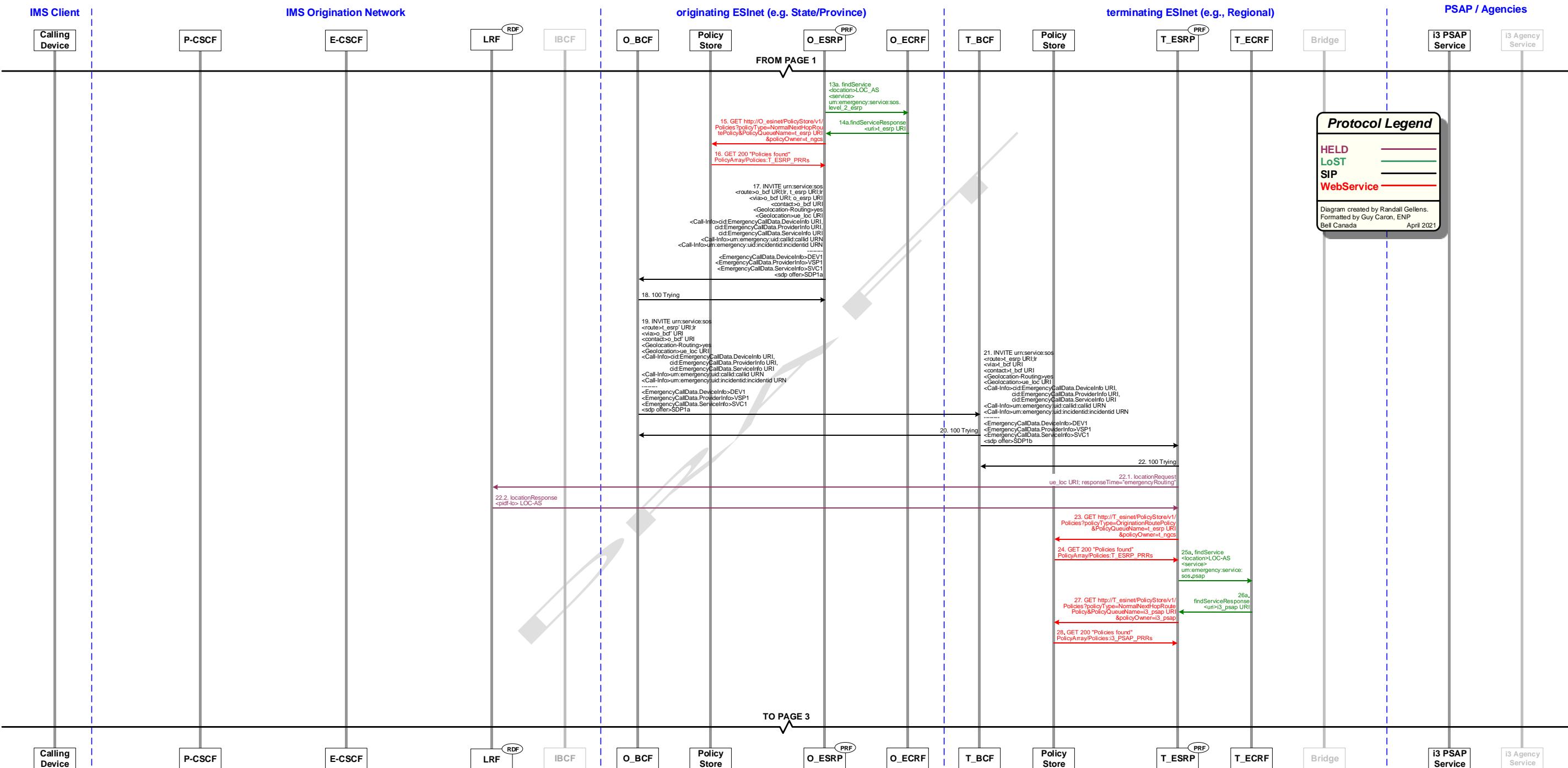
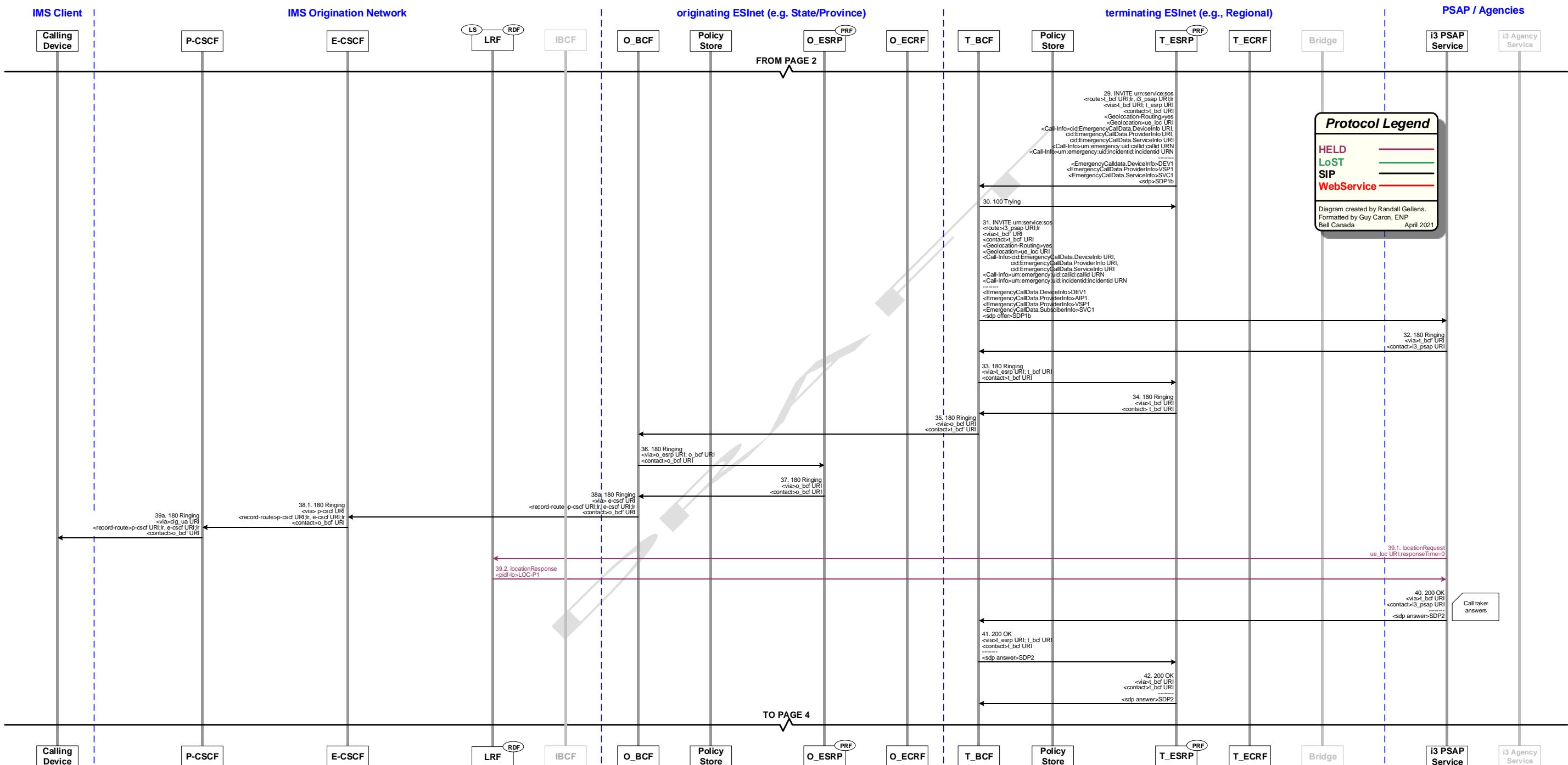
Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 2

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 3



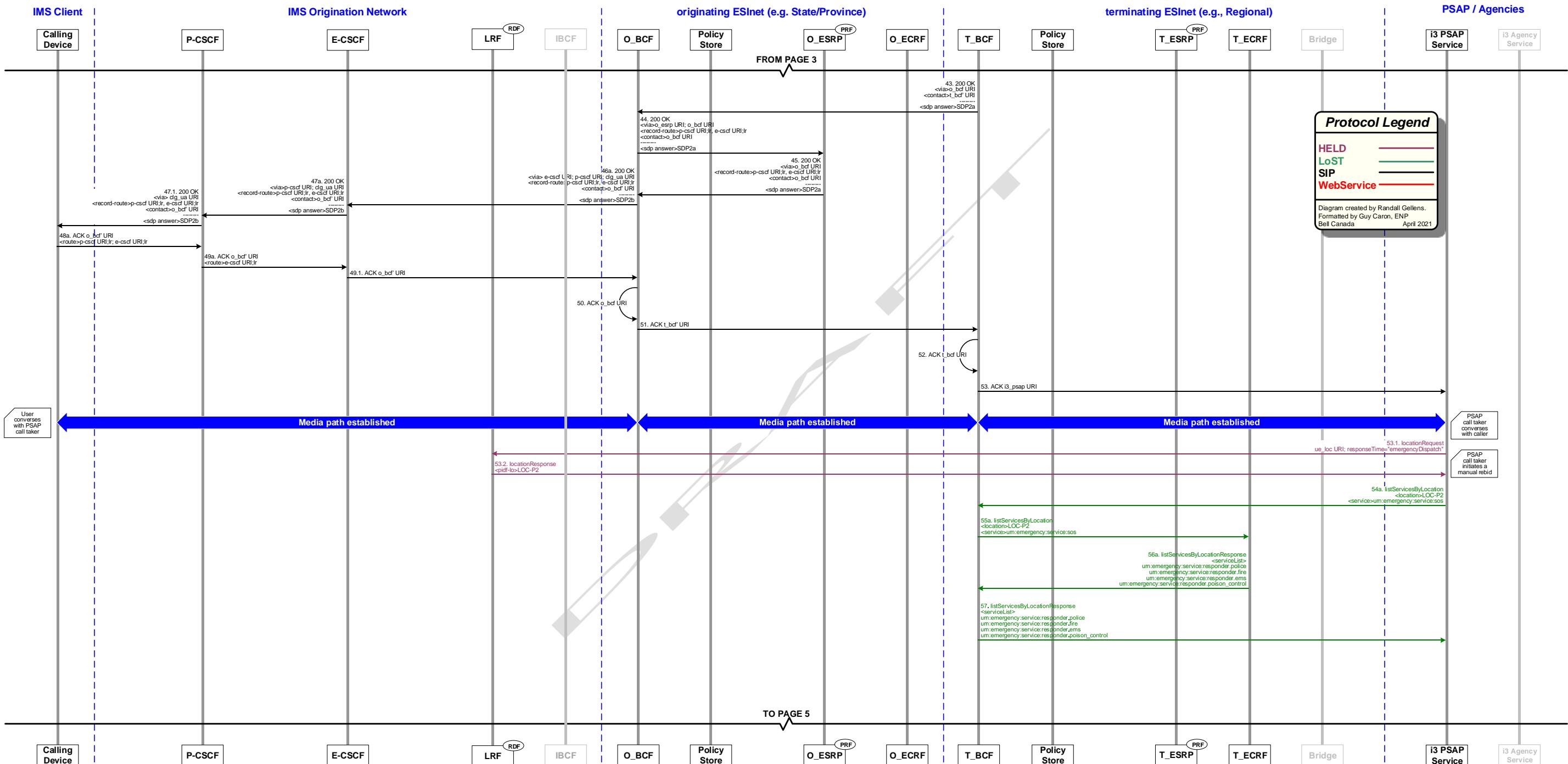
13488

[MM/DD/YYYY]

Page 564 of 675



13489

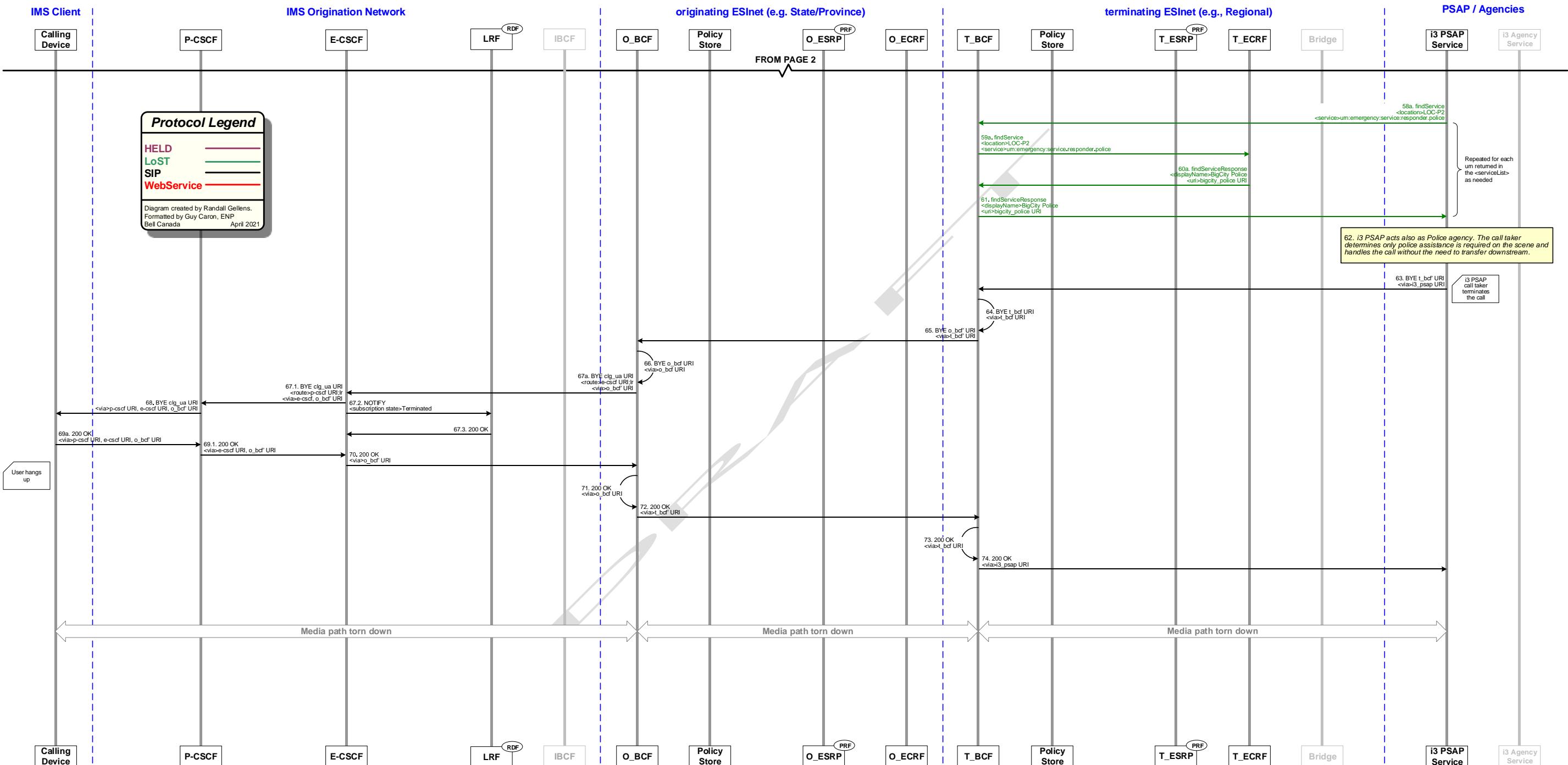
Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 4

[MM/DD/YYYY]

Page 565 of 675



© Copyright 2011-2019 National Emergency Number Association, Inc.

Figure D2. Diagram Example i3 Call Flow – Cellular / HELD Location-by Reference – Part 5

13493 **D.2.1 Step-by-Step Description**

13494 **D.2.1.1 Provisioning Activities (Steps Not Shown)**

13495 The Location Retrieval Function (LRF) in the IMS-based originating network may be
13496 provisioned with routing and Phase I static locations for the cell sectors of its serving
13497 footprint.

13498 The Routing Determination Function (RDF) in the IMS-based originating network may be
13499 provisioned with data to assist in determining the URI based on the Associated Location
13500 [49] for routing purposes.

13501 **D.2.1.2 Pre-call Activities**

- 13502 a1 The Calling Device boots up, attaches to the access network (i.e., it gets a service IP
13503 address and DNS server IP addresses), and discovers its P-CSCF (and possibly also
13504 local emergency numbers). Steps not shown.
- 13505 b1 If the Calling Device has credentials with the serving network, it may perform a
13506 normal (non-emergency) registration, in which case the P-CSCF communicates with
13507 the S-CSCF to authenticate the UE. Steps not shown.

13508 **D.2.1.3 Call-Related Activities**

- 13509 1a. The user is confronted with an emergency situation and uses the Calling Device to
13510 dial an emergency number (either a number the user is accustomed to, or a number
13511 known by the user as valid locally); in this example, 9-1-1. The Calling Device
13512 recognizes the dialstring “911” as an emergency service number (either by
13513 configuration in USIM, ISIM, etc., or by configuration information from the serving
13514 cellular network, or by static configuration), enters in “emergency calling mode”
13515 (typically, disabling certain features and enabling support for position determination
13516 mechanisms such as Control Plane or SUPL);
- 13517 1.1a The Calling Device may perform an emergency registration with the P-CSCF (to
13518 obtain emergency bearer media and other emergency treatment); the P-CSCF
13519 communicates with an S-CSCF to perform this. Steps not shown;
- 13520 2-4. (omitted)

[MM/DD/YYYY]

Page 567 of 675



- 13521 5a. The Calling SIP UA sends an INVITE with the Request-URI set to "urn:service.sos", a
13522 Route header field containing the "p-cscf URI;lr", a Contact header field for itself
13523 ("clg_ue URI"), a P-Access-Network-Info header field containing information about
13524 the cell it is connected via, no Geolocation header field, along with its SDP offer
13525 "SDP1". It may also include a Call-Info header field with a purpose parameter set to
13526 "EmergencyCallData.DeviceInfo" and a cid: URI pointing to Additional Data about
13527 itself in the body <EmergencyCallData.DeviceInfo> "DEV1". It may also include a
13528 Call-Info header field with a purpose parameter set to
13529 "EmergencyCallData.ProviderInfo" and a cid: URI pointing to Additional Data about
13530 itself in the body <EmergencyCallData.ProviderInfo>. If provided, these additional
13531 data body blocks contain a <DataProviderReference> element set to the same
13532 value.
- 13533 6a. The P-CSCF receives the INVITE and replies with a provisional 100 Trying SIP
13534 response to the Calling UA.
- 13535 6.1. The P-CSCF recognizes the Request-URI in the INVITE matching "urn:service:sos" to
13536 be an emergency call and forwards the INVITE to the E-CSCF by:
13537 • removing the Route header field containing its own URI;
13538 • adding a Route header field at the top of the INVITE containing a SIP URI for the
13539 E-CSCF;
13540 • adding a Record-Route header field containing its own SIP URI;
13541 • sending the INVITE to an IP address for the E-CSCF.
- 13542 6.2. The E-CSCF:
13543 • forwards the INVITE to the Location Retrieval Function (LRF) to obtain a route
13544 towards the PSAP, and also for the LRF to add a location reference, and also for
13545 the LRF to initiate position determination processing with the Calling Device (e.g.,
13546 via control plane signaling or SUPL).
- 13547 6.3. The LRF:
13548 • creates a HELD location reference URI (ue_loc URI) for the Calling Device (e.g., an
13549 HTTPS URL with a reference created for the Calling Device for this call);
13550 • determines a location associated with the cell currently used by the Calling Device
13551 (e.g., using a cell identified in a P-Access-Network-Info header field inserted by the

[MM/DD/YYYY]

Page 568 of 675



- 13552 UE or the P-CSCF or other network element) and sets this ("LOC-AS") as the
13553 location for routing for the Calling Device;
- 13554 • determines the location of the cell currently used by the Calling Device and sets
13555 this ("LOC-P1") as the initial location for the Calling Device (pending results from
13556 the positioning determination procedures);
- 13557 • initiates position determination procedures with the Calling Device (e.g., using
13558 control plane or SUPL);
- 13559 • obtains the route towards the PSAP based on the associated location ("LOC-AS");
- 13560 the LRF consults an RDF to obtain the route (the RDF is a LoST server). Interaction
13561 with an RDF not shown.
- 13562 6.4. The LRF returns a SIP 300 Multiple Choices response to the E-CSCF:
- 13563 • the 300 Multiple Choices response includes a Contact header field containing a URI
13564 for the ESInet ESRP ("o_esrp URI");
- 13565 • the LRF also inserts an encoded Route URI containing the o_esrp URI as a
13566 parameter of the URI in the Contact header field;
- 13567 • adds a Geolocation header field containing the created location reference (ue_loc
13568 URI) as a parameter (suitably encoded) of the URI in the Contact header field;
- 13569 • adds a Geolocation-Routing header field with value "yes" as a parameter (suitably
13570 encoded) of the URI in the Contact header field;
- 13571 • may encode other header fields in the URI in the Contact header field.
- 13572 6.5. Because the LRF needs to maintain the validity of the location reference for the
13573 Calling Device (the "ue_loc URI") for the duration of the dialog plus additional time,
13574 the LRF needs to subscribe to either the specific dialog or to all dialogs. The LRF
13575 sends a SUBSCRIBE request to the E-CSCF to receive state notifications, and the
13576 E-CSCF sends a 200 OK response to the SUBSCRIBE request, followed by an initial
13577 NOTIFY, to which the LRF responds with 200 OK. These steps not shown.
- 13578 6.6. The E-CSCF receives the 300 Multiple Choices response from the LRF and updates
13579 the SIP INVITE accordingly:
- 13580 • the E-CSCF decodes the header field parameters of the Contact header field and
13581 adds them to the INVITE; if the original INVITE contained Geolocation or
13582 Geolocation-Routing header fields, they are removed (replaced by the encoded
13583 header fields);

[MM/DD/YYYY]

Page 569 of 675



- 13584 • the E-CSCF places the URI from the Contact header field URI (minus the header
13585 field parameters) of the 300 response in the topmost entry Route header field;
13586 • the E-CSCF preserves the original Contact header field as received in the SIP
13587 INVITE from the P-CSCF.
- 13588 7a. The E-CSCF then:
13589 • removes the first Route header field referring to itself;
13590 • adds Via and Record-Route header fields pointing to itself ("e-cscf URI");
13591 • adds a Call-Info header field and body part for <EmergencyCallData.ProviderInfo>
13592 "VSP1" (additional data about the originating network);
13593 • optionally, adds a Call-Info header field and body part for
13594 <EmergencyCallData.ServiceInfo> "SUB1" (additional data about the service);
13595 • (the SDP offer "SDP1" remains since neither the P-CSCF nor the E-CSCF anchors
13596 media);
13597 • performs a DNS lookup on the o_esrp URI in the Contact header field URI set by
13598 the LRF; the DNS resolution of this URI in the originating network returns one or
13599 more O_BCF IP.
- 13600 8a. The O_BCF receives the INVITE, inspects the message for malicious content (steps
13601 not shown), and replies with a provisional 100 Trying SIP response to the E-CSCF
13602 (e.g., if there is a relationship with the VSP).
- 13603 9. (unchanged) The O_BCF behaves as a full B2BUA, performs topology hiding, anchors
13604 media, and acts as the UAS for the ingress dialog. On the egress side, acting as a
13605 UAC, it creates a new transaction for the egress dialog by sending an INVITE
13606 populated with a Route header field set to "o_esrp URI;lr", Via and Contact header
13607 fields pointing to itself ("o_bcf URI"), and an SDP offer "SDP1a". It generates Call and
13608 Incident tracking identifiers and adds them to Call-Info header fields with purpose
13609 parameters of "emergency-CallId" and "emergency-IncidentId", respectively. It also
13610 copies the Call-Info, Geolocation header field, and Geolocation-Routing fields found in
13611 the incoming INVITE, as well as the other elements found in the body. The O_BCF
13612 then performs a DNS lookup on the URI found in the Route header field ("o_esrp
13613 URI") of the INVITE. The DNS resolution of this URI in the originating (state) ESInet
13614 returns the O_ESRP IP address(es). The INVITE is forwarded there. The O_BCF
13615 maintains independently the state of the ingress and egress dialog-initiating
13616 transactions as well as the association between them.

[MM/DD/YYYY]

Page 570 of 675



- 13617 10. (unchanged) The O_ESRP receives the INVITE on the call queue associated with
13618 "o_esrp URI", authenticates the O_BCF (steps not shown) and responds with a
13619 provisional 100 Trying SIP message to the O_BCF. It deletes the top Route header
13620 field referring to it.
- 13621 10.1. The O_ESRP resolves the ue_loc URI in the Geolocation header field to obtain a
13622 location to be used for routing: the O_ESRP sends a HELD location dereferencing
13623 request to the LRF as indicated in the ue_loc URI; the locationRequest contains a
13624 responseTime parameter set to emergencyRouting to indicate a request for location
13625 for routing.
- 13626 10.2. The LRF receives the HELD location dereferencing request; because the request is
13627 for a location for routing, the LRF returns the location associated for routing with the
13628 cell ("LOC-AS") in Step 6.3; the LRF sends a HELD locationResponse containing the
13629 location "LOC-AS" to the O_ESRP.
- 13630 11. (unchanged) The O_ESRP is statically provisioned with the address of its Policy Store.
13631 It formulates a RetrievePolicy through an HTTP GET request to
13632 O_esinet/PolicyStore/v1/Policies (with parameters "policyType" as
13633 "OriginationRoutePolicy", "policyQueueName" as "o_esrp URI", which is the URI of the
13634 queue the call was received on and "policyOwner" as "o_ngcs", which is the Agency
13635 Identifier of the agency responsible for O_ESRP) to retrieve the origination route
13636 policy set associated with it. Credentials are also provided.
- 13637 12. (unchanged) The "O_esinet" Policy Store is provisioned with all the policies associated
13638 with its serving clients (step not shown). It receives the RetrievePolicy HTTP GET
13639 request, authenticates the O_ESRP, then dips into its database to find a record
13640 associated with the provided parameters. It returns the result in an HTTP response
13641 message with the origination route policy set for queue "o_esrp URI" in a PolicyArray
13642 object.
- 13643 13a. The O_ESRP invokes its internal Policy Routing Function (PRF) that processes the
13644 rules in the policy received and applies them to the incoming INVITE (step not
13645 shown). The originating policy contains the highest priority rule specifying a
13646 LoSTServiceURNCondition object which, when executed, results in a LoST query to
13647 its serving O_ECRF. The O_ESRP is provisioned with the address of the O_ECRF. It
13648 launches a LoST findService request with the following parameters: <location>
13649 "LOC-AS" as returned in the HELD dereference, <service>

[MM/DD/YYYY]

Page 571 of 675



- 13650 "urn:emergency:service:sos.level_2_esrp" as found in the origination policy.
13651 Credentials are also provided.
- 13652 14a. The O_ECRF authenticates the O_ESRP, processes the request for "LOC-AS" and
13653 "urn:emergency:service:sos.level_2_esrp", and returns a LoST findServiceResponse
13654 with the URI of the next hop ("t_esrp URI") to the O_ESRP.
- 13655 15. (unchanged) The O_ESRP receives the LoST response and since the ECRF query was
13656 successful, it stores the URI received in the Normal-NextHop variable and then
13657 executes the actions associated to the rule containing the
13658 "LoSTServiceURNCondition" object. One of the actions contains an
13659 "InvokePolicyAction" with "policyType" set to "NormalNexthopRoutePolicy" thus it
13660 determines it requires the route policy associated with "t_esrp URI". As such, It
13661 formulates a RetrievePolicy HTTP GET request to O_esinet/PolicyStore/v1/Policies
13662 (with parameters "policyType" as "NormalNextHopRoutePolicy" and
13663 "policyQueueName" as "t_esrp URI", which is the URI stored in the Normal-NextHop
13664 variable and "policyOwner" as "o_ngcs", which is the Agency Identifier of the agency
13665 responsible for T_ESRP) to retrieve the origination policy associated with it.
13666 Credentials are also provided.
- 13667 16. (unchanged) The Policy Store receives the RetrievePolicy HTTP GET request,
13668 authenticates the O_ESRP, then dips into its database to find a record associated
13669 with the provided parameters. It returns the result in a response message with the
13670 route policy for queue "t_esrp URI" in a PolicyArray object.
- 13671 17. (unchanged) The O_ESRP invokes its internal PRF that processes the rules within the
13672 policy received to determine where to send the INVITE. The route policy has a Route
13673 action that forwards the call to the normalNextHop that, in this case, is the T_ESRP.
13674 The O_ESRP adds a Route header field set to "t_esrp URI;lr" and adds a Via header
13675 field pointing to itself ("o_esrp URI"). Following its provisioned behavior for all calls
13676 exiting the local ESInet, the O_ESRP then adds a front value in the topmost Route
13677 header field pointing to its desired next hop "o_bcf URI;lr", performs a DNS lookup
13678 on it and sends the INVITE to the O_BCF IP address.
- 13679 18. (unchanged) The O_BCF receives the INVITE, inspects the message for malicious
13680 content, authenticates the O_ESRP (steps not shown), and replies with a provisional
13681 100 Trying SIP response to the O_ESRP.

[MM/DD/YYYY]

Page 572 of 675



- 13682 19. (unchanged) The O_BCF behaves as a full B2BUA¹⁰¹ and terminates the ingress
13683 dialog. On the egress side, it creates a new dialog by sending an INVITE populated
13684 with a Route header field set to "t_esrp' URI;lr", Via and Contact header fields
13685 pointing to itself ("o_bcf' URI"), and copies the Call-Info, Geolocation and
13686 Geolocation-Routing header fields, and the elements found in the body of the
13687 incoming INVITE, including the SDP offer "SDP1a". The O_BCF then performs a DNS
13688 lookup on the URI found in the Route header field ("t_esrp' URI") of the INVITE. The
13689 DNS resolution of this URI in the originating ESInet returns the T_BCF' IP
13690 address(es). The INVITE is forwarded there. The O_BCF maintains independently the
13691 state of the ingress and egress dialogs as well as the association between the two
13692 dialogs.
- 13693 20. (unchanged) The T_BCF receives the INVITE, inspects the message for malicious
13694 content, authenticates the O_BCF (steps not shown), and responds with a provisional
13695 100 Trying SIP message to the O_BCF.
- 13696 21. (unchanged) The T_BCF behaves as a full B2BUA¹⁰¹, anchors media, and acts as the
13697 UAS for the ingress dialog. On the egress side, acting as a UAC, it creates a new
13698 transaction for the egress dialog by sending an INVITE populated with a Route
13699 header field set to "t_esrp URI;lr", Via and Contact header fields pointing to itself
13700 ("t_bcf URI") and an SDP offer "SDP1b". It also copies the Call-Info, Geolocation and
13701 Geolocation-Routing header fields, and other elements found in the body of the
13702 incoming INVITE. The T_BCF then performs a DNS lookup on the URI found in the
13703 Route header field ("t_esrp URI") of the INVITE. The DNS resolution of this URI in
13704 the terminating (regional) ESInet returns the T_ESRP IP address(es). The INVITE is
13705 forwarded there. The T_BCF maintains independently the state of the ingress and
13706 egress dialog-initiating transactions as well as the association between them.
- 13707 22. (unchanged) The T_ESRP receives the INVITE on the call queue associated with
13708 "t_esrp URI", authenticates the T_BCF (steps not shown), and responds with a
13709 provisional 100 Trying SIP message to the T_BCF. It deletes the top Route header
13710 field referring to it.

¹⁰¹ Topology hiding may occur between ESInets, but consideration should be given to not doing so in support of improved ability to diagnose problems.

- 13711 22.1. The T_ESRP resolves the ue_loc URI in the Geolocation header field to obtain a
13712 location to be used for routing; the T_ESRP sends a HELD location dereferencing
13713 request to the LRF as indicated in the ue_loc URI; the locationRequest contains a
13714 responseTime parameter set to emergencyRouting to indicate a request for a
13715 routing location.
- 13716 22.2. The LRF receives the HELD location dereferencing request; because the request is
13717 for a routing location, the LRF returns the location associated for routing with the
13718 cell ("LOC-AS") in Step 6.3; the LRF sends a HELD locationResponse containing the
13719 location "LOC-AS" to the T_ESRP.
- 13720 23. (unchanged) The T_ESRP is statically provisioned with the address of its Policy Store.
13721 It formulates a RetrievePolicy through an HTTP GET request to
13722 T_esinet/PolicyStore/v1/Policies (with parameters "policyType" as
13723 "OriginationRoutePolicy", "policyQueueName" as "t_esrp URI", which is the URI of
13724 the queue the call was received on and "policyOwner" as "t_ngcs", which is the
13725 Agency Identifier of the agency responsible for T_ESRP) to retrieve the origination
13726 route policy set associated with it. Credentials are also provided.
- 13727 24. (unchanged) The "T_esinet" Policy Store is provisioned with all the policies
13728 associated with its serving clients (step not shown). It receives the RetrievePolicy
13729 HTTP GET request, authenticates the T_ESRP, then queries its database to find a
13730 record associated with the provided parameters. It returns the result in a response
13731 message with the origination route policy set for queue "t_esrp URI" in a PolicyArray
13732 object.
- 13733 25a. The T_ESRP invokes its internal Policy Routing Function (PRF) that processes the
13734 rules in the policy received and applies them to the incoming INVITE (step not
13735 shown). The originating policy contains the highest priority rule specifying a
13736 LoSTServiceURNCondition object which, when executed, results in a LoST query to
13737 its serving T_ECRF. The T_ESRP is provisioned with the address of the T_ECRF. It
13738 launches a LoST findService request with the following parameters: <location>
13739 "LOC-AS" as returned in the HELD dereference, <service>
13740 "urn:emergency:service:sos.psap" as found in the originating policy. Credentials are
13741 also provided.

[MM/DD/YYYY]

Page 574 of 675



- 13742 26a. The T_ECRF authenticates the T_ESRP, processes the request for "LOC-AS" and
13743 "urn:emergency:service:sos.psap", and returns a LoST findService Response with
13744 the URI of the next hop ("i3_psap URI") to the T_ESRP.
- 13745 27. (unchanged) The T_ESRP receives the LoST response and since the ECRF query was
13746 successful, it stores the URI received in the Normal-NextHop variable and then
13747 executes the actions associated to the rule containing "LoSTServiceURNCondition"
13748 object. One of the actions contains an "InvokePolicyAction" actionType with
13749 "policyType" set to "NormalNexthopRoutePolicy" thus it determines it requires the
13750 route policy associated with "i3_psap URI". As such, it formulates a RetrievePolicy
13751 HTTP GET request to T_esinet/PolicyStore/v1/Policies (with parameters "policyType"
13752 as "NormalNextHopRoutePolicy" and "policyQueueName" as "i3_psap URI", which is
13753 the URI stored in the Normal-NextHop variable and "policyOwner" as "i3_psap",
13754 which is the Agency Identifier of the agency responsible for i3_PSAP) to retrieve the
13755 origination route policy set associated with it. Credentials are also provided.
- 13756 28. (unchanged) The Policy Store receives the RetrievePolicy HTTP GET request,
13757 authenticates the T_ESRP, then queries its database to find a record associated with
13758 the provided parameters. It returns the result in a response message with the route
13759 policy for queue "i3_psap URI" in a PolicyArray object.
- 13760 29. (unchanged) The T_ESRP invokes its internal PRF that processes the rules within the
13761 policy received to determine where to send the INVITE. The terminating policy has a
13762 Route action that forwards the call to the normalNextHop that, in this case, is the
13763 i3_PSAP. The T_ESRP adds a Route header field set to "i3_psap URI;lr" and adds a
13764 Via header field pointing to itself ("t_esrp URI"). Following its provisioned behavior
13765 for all calls exiting the local ESInet, the T_ESRP then adds a front value in the
13766 topmost Route header field pointing to its desired next hop "t_bcf URI;lr", performs a
13767 DNS lookup on it, and sends the INVITE to the T_BCF IP address.
- 13768 30. (unchanged) The T_BCF receives the INVITE, inspects the message for malicious
13769 content, authenticates the T_ESRP (steps not shown), and replies with a provisional
13770 100 Trying SIP response to the T_ESRP.
- 13771 31. (unchanged) The T_BCF behaves as a full B2BUA¹⁰¹ and terminates the ingress
13772 dialog. On the egress side, it creates a new dialog by sending an INVITE populated
13773 with a Route header field set to "i3_psap URI;lr", Via and Contact header fields
13774 pointing to itself ("t_bcf' URI"), and copies the Call-Info, Geolocation and

[MM/DD/YYYY]

Page 575 of 675



- 13775 Geolocation-Routing header fields, and the elements found in the body of the
13776 incoming INVITE, including the SDP offer "SDP1b". The T_BCF then performs a DNS
13777 lookup on the URI found in the Route header field ("i3_psap URI") of the INVITE.
13778 The DNS resolution of this URI in the regional (terminating) ESInet returns the
13779 i3_PSAP IP address(es). The INVITE is forwarded there. The T_BCF maintains
13780 independently the state of the ingress and egress dialogs as well as the association
13781 between the two dialogs.
- 13782 32. (unchanged) The i3_PSAP receives the INVITE, authenticates the T_BCF (steps not
13783 shown), presents the call on its normal call queue for the next available agent to
13784 answer, and replies with a provisional 180 Ringing¹⁰² SIP response to the URI found
13785 in the top Via header field ("t_bcf" URI").
- 13786 33. (unchanged) The T_BCF receives the provisional 180 Ringing message on the egress
13787 transaction and creates a reciprocal response on the ingress transaction using the Via
13788 header fields of the associated ingress INVITE pointing to the T_ESRP.
- 13789 34. (unchanged) The T_ESRP receives the provisional 180 Ringing message, removes the
13790 Via header field referring to it, and forwards the response to the URI in the next Via
13791 header field, in this case, the T_BCF.
- 13792 35. (unchanged) The T_BCF receives the provisional 180 Ringing message on the egress
13793 dialog and creates a reciprocal response on the ingress dialog using the Via header
13794 fields of the associated ingress INVITE pointing to the O_BCF.
- 13795 36. (unchanged) The O_BCF receives the provisional 180 Ringing message on the egress
13796 dialog and creates a reciprocal response on the ingress dialog using the Via header
13797 fields of the associated ingress INVITE pointing to the O_ESRP.
- 13798 37. (unchanged) The O_ESRP receives the provisional 180 Ringing message, removes
13799 the Via header field referring to it, and forwards the response to the URI in the next
13800 Via header field, in this case, the O_BCF.
- 13801 38a. The O_BCF receives the provisional 180 Ringing message on the egress dialog and
13802 creates a reciprocal response on the ingress dialog using the Via header fields of the
13803 associated ingress INVITE pointing to the E-CSCF. The O_BCF also reinstates the

¹⁰² The 180 Ringing message may be preceded by a 100 Trying message.

- 13804 Record-Route header field previously received in the INVITE. It provides a different
13805 value in the Contact header field ("o_bcf' URI").
- 13806 38.1. The E-CSCF receives the provisional 180 Ringing message, removes the Via header
13807 field referring to it, and forwards the response to the URI in the next Via header
13808 field, in this case, the P-CSCF.
- 13809 39a. The P-CSCF receives the provisional 180 Ringing message, removes the Via header
13810 field referring to it, and forwards the response to the URI in the next Via header
13811 field, in this case, the Calling UA.
- 13812 *The Calling UA receives the provisional 180 Ringing SIP response, processes the
13813 response, and generates a ring back tone towards the hearing medium (speaker
13814 phone, handset, headset, etc.) to alert the user that the call has reached its
13815 destination.*
- 13816 *(unchanged) Some ringing cycles later, the i3 PSAP call taker answers the call.*
- 13817 39.1. The i3 PSAP has a policy of performing an initial "bid" (also referred to as an
13818 "automatic rebid") to obtain the current location information when a call taker
13819 becomes available. To do so, the i3 PSAP resolves the ue_loc URI in the Geolocation
13820 header field to obtain the current location to be used (typically Phase I) and sends
13821 an HTTPS HELD location dereferencing request to the LRF as indicated in the ue_loc
13822 URI; the locationRequest contains a responseTime parameter with a wait timer
13823 value of "0".
- 13824 39.2. The LRF receives the HTTPS HELD location dereferencing request; because the
13825 request is for the current location and the position determination procedures
13826 initiated in Step 6.3 have not yet resulted in a location estimate, the LRF returns the
13827 location of the cell used by the calling device ("LOC-P1"); the LRF sends a HELD
13828 locationResponse containing the location "LOC-P1" to the i3 PSAP.
- 13829 40. (unchanged) The i3 PSAP returns a final 200 OK SIP response to the URI found in
13830 the Via header field ("t_bcf' URI") with its SDP answer set to "SDP2".
- 13831 41. (unchanged) The T_BCF receives the final 200 OK message on the egress
13832 transaction, marking the establishment of the egress dialog. It creates a reciprocal
13833 response on the ingress transaction using the Via header fields of the associated
13834 ingress INVITE pointing to the T_ESRP.

[MM/DD/YYYY]

Page 577 of 675



- 13835 42. (unchanged) The T_ESRP receives the final 200 OK message, removes the Via
13836 header field referring to it, and forwards the response to the URI in the next Via
13837 header field, in this case, the T_BCF.
- 13838 43. (unchanged) The T_BCF receives the final 200 OK message on the egress transaction
13839 and creates a reciprocal response on the ingress transaction using the Via header
13840 fields of the associated ingress INVITE pointing to the O_BCF. Because it anchors
13841 media on ingress, the SDP answer is now "SDP2a". It also provides a different value
13842 in the Contact header field ("t_bcf' URI").
- 13843 44. (unchanged) The O_BCF receives the final 200 OK message on the egress
13844 transaction and creates a reciprocal response on the ingress transaction using the Via
13845 header fields of the associated ingress INVITE pointing to the O_ESRP.
- 13846 45. (unchanged) The O_ESRP receives the final 200 OK message, removes the Via
13847 header field referring to it, and forwards the response to the URI in the next Via
13848 header field, in this case, the O_BCF.
- 13849 46a. The O_BCF receives the final 200 OK message on the egress transaction and creates
13850 a reciprocal response on the ingress transaction using the Via header fields of the
13851 associated ingress INVITE pointing to the E-CSCF. The O_BCF also reinstates the
13852 Record-Route header field previously received in the INVITE. Because it anchors
13853 media on ingress, the SDP answer is now "SDP2b". It also provides a different value
13854 in the Contact header field ("o_bcf' URI").
- 13855 47a. The E-CSCF receives the final 200 OK message, removes the Via header field
13856 referring to itself and forwards the response to the URI in the next Via header field,
13857 in this case, the P-CSCF.
- 13858 47.1. The P-CSCF receives the final 200 OK message, removes the Via header field
13859 referring to itself, and forwards the response to the URI in the next Via header field,
13860 in this case, the Calling UA.
- 13861 48a. The Calling UA receives the final 200 OK response and builds its route-set with the
13862 information contained in the Record-Route header fields ("p-cscf URI;lr, e-cscf
13863 URI;lr"). After accepting the session media offer, it then creates an ACK request with
13864 Route header fields set to the values of its route-set. It sets the Request-URI to the
13865 value of the Contact header field ("o_bcf' URI") and sends the ACK to the first URI
13866 in the topmost Route header field, in this case, the P-CSCF.

[MM/DD/YYYY]

Page 578 of 675



- 13867 49a. The P-CSCF removes the Route header field referring to itself and forwards the ACK
13868 using the Request-URI ("e-cscf URI").
- 13869 49.1. The E-CSCF removes the Route header field referring to itself and forwards the ACK
13870 using the Request-URI ("o_bcf' URI").
- 13871 50. (unchanged) The O_BCF behaves as a full B2BUA¹⁰¹. On the egress side, it sends an
13872 ACK populated with a Request-URI set to "o_bcf URI" found in the Contact header of
13873 the associated 200 OK response (Step 44).
- 13874 51. (unchanged) The O_BCF behaves as a full B2BUA¹⁰¹ and terminates the ingress
13875 dialog. On the egress side, it uses the previously opened egress dialog and sends an
13876 ACK populated with a Request-URI set to "t_bcf' URI" found in the Contact header
13877 field of the associated 200 OK response (Step 43).
- 13878 52. (unchanged) The T_BCF behaves as a full B2BUA¹⁰¹ and terminates the ingress
13879 dialog. On the egress side, it uses the previously opened egress dialog and sends an
13880 ACK populated with a Request-URI set to "t_bcf URI" found in the Contact header
13881 field of the associated 200 OK response (Step 41).
- 13882 53. (unchanged) The T_BCF behaves as a full B2BUA, performs topology hiding, and
13883 terminates the ingress dialog. On the egress side, it uses the previously opened
13884 egress dialog and sends an ACK populated with a Request-URI set to "i3_psap URI"
13885 found in the Contact header field of the associated 200 OK response (Step 40).
*(unchanged) Media path is established between the Calling UA and the i3 PSAP with
anchoring points at the BCFs (SBC part). Conversation between the call taker and the
caller commences.*
- 13886 53.1. The call taker initiates a manual rebid to obtain updated location information for the
13887 caller; the i3 PSAP resolves the ue_loc URI in the Geolocation header field to obtain
13888 an updated location; the i3 PSAP sends an HTTPS HELD location dereferencing
13889 request to the LRF as indicated in the ue_loc URI; the locationRequest contains a
13890 responseTime parameter set to emergencyDispatch to indicate a request for location
13891 for dispatch.
- 13892 53.2. The LRF receives the HTTPS HELD location dereferencing request; the request is for
13893 a location for dispatch, and the position determination procedures initiated in Step
13894 6.3 have resulted in at least an initial location estimate ("LOC-P2"); the LRF sends a
13895 HELD locationResponse containing the location "LOC-P2" to the i3 PSAP; position

[MM/DD/YYYY]

Page 579 of 675



- 13899 determination procedures may continue and may provide a better location estimate
13900 on a subsequent rebid.
- 13901 54a. The i3 PSAP has built-in logic to gather agency information in preparation of a
13902 potential transfer to downstream agencies. The i3 PSAP is provisioned with its
13903 serving ECRF (T_ECRF), however, the T_ECRF is only reachable by a static route
13904 through the T_BCF (firewall part). The i3 PSAP sends a LoST listServicesByLocation
13905 request using the most recently received location "LOC-P2" against the top-level
13906 service URN "urn:emergency:service:sos". Credentials are also provided.
- 13907 55a. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the
13908 source and destination IP addresses, inspects the message for malicious content,
13909 and lets the message go through to the T_ECRF. The location is LOC-P2, as the
13910 most recently received location.
- 13911 56a. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST
13912 request, dips in its database for "LOC-P2", and formulates a LoST
13913 listServicesByLocationResponse populated with the services available for "LOC-P2"
13914 ("urn:emergency:service:responder.police", "urn:emergency:service:responder.fire",
13915 "urn:emergency:service:responder.ems", and
13916 "urn:emergency:service:responder.poison_control") back to the i3 PSAP through the
13917 T_BCF.
- 13918 57. (unchanged) The T_BCF (firewall part) receives the LoST response from the T_ECRF,
13919 examines the source and destination IP addresses, inspects the message for
13920 malicious content, and lets the message go through to the i3 PSAP.
- 13921 58a. With the list of available services in hand, the i3 PSAP proactively launches a LoST
13922 findServiceRequest to the T_ECRF for each of the services available. As above, the
13923 requests are sent to the T_BCF (firewall part). In this example, only the
13924 "urn:emergency:service:responder.police" service URN is shown. The location is
13925 LOC--P2.
- 13926 59a. The T_BCF (firewall part) receives the LoST request from the i3 PSAP, examines the
13927 source and destination IP addresses, inspects the message for malicious content,
13928 and lets the message go through to the T_ECRF. The location remains LOC-P2.
- 13929 60a. The T_ECRF authenticates the i3 PSAP (steps not shown), processes the LoST
13930 requests, dips in its database for "LOC-P2" and the service URN provided in the

[MM/DD/YYYY]

Page 580 of 675



- 13931 requests (in this example, "urn:emergency:service:responder.police"), and
13932 formulates LoST findServiceResponse messages populated with the URI of the
13933 requested service along with the display name of the agency (a.k.a., English
13934 Language Translation) back to the i3 PSAP through the T_BCF.
- 13935 61. (unchanged) The T_BCF (firewall part) receives the LoST response from the T_ECRF,
13936 examines the source and destination IP addresses, inspects the message for
13937 malicious content, and lets the message go through to the i3 PSAP.
- 13938 62. (unchanged) The i3 PSAP acts also as the police agency. The call taker determines
13939 only police assistance is required on the scene and handles the call without the need
13940 to transfer downstream.
- 13941 62.1. The call taker (who might be different from the original call taker if the call was
13942 transferred) may decide to initiate a manual rebid at any point, in which case Steps
13943 53.1 and 53.2 are repeated. Steps not shown.
- 13944 *Once all the information has been gathered and the caller is comforted that first
13945 responders are on their way, the call taker terminates the call (hangs up).*
- 13946 63.-68. Upon detecting the hang-up signal, the i3 PSAP sends a SIP BYE request towards
13947 the Calling UA. Each UAS and B2BUA uses its route-set and Contact header fields
13948 previously populated for its dialog(s) to populate the Route header fields and
13949 Request-URIs. The BYE request is propagated on the path, each element applying the
13950 routing logic gathered from the associated dialog until it reaches the Calling UA.
13951 These steps are unchanged from D.1 except that instead of transiting the VSP CS, the
13952 signaling transits the E-CSCF and P-CSCF (Steps 67a, 67.1, 68a). In addition, upon
13953 receiving the BYE, the E-CSCF sends a last NOTIFY to the LRF and terminates the
13954 subscription created in Step 6.5 (Steps 67.2 and 67.3).
- 13955 69.-74. (unchanged) The Calling UA receives the BYE request and starts the tear down
13956 procedures. It then sends a final 200 OK response that gets propagated on the
13957 reverse path towards the i3 PSAP terminating the dialog and the session.
- 13958 *The media is torn down end-to-end. This emergency call is over.*
- 13959

13960 **Appendix E - REST/JSON Definitions (Normative)**

13961 Web Services defined in this document are described using OpenAPI V3, with JSON-ld
13962 exchange schemas for NIEM conformance. This section contains the OpenAPI interface
13963 definition as a YAML object. Examples of each interface are provided (future).

13964 **E.1 Policy Store**

13965 **E.1.1 OpenAPI Interface Description**

```
13966 openapi: 3.0.1
13967 info:
13968   title: Policy Store
13969   version: "1.0"
13970 servers:
13971   - url: http://localhost/PolicyStore/v1
13972 paths:
13973   /Policies:
13974     get:
13975       tags:
13976         - RetrievePolicy, UpdatedPolicy
13977       summary: Retrieves all policies from the store. Use limit and start
13978 parameters for pagination.
13979       operationId: RetrievePolicy
13980       parameters:
13981         - name: limit
13982           in: query
13983           description: Maximum number of results to return
13984           required: false
13985           schema:
13986             type: integer
13987             format: int32
13988         - name: start
13989           in: query
13990           description: First item in the page of results, as an ordinal 1-
13991 based integer
13992           required: false
13993           schema:
13994             type: integer
13995             format: int32
13996             minimum: 1
13997         - name: policyOwner
13998           in: query
```

[MM/DD/YYYY]

Page 582 of 675



```
13999      description: ID of the Agency owning policy(ies)
14000      required: false
14001      schema:
14002          type: string
14003      - name: policyType
14004          in: query
14005          description: Type of the policy
14006          required: false
14007          schema:
14008              type: string
14009      - name: policyQueueName
14010          in: query
14011          description: Policy queue name
14012          required: false
14013          schema:
14014              type: string
14015              format: uri
14016      - name: policyId
14017          in: query
14018          description: Id of the policy
14019          required: false
14020          schema:
14021              type: string
14022      responses:
14023          '200':
14024              description: Policies found
14025              content:
14026                  application/json:
14027                      schema:
14028                          $ref: '#/components/schemas/PolicyArray'
14029
14030          '307':
14031              description: Temporary Redirect
14032              headers:
14033                  Location:
14034                      description: Referral URI of another Policy Store which may
14035                      store the policy requested
14036              schema:
14037                  type: string
14038          '404':
14039              description: Not found
14040          '451':
14041              description: Unknown or bad Policy Type
14042          '452':
14043              description: Unknown or bad Agency Name
```



```
14043      '453':
14044          description: Not available here, no referral available
14045      '454':
14046          description: Unspecified Error
14047  post:
14048      tags:
14049          - CreatePolicy
14050      summary: Creates a new policy in the Policy Store
14051      operationId: CreatePolicy
14052      requestBody:
14053          description: Policy to add (JWS using flattened JSON
14054  serialization)
14055      content:
14056          application/json:
14057              schema:
14058                  $ref: 'i3-common.yaml#/components/schemas/Jws'
14059      required: true
14060  responses:
14061      '201':
14062          description: Policy successfully created
14063      '434':
14064          description: Signature Verification Failure
14065      '436':
14066          description: Duplicate or Invalid Priority
14067      '437':
14068          description: Bad Policy Structure
14069      '438':
14070          description: Unacceptable Algorithm
14071      '451':
14072          description: Unknown or bad Policy Type
14073      '452':
14074          description: Unknown or bad Agency Name
14075      '454':
14076          description: Unspecified Error
14077      '459':
14078          description: Bad policyExpirationTime
14079  put:
14080      tags:
14081          - UpdatePolicy
14082      summary: Updates an existing policy. In order to identify a policy
14083      the following parameters must be specified - policyType, policyQueueName
14084      OR policyId.
14085      operationId: UpdatePolicy
14086      parameters:
```

[MM/DD/YYYY]

Page 584 of 675



```
14087      - name: policyOwner
14088          in: query
14089          description: Owner of the policy
14090          required: true
14091          schema:
14092              type: string
14093      - name: policyType
14094          in: query
14095          description: Type of the policy
14096          required: true
14097          schema:
14098              type: string
14099      - name: policyQueueName
14100          in: query
14101          description: Policy queue name
14102          required: false
14103          schema:
14104              type: string
14105              format: uri
14106      - name: policyId
14107          in: query
14108          description: Id of the policy
14109          required: false
14110          schema:
14111              type: string
14112      requestBody:
14113          description: Policy to update (JWS using flattened JSON
14114      serialization)
14115          content:
14116              application/json:
14117                  schema:
14118                      $ref: 'i3-common.yaml#/components/schemas/Jws'
14119                  required: true
14120          responses:
14121              '200':
14122                  description: Policy successfully updated
14123              '404':
14124                  description: Not found
14125              '434':
14126                  description: Signature Verification Failure
14127              '436':
14128                  description: Duplicate or Invalid Priority
14129              '437':
14130                  description: Bad Policy Structure
```

[MM/DD/YYYY]

Page 585 of 675



```
14131      '451':
14132          description: Unknown or bad Policy Type
14133      '452':
14134          description: Unknown or bad Agency Name
14135      '454':
14136          description: Unspecified Error
14137      '460':
14138          description: Bad PolicyExpirationTime
14139  delete:
14140      tags:
14141          - DeletePolicy
14142      summary: Deletes an existing policy. In order to identify a policy
14143  the following parameters must be specified - policyType, policyQueueName
14144  OR policyId.
14145      operationId: DeletePolicy
14146  parameters:
14147      - name: policyOwner
14148          in: query
14149          description: Owner of the policy
14150          required: true
14151          schema:
14152              type: string
14153      - name: policyType
14154          in: query
14155          description: Type of the policy
14156          required: true
14157          schema:
14158              type: string
14159      - name: policyQueueName
14160          in: query
14161          description: Policy queue name
14162          required: false
14163          schema:
14164              type: string
14165              format: uri
14166      - name: policyId
14167          in: query
14168          description: Id of the policy
14169          required: false
14170          schema:
14171              type: string
14172  responses:
14173      '200':
14174          description: Policy successfully deleted
```

[MM/DD/YYYY]

Page 586 of 675



```
14175      '404':
14176          description: Not found
14177      '451':
14178          description: Unknown or bad Policy Type
14179      '452':
14180          description: Unknown or bad Agency Name
14181      '454':
14182          description: Unspecified Error
14183 /PolicyEnums:
14184     get:
14185       tags:
14186         - EnumeratePolicy
14187       summary: Returns a list of policy types available in the store for a
14188       specific agency/service. Use limit and start parameters for pagination.
14189       operationId: EnumeratePolicy
14190     parameters:
14191       - name: limit
14192           in: query
14193           description: Maximum number of results to return
14194           required: false
14195           schema:
14196             type: integer
14197             format: int32
14198       - name: start
14199           in: query
14200           description: First item in the page of results, as an ordinal 1-
14201           based integer
14202           required: false
14203           schema:
14204             type: integer
14205             format: int32
14206             minimum: 1
14207       - name: policyOwner
14208           in: query
14209           description: ID of the Agency owning policy(ies)
14210           required: false
14211           schema:
14212             type: string
14213       - name: policyType
14214           in: query
14215           description: Type of the policy
14216           required: true
14217           schema:
14218             type: string
```

[MM/DD/YYYY]

Page 587 of 675



```
14219      - name: policyQueueName
14220          in: query
14221          description: Policy queue name
14222          required: false
14223          schema:
14224              type: string
14225              format: uri
14226      - name: policyId
14227          in: query
14228          description: Id of the policy
14229          required: false
14230          schema:
14231              type: string
14232      - name: policiesUpdatedSince
14233          in: query
14234          description: The query will return all policies having the time
14235          of creation or last modification greater than policiesUpdatedSince
14236          required: false
14237          schema:
14238              type: string
14239              format: date-time
14240              example: '2020-03-10T10:00:00-05:00'
14241      responses:
14242          '200':
14243              description: Policies enumerations found
14244              content:
14245                  application/json:
14246                      schema:
14247                          $ref: '#/components/schemas/PolicyEnumArray'
14248          '404':
14249              description: Not found
14250          '451':
14251              description: Unknown or bad Policy Type
14252          '452':
14253              description: Unknown or bad Agency Name
14254          '454':
14255              description: Unspecified Error
14256      /Versions:
14257          servers:
14258              - url: https://api.example.com/PolicyStore
14259                  description: Override base path for Versions query
14260      get:
14261          tags:
14262              - RetrieveVersions
```

[MM/DD/YYYY]

Page 588 of 675



```
14263      summary: Retrieves all supported versions, vendor parameter is
14264      optional.
14265          operationId: RetrieveVersions
14266          responses:
14267              '200':
14268                  description: Versions found
14269                  content:
14270                      application/json:
14271                          schema:
14272                              $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
14273          components:
14274              schemas:
14275                  PolicyArray:
14276                      type: object
14277                      required:
14278                          - count
14279                          - totalCount
14280                          - policies
14281                  properties:
14282                      count:
14283                          type: integer
14284                          format: int32
14285                          description: Number of items in the array
14286                      totalCount:
14287                          type: integer
14288                          format: int32
14289                          description: Total number of items found
14290                      policies:
14291                          type: array
14292                          items:
14293                              $ref: 'i3-common.yaml#/components/schemas/Jws'
14294                              description: Array of Policy objects, each in JWS format (JWS
14295 using flattened JSON serialization)
14296          Policy:
14297              type: object
14298              required:
14299                  - policyType
14300                  - policyOwner
14301                  - policyRules
14302              properties:
14303                  policyType:
14304                      type: string
14305                      description: Values limited to those in the policyType registry
14306                  policyOwner:
```

[MM/DD/YYYY]

Page 589 of 675



```
14307      type: string
14308  policyQueueName:
14309      type: string
14310      format: uri
14311  policyId:
14312      type: string
14313  policyExpirationTime:
14314      type: string
14315      format: date-time
14316      example: '2020-03-10T10:00:00-05:00'
14317  policyRules:
14318      type: array
14319      items:
14320          $ref: '#/components/schemas/Rule'
14321  policyLastModificationTime:
14322      type: string
14323      format: date-time
14324      example: '2020-03-10T10:00:00-05:00'
14325  description:
14326      type: string
14327  PolicyEnumArray:
14328      type: object
14329      required:
14330          - count
14331          - totalCount
14332          - policyEnums
14333  properties:
14334  count:
14335      type: integer
14336      format: int32
14337      description: Number of items in the array
14338  totalCount:
14339      type: integer
14340      format: int32
14341      description: Total number of items found
14342  policyEnums:
14343      type: array
14344      items:
14345          $ref: '#/components/schemas/PolicyEnum'
14346          description: Array of Policy Enums objects
14347  PolicyEnum:
14348      type: object
14349      required:
14350          - policyType
```

[MM/DD/YYYY]

Page 590 of 675



```
14351      - policyOwner
14352      - policyExpirationTime
14353      - policyLastModificationTime
14354  properties:
14355    policyType:
14356      type: string
14357    policyOwner:
14358      type: string
14359    policyQueueName:
14360      type: string
14361      format: uri
14362    policyId:
14363      type: string
14364    policyExpirationTime:
14365      type: string
14366      format: date-time
14367      example: '2020-03-10T10:00:00-05:00'
14368  policyLastModificationTime:
14369    type: string
14370    format: date-time
14371    example: '2020-03-10T10:00:00-05:00'
14372  Rule:
14373    type: object
14374    required:
14375      - id
14376      - priority
14377      - actions
14378    properties:
14379      id:
14380        type: string
14381        description: Unique ID within a Policy,
14382      priority:
14383        type: integer
14384        format: int32
14385        minimum: 0
14386      conditions:
14387        type: array
14388        items:
14389          $ref: '#/components/schemas/Condition'
14390      actions:
14391        type: array
14392        items:
14393          $ref: '#/components/schemas/Action'
14394  description:
```

[MM/DD/YYYY]

Page 591 of 675



```
14395          type: string
14396      Action:
14397          type: object
14398          required:
14399              - actionType
14400          properties:
14401              actionType:
14402                  type: string
14403                  enum: [RouteAction, NotifyAction, LogAction, BusyAction,
14404          InvokePolicyAction]
14405          description:
14406              type: string
14407          discriminator:
14408              propertyName: actionType
14409      RouteAction:
14410          allOf:
14411              - $ref: '#/components/schemas/Action'
14412              - type: object
14413                  required:
14414                      - recipientUri
14415                  properties:
14416                      recipientUri:
14417                          type: string
14418                          format: uri
14419                      rnaTimer:
14420                          type: integer
14421                          format: int32
14422                      cause:
14423                          type: string
14424      NotifyAction:
14425          allOf:
14426              - $ref: '#/components/schemas/Action'
14427              - type: object
14428                  required:
14429                      - eventCode
14430                      - urgency
14431                  properties:
14432                      recipient:
14433                          type: string
14434                          format: uri
14435                      eventCode:
14436                          type: string
14437                          description: Values limited to those in the
14438      EsrpNotifyEventCodes registry
```

[MM/DD/YYYY]

Page 592 of 675



```
14439         urgency:  
14440             type: integer  
14441             format: int32  
14442             comment:  
14443                 type: string  
14444             BusyAction:  
14445                 allOf:  
14446                     - $ref: '#/components/schemas/Action'  
14447             LogAction:  
14448                 allOf:  
14449                     - $ref: '#/components/schemas/Action'  
14450                     - type: object  
14451                         required:  
14452                             - message  
14453                         properties:  
14454                             message:  
14455                                 type: string  
14456             InvokePolicyAction:  
14457                 allOf:  
14458                     - $ref: '#/components/schemas/Action'  
14459                     - type: object  
14460                         required:  
14461                             - policyType  
14462                         properties:  
14463                             policyType:  
14464                                 type: string  
14465                             policyQueueName:  
14466                                 type: string  
14467                                 format: uri  
14468                             policyId:  
14469                                 type: string  
14470             Condition:  
14471                 type: object  
14472                 required:  
14473                     - conditionType  
14474                 properties:  
14475                     conditionType:  
14476                         $ref: 'i3-common.yaml#/components/schemas/ConditionType'  
14477                     negation:  
14478                         type: boolean  
14479                     description:  
14480                         type: string  
14481                     discriminator:  
14482                         propertyName: conditionType
```

[MM/DD/YYYY]

Page 593 of 675



```
14483     TimePeriodCondition:  
14484         allOf:  
14485             - $ref: '#/components/schemas/Condition'  
14486             - type: object  
14487                 required:  
14488                     - dateStart  
14489                     - dateEnd  
14490             properties:  
14491                 dateStart:  
14492                     type: string  
14493                     format: date-time  
14494                     example: '2019-11-04T02:00:00-05:00'  
14495             dateEnd:  
14496                     type: string  
14497                     format: date-time  
14498                     example: '2020-03-10T01:59:59-05:00'  
14499             timeStart:  
14500                     type: string  
14501                     example: '08:00:00'  
14502             timeEnd:  
14503                     type: string  
14504                     example: '18:00:00'  
14505             weekdayList:  
14506                     type: string  
14507                     example: 'MO,TU,WE,TH,FR'  
14508     SipHeaderCondition:  
14509         allOf:  
14510             - $ref: '#/components/schemas/Condition'  
14511             - type: object  
14512                 required:  
14513                     - field  
14514                     - operator  
14515                     - content  
14516             properties:  
14517                 field:  
14518                     type: string  
14519                 operator:  
14520                     type: string  
14521                     enum: [EQ, SS, IS]  
14522                 content:  
14523                     type: string  
14524     AdditionalDataCondition:  
14525         allOf:  
14526             - $ref: '#/components/schemas/Condition'
```

[MM/DD/YYYY]

Page 594 of 675



```
14527      - type: object
14528          required:
14529              - type
14530              - operator
14531      properties:
14532          type:
14533              type: string
14534          element:
14535              type: string
14536          operator:
14537              type: string
14538              enum: [exists, missing, EQ, SS, NE, GT, LT, GE, LE]
14539          content:
14540              type: string
14541      MimeBodyCondition:
14542          allOf:
14543              - $ref: '#/components/schemas/Condition'
14544          - type: object
14545              required:
14546                  - mimeList
14547          properties:
14548              mimeList:
14549                  type: array
14550                  items:
14551                      type: string
14552      LocationCondition:
14553          allOf:
14554              - $ref: '#/components/schemas/Condition'
14555          - type: object
14556              required:
14557                  - location
14558          properties:
14559              location:
14560                  type: object
14561                  required:
14562                      - lo
14563                      - profile
14564                      - label
14565                      - lang
14566          properties:
14567              lo:
14568                  type: string
14569              profile:
14570                  type: string
```

[MM/DD/YYYY]

Page 595 of 675



```
14571         enum: [civic, geodetic]
14572         label:
14573             type: string
14574             lang:
14575                 type: string
14576             extension:
14577                 type: object
14578             extension:
14579                 type: object
14580     CallSuspicionCondition:
14581         allOf:
14582             - $ref: '#/components/schemas/Condition'
14583             - type: object
14584             required:
14585                 - scoreFrom
14586                 - scoreTo
14587             properties:
14588                 scoreFrom:
14589                     type: integer
14590                     format: int32
14591                 scoreTo:
14592                     type: integer
14593                     format: int32
14594     SecurityPostureCondition:
14595         allOf:
14596             - $ref: '#/components/schemas/Condition'
14597             - type: object
14598             required:
14599                 - service
14600                 - condition
14601                 - value
14602             properties:
14603                 service:
14604                     type: string
14605                 condition:
14606                     type: string
14607                     enum: [EQ, NE]
14608                 value:
14609                     type: string
14610                     description: Values limited to those in the SecurityPosture
14611             registry
14612     QueueStateCondition:
14613         allOf:
14614             - $ref: '#/components/schemas/Condition'
```

[MM/DD/YYYY]

Page 596 of 675



```
14615      - type: object
14616          required:
14617              - queue
14618              - condition
14619              - value
14620      properties:
14621          queue:
14622              type: string
14623              format: uri
14624          condition:
14625              type: string
14626              enum: [EQ, NE]
14627          value:
14628              type: string
14629              description: Values limited to those in the QueueState
14630  registry
14631      LostServiceUrnCondition:
14632          allOf:
14633              - $ref: '#/components/schemas/Condition'
14634              - type: object
14635                  required:
14636                      - urn
14637                  properties:
14638                      urn:
14639                          type: string
14640      ServiceStateCondition:
14641          allOf:
14642              - $ref: '#/components/schemas/Condition'
14643              - type: object
14644                  required:
14645                      - service
14646                      - condition
14647                      - value
14648                  properties:
14649                      service:
14650                          type: string
14651                      condition:
14652                          type: string
14653                          enum: [EQ, NE]
14654                      value:
14655                          type: string
14656                          description: Values limited to those in the serviceState
14657  registry
14658      CallSourceCondition:
```

[MM/DD/YYYY]

Page 597 of 675



```
14659      allOf:
14660        - $ref: '#/components/schemas/Condition'
14661        - type: object
14662          required:
14663            - operator
14664            - content
14665          properties:
14666            operator:
14667              type: string
14668              enum: [EQ, SS, NE]
14669            content:
14670              type: string
14671      BodyPartCondition:
14672        allOf:
14673          - $ref: '#/components/schemas/Condition'
14674          - type: object
14675            required:
14676              - contentType
14677              - element
14678              - operator
14679              - content
14680            properties:
14681              contentType:
14682                type: string
14683              element:
14684                type: string
14685              operator:
14686                type: string
14687                enum: [EQ, SS, NE, GT, LT, GE, LE, exists, missing]
14688              content:
14689                type: string
14690      RequestUriCondition:
14691        allOf:
14692          - $ref: '#/components/schemas/Condition'
14693          - type: object
14694            required:
14695              - operator
14696              - content
14697            properties:
14698              operator:
14699                type: string
14700                enum: [EQ, SS, NE]
14701              content:
14702                type: string
```

[MM/DD/YYYY]

Page 598 of 675



```
14703     NormalNextHopCondition:  
14704         allOf:  
14705             - $ref: '#/components/schemas/Condition'  
14706             - type: object  
14707                 required:  
14708                     - operator  
14709                     - content  
14710                 properties:  
14711                     operator:  
14712                         type: string  
14713                         enum: [EQ, SS, NE]  
14714                     content:  
14715                         type: string  
14716     IncomingQueueCondition:  
14717         allOf:  
14718             - $ref: '#/components/schemas/Condition'  
14719             - type: object  
14720                 required:  
14721                     - operator  
14722                     - content  
14723                 properties:  
14724                     operator:  
14725                         type: string  
14726                         enum: [EQ, SS, NE]  
14727                     content:  
14728                         type: string  
14729                         format: uri  
14730     SdpOfferCondition:  
14731         allOf:  
14732             - $ref: '#/components/schemas/Condition'  
14733             - type: object  
14734                 properties:  
14735                     video:  
14736                         type: boolean  
14737                     audio:  
14738                         type: boolean  
14739                     rtt:  
14740                         type: boolean  
14741                     im:  
14742                         type: boolean  
14743                     text:  
14744                         type: boolean  
14745                     langVideo:  
14746                         type: array
```

[MM/DD/YYYY]

Page 599 of 675



```
14747           items:
14748             type: string
14749   langAudio:
14750     type: array
14751     items:
14752       type: string
14753   langRTT:
14754     type: array
14755     items:
14756       type: string
14757   langIm:
14758     type: array
14759     items:
14760       type: string
14761   langText:
14762     type: array
14763     items:
14764       type: string
14765   langVideoPref:
14766     $ref: '#/components/schemas/Pref'
14767   langAudioPref:
14768     $ref: '#/components/schemas/Pref'
14769   langRttPref:
14770     $ref: '#/components/schemas/Pref'
14771   langImPref:
14772     $ref: '#/components/schemas/Pref'
14773   langTextPref:
14774     $ref: '#/components/schemas/Pref'
14775 CapCondition:
14776   allOf:
14777     - $ref: '#/components/schemas/Condition'
14778     - type: object
14779       required:
14780         - tag
14781       properties:
14782         tag:
14783           type: string
14784           enum: [Identifier, Sender, Address, InfoEventCode,
14785 InfoValueName]
14786         operator:
14787           type: string
14788           enum: [EQ, SS, NE]
14789         content:
14790           type: string
```

[MM/DD/YYYY]

Page 600 of 675



```
14791           nonInteractive:  
14792             type: boolean  
14793       CallingNumberVerificationStatusCondition:  
14794         allOf:  
14795           - $ref: '#/components/schemas/Condition'  
14796           - type: object  
14797             required:  
14798               - operator  
14799               - content  
14800             properties:  
14801               operator:  
14802                 type: string  
14803                 enum: [EQ, NE]  
14804               content:  
14805                 type: string  
14806         Pref:  
14807           type: object  
14808             required:  
14809               - langList  
14810               - langTest  
14811             properties:  
14812               langList:  
14813                 type: string  
14814               langTest:  
14815                 type: string
```

14816 **E.1.2 Examples**

14817 **E.2 Discrepancy Report**

14818 **E.2.1 OpenAPI Interface Description**

```
14819   openapi: 3.0.1  
14820   info:  
14821     title: Discrepancy Reports Service  
14822     version: "1.0"  
14823   servers:  
14824     - url: http://localhost/DiscrepancyReports/v1  
14825   paths:  
14826     /Reports:  
14827       post:  
14828         tags:  
14829           - SubmitReport
```

[MM/DD/YYYY]

Page 601 of 675



```
14830     summary: Submits a new Discrepancy Report
14831     operationId: SubmitReport
14832     requestBody:
14833         description: Discrepancy Report data
14834         content:
14835             application/json:
14836                 schema:
14837                     $ref: '#/components/schemas/DiscrepancyReport'
14838                     required: true
14839     callbacks:
14840         submitResolution:
14841             '#{#/components/schemas/DiscrepancyReport/resolutionUri}':
14842             post:
14843                 requestBody:
14844                     required: true
14845                     content:
14846                         application/json:
14847                             schema:
14848                                 $ref: '#/components/schemas/DiscrepancyResolution'
14849                     responses:
14850                         '201':
14851                             description: Resolution received
14852                     responses:
14853                         '201':
14854                             description: Report successfully created
14855                             content:
14856                                 application/json:
14857                                     schema:
14858                                         $ref: '#/components/schemas/DiscrepancyReportResponse'
14859                         '454':
14860                             description: Unspecified Error
14861                         '470':
14862                             description: Unknown Service/Database ("not ours")
14863                         '471':
14864                             description: Unauthorized Reporter
14865     /Resolutions:
14866         post:
14867             tags:
14868                 - SubmitResolution
14869             summary: Submits a new Discrepancy Resolution
14870             operationId: SubmitResolutiuon
14871             requestBody:
14872                 description: Discrepancy Resolution data
14873                 content:
```



```
14874           application/json:  
14875             schema:  
14876               $ref: '#/components/schemas/DiscrepancyResolution'  
14877             required: true  
14878           responses:  
14879             '201':  
14880               description: Discrepancy Resolution successfully created  
14881             '454':  
14882               description: Unspecified Error  
14883             '472':  
14884               description: Unauthorized Responder  
14885             '473':  
14886               description: Unknown ReportId  
14887         get:  
14888           tags:  
14889             - GetResolution  
14890           summary: Retrieves a Discrepancy Report Resolution based on Agency  
Name and Discrepancy Report ID  
14891           operationId: GetResolution  
14892           parameters:  
14893             - name: agencyName  
14894               in: query  
14895               description: Reporting Agency Name  
14896               required: true  
14897               schema:  
14898                 type: string  
14899             - name: discrepancyReportId  
14900               in: query  
14901               description: ID of the Discrepancy Report  
14902               required: true  
14903               schema:  
14904                 type: string  
14905           responses:  
14906             '200':  
14907               description: Resolution found  
14908               content:  
14909                 application/json:  
14910                   schema:  
14911                     $ref: '#/components/schemas/DiscrepancyResolution'  
14912             '404':  
14913               description: Not found  
14914             '471':  
14915               description: Unauthorized Reporter  
14916             '473':  
14917
```

[MM/DD/YYYY]

Page 603 of 675



```
14918      description: Unknown ReportId
14919      '475':
14920          description: Response not available yet
14921      /StatusUpdates:
14922          get:
14923              tags:
14924                  - StatusUpdateRequest
14925          summary: Request a Status Update for a previously submitted
14926          Discrepancy Report
14927          operationId: StatusUpdateRequest
14928          parameters:
14929              - name: agencyName
14930                  in: query
14931                  description: Reporting Agency Name
14932                  required: true
14933                  schema:
14934                      type: string
14935              - name: discrepancyReportId
14936                  in: query
14937                  description: ID of the Discrepancy Report
14938                  required: true
14939                  schema:
14940                      type: string
14941          responses:
14942              '200':
14943                  description: Status Update found
14944                  content:
14945                      application/json:
14946                          schema:
14947                          $ref: '#/components/schemas/StatusUpdate'
14948          '404':
14949                  description: Not found
14950          '454':
14951                  description: Unspecified Error
14952          '471':
14953                  description: Unauthorized Reporter
14954          '473':
14955                  description: Unknown ReportId
14956          '474':
14957                  description: Resolution already provided
14958      /Versions:
14959          servers:
14960              - url: https://api.example.com/DiscrepancyReports
14961                  description: Override base path for Versions query
```

[MM/DD/YYYY]

Page 604 of 675



```
14962      get:
14963          tags:
14964              - RetrieveVersions
14965          summary: Retrieves all supported versions, vendor parameter is
14966          optional.
14967          operationId: RetrieveVersions
14968          responses:
14969              '200':
14970                  description: Versions found
14971                  content:
14972                      application/json:
14973                          schema:
14974                              $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
14975          components:
14976              schemas:
14977                  DiscrepancyReport:
14978                      type: object
14979                      required:
14980                          - resolutionUri
14981                          - reportType
14982                          - discrepancyReportSubmitTimeStamp
14983                          - discrepancyReportId
14984                          - reportingAgencyName
14985                          - reportingContactJcard
14986                          - problemSeverity
14987                      properties:
14988                          resolutionUri:
14989                              type: string
14990                              format: uri
14991                              example: https://agencyX.com/DiscrepancyReports/resolutions
14992                          reportType:
14993                              type: string
14994                              enum: [PolicyStoreDiscrepancyReport, LostDiscrepancyReport,
14995                                BcfDiscrepancyReport, LoggingDiscrepancyReport,
14996                                CallTakerDiscrepancyReport,
14997                                SipDiscrepancyReport, PermissionsDiscrepancyReport,
14998                                GisDiscrepancyReport, LisDiscrepancyReport, PolicyDiscrepancyReport,
14999                                OriginatingServiceDiscrepancyReport,
15000                                CallTransferDiscrepancyReport, McsDiscrepancyReport,
15001                                EsrpDiscrepancyReport, AdrDiscrepancyReport,
15002                                NetworkDiscrepancyReport, ImrDiscrepancyReport,
15003                                TestCallDiscrepancyReport, LogSignatureCertificateDiscrepancyReport]
15004                          discrepancyReportSubmitTimeStamp:
15005                              type: string
```

[MM/DD/YYYY]

Page 605 of 675



```
15006      format: date-time
15007      example: '2020-03-10T10:00:00-05:00'
15008      discrepancyReportId:
15009          type: string
15010      reportingAgencyName:
15011          type: string
15012      reportingAgentId:
15013          type: string
15014      reportingContactJcard:
15015          type: string
15016      problemService:
15017          type: string
15018      problemSeverity:
15019          type: string
15020      problemComments:
15021          type: string
15022      discriminator:
15023          propertyName: reportType
15024      DiscrepancyReportResponse:
15025          type: object
15026          required:
15027              - respondingAgencyName
15028              - respondingContactJcard
15029      properties:
15030          respondingAgencyName:
15031              type: string
15032          respondingContactJcard:
15033              type: string
15034          respondingAgentId:
15035              type: string
15036          responseEstimatedReturnTime:
15037              type: string
15038              format: date-time
15039              example: '2020-03-10T10:00:00-05:00'
15040          responseComments:
15041              type: string
15042      DiscrepancyResolution:
15043          type: object
15044          required:
15045              - respondingAgencyName
15046              - respondingContactJcard
15047              - discrepancyReportId
15048              - reportingAgencyName
15049              - problemService
```

[MM/DD/YYYY]

Page 606 of 675



```
15050      - responseTime
15051      - resolution
15052 properties:
15053     respondingAgencyName:
15054       type: string
15055     respondingContactJcard:
15056       type: string
15057     respondingAgentId:
15058       type: string
15059     discrepancyReportId:
15060       type: string
15061     reportingAgencyName:
15062       type: string
15063     problemService:
15064       type: string
15065     responseTime:
15066       type: string
15067       format: date-time
15068       example: '2020-03-10T10:00:00-05:00'
15069     reportingAgentId:
15070       type: string
15071     responseComments:
15072       type: string
15073     resolution:
15074       type: string
15075       enum: [DiscrepancyCorrected, NoDiscrepancy, OtherResponse,
15076 PolicyAdded, PolicyUpdated, NoSuchPolicy, InsufficientCredentials,
15077 EntryAdded,
15078           PerPolicy, CallTakerAdvised, TransferCorrect,
15079 BadCertificateChain, DataCorrected, RecordsCorrected,
15080 PermissionsCorrected,
15081           DeviceConfigError, PolicyCorrected, NoError,
15082 ProblemCorrected, InvalidRecord, Gis, Acknowledged, OtherResponse]
15083   StatusUpdate:
15084     type: object
15085   required:
15086     - respondingAgencyName
15087     - respondingContactJcard
15088     - responseEstimatedReturnTime
15089 properties:
15090   respondingAgencyName:
15091     type: string
15092   respondingContactJcard:
15093     type: string
```

[MM/DD/YYYY]

Page 607 of 675



```
15094      respondingAgentId:  
15095          type: string  
15096      responseEstimatedReturnTime:  
15097          type: string  
15098          format: date-time  
15099          example: '2020-03-10T10:00:00-05:00'  
15100      statusComments:  
15101          type: string  
15102  PolicyStoreDiscrepancyReport:  
15103      allOf:  
15104          - $ref: '#/components/schemas/DiscrepancyReport'  
15105          - type: object  
15106          required:  
15107              - policyAgencyName  
15108              - problem  
15109              - retrievePolicyResponse  
15110      properties:  
15111          policyType:  
15112              type: string  
15113          policyQueueName:  
15114              type: string  
15115          policyId:  
15116              type: string  
15117          policyAgencyName:  
15118              type: string  
15119          problem:  
15120              type: string  
15121              enum: [PolicyInvalid, PolicyAltered,  
15122                  SignatureVerificationFailure, PolicyMissing, OtherPolicyStore]  
15123          retrievePolicyResponse:  
15124              type: string  
15125  LostDiscrepancyReport:  
15126      allOf:  
15127          - $ref: '#/components/schemas/DiscrepancyReport'  
15128          - type: object  
15129          required:  
15130              - query  
15131              - request  
15132              - response  
15133              - problem  
15134          properties:  
15135              query:  
15136                  type: string
```

[MM/DD/YYYY]

Page 608 of 675



```
15137          enum: [findService, getServiceBoundary, listServices,
15138      listServicesByLocation]
15139          request:
15140              type: string
15141          response:
15142              type: string
15143          problem:
15144              type: string
15145              enum: [BelievedValid, BelievedInvalid, NoSuchLocation,
15146 RouteIncorrect, MultipleMappings, ServiceBoundaryIncorrect,
15147 ServiceNumberIncorrect, DataExpired, IncorrectUri, LocationErrorInError,
15148 OtherLost]
15149          discrepancyDetail:
15150              type: string
15151      BcfDiscrepancyReport:
15152          allOf:
15153              - $ref: '#/components/schemas/DiscrepancyReport'
15154              - type: object
15155                  required:
15156                      - problem
15157                      - sosSource
15158                      - eventTimestamp
15159                  properties:
15160                      request:
15161                          type: string
15162                      problem:
15163                          type: string
15164                          enum: [InitialTrafficBlocked, MidTrafficBlocked, BadSdp,
15165 BadSip, MediaLoss, TrafficNotBlockedBadActor, TrafficNotBlocked, Qos,
15166 BadCdr, Tty, Firewall, OtherBcf]
15167                      sosSource:
15168                          type: string
15169                          format: byte
15170                      eventTimestamp:
15171                          type: string
15172                          format: date-time
15173                          example: '2020-03-10T10:00:00-05:00'
15174                      packetHeader:
15175                          type: string
15176      LoggingDiscrepancyReport:
15177          allOf:
15178              - $ref: '#/components/schemas/DiscrepancyReport'
15179              - type: object
15180                  required:
```

[MM/DD/YYYY]

Page 609 of 675



```
15181      - request
15182      - problem
15183      - result
15184      properties:
15185          request:
15186              type: string
15187          problem:
15188              type: string
15189              enum: [InviteSrsError, LogEventError, RetrieveLogEventError,
15190      OtherLogging]
15191          result:
15192              type: string
15193          callIdUrn:
15194              type: string
15195          incidentIdUrn:
15196              type: string
15197      CallTakerDiscrepancyReport:
15198          allOf:
15199              - $ref: '#/components/schemas/DiscrepancyReport'
15200              - type: object
15201                  required:
15202                      - callIdUrn
15203                      - incidentIdUrn
15204                      - pidfLo
15205                      - callHeader
15206                  properties:
15207                      callIdUrn:
15208                          type: string
15209                      incidentIdUrn:
15210                          type: string
15211                      pidfLo:
15212                          type: string
15213                      callHeader:
15214                          type: string
15215      SipDiscrepancyReport:
15216          allOf:
15217              - $ref: '#/components/schemas/DiscrepancyReport'
15218              - type: object
15219                  required:
15220                      - problem
15221                  properties:
15222                      problem:
15223                          type: string
```

[MM/DD/YYYY]

Page 610 of 675



```
15224          enum: [InitialINVITE, MESSAGE, OPTIONS, MidDialog,
15225  RequiredMedia, MediaProblem, EngorgedQ, Signaling, OtherSip]
15226          callIdUrn:
15227              type: string
15228          incidentIdUrn:
15229              type: string
15230          testCallGenerator:
15231              type: string
15232          request:
15233              type: string
15234          result:
15235              type: string
15236          queueName:
15237              type: string
15238      PermissionsDiscrepancyReport:
15239          allOf:
15240              - $ref: '#/components/schemas/DiscrepancyReport'
15241              - type: object
15242                  required:
15243                      - problem
15244                      - resource
15245                      - identity
15246                      - result
15247                  properties:
15248                      problem:
15249                          type: string
15250                          enum: [UnableAuthenticate, UnableSubscribe, AbleSubscribe,
15251  UnableRead, UnableWrite, UnableDelete, AbleRead, AbleWrite, AbleDelete,
15252  OtherPermissions]
15253                      resource:
15254                          type: string
15255                      identity:
15256                          type: string
15257                      result:
15258                          type: string
15259                      detail:
15260                          type: string
15261      GisDiscrepancyReport:
15262          allOf:
15263              - $ref: '#/components/schemas/DiscrepancyReport'
15264              - type: object
15265                  required:
15266                      - problem
15267                  properties:
```

[MM/DD/YYYY]

Page 611 of 675



```
15268     problem:
15269         type: string
15270         enum: [Gap, Overlap, IncorrectLost, BadGeometry,
15271             DuplicateAttribute, OmittedField, IncorrectDataType, AddressRange,
15272             GeneralProvisioning, MalformedUri, DisplayData, OtherGis]
15273         layerIds:
15274             type: string
15275         location:
15276             type: string
15277         lostUri:
15278             type: string
15279             format: uri
15280         detail:
15281             type: string
15282     LisDiscrepancyReport:
15283         allOf:
15284             - $ref: '#/components/schemas/DiscrepancyReport'
15285             - type: object
15286                 required:
15287                     - problem
15288                 properties:
15289                     problem:
15290                         type: string
15291                         enum: [IncorrectRecords, OwnLocationUnavailable,
15292                             LocationReferenceNotResolved, BadPidfLo, IncorrectLocation, OtherLis]
15293                     ownLocationRequest:
15294                         type: string
15295                     locationUrn:
15296                         type: string
15297                     pidfLo:
15298                         type: string
15299     PolicyDiscrepancyReport:
15300         allOf:
15301             - $ref: '#/components/schemas/DiscrepancyReport'
15302             - type: object
15303                 required:
15304                     - policyId
15305                 properties:
15306                     policyId:
15307                         type: string
15308                     problem:
15309                         type: string
```

[MM/DD/YYYY]

Page 612 of 675



```
15310          enum: [InvalidUrn, UnknownPSAP, ConflictingRoute,
15311          OtherConflict, IncorrectUrn, Malformed, Loop, VerificationFailure,
15312          OtherPolicy]
15313          location:
15314              type: string
15315          callId:
15316              type: string
15317          routeUrn:
15318              type: string
15319      OriginatingServiceDiscrepancyReport:
15320          allOf:
15321              - $ref: '#/components/schemas/DiscrepancyReport'
15322              - type: object
15323                  required:
15324                      - problem
15325                  properties:
15326                      problem:
15327                          type: string
15328                          enum: [LocationNotLvfValid, LocationNotUsable, NoAni,
15329                          BadPidfLo, QueryTimeOut, CallDropped, IncorrectLocation, BadSip,
15330                          CallDrought, CallFlood, InvalidAddr, BadAdditionalData, OtherOsp, StiError]
15331                      status:
15332                          type: string
15333                      location:
15334                          type: string
15335                      locationId:
15336                          type: string
15337                      locationCorrect:
15338                          type: string
15339                      callHeader:
15340                          type: string
15341                      callVolume:
15342                          type: integer
15343                          format: int32
15344                      callVolumeTimePeriod:
15345                          type: integer
15346                          format: int32
15347      CallTransferDiscrepancyReport:
15348          allOf:
15349              - $ref: '#/components/schemas/DiscrepancyReport'
15350              - type: object
15351                  required:
15352                      - callId
15353                      - incidentId
```

[MM/DD/YYYY]

Page 613 of 675



```
15354      - origin
15355      - status
15356      - destination
15357      properties:
15358          callId:
15359              type: string
15360          incidentId:
15361              type: string
15362          origin:
15363              type: string
15364          status:
15365              type: string
15366          destination:
15367              type: string
15368      McsDiscrepancyReport:
15369          allOf:
15370              - $ref: '#/components/schemas/DiscrepancyReport'
15371              - type: object
15372                  required:
15373                      - serviceCall
15374                      - pidfLo
15375                      - msag
15376                      - statusCode
15377          properties:
15378              serviceCall:
15379                  type: string
15380              pidfLo:
15381                  type: string
15382              msag:
15383                  type: string
15384              statusCode:
15385                  type: string
15386              referral:
15387                  type: string
15388      EsrpDiscrepancyReport:
15389          allOf:
15390              - $ref: '#/components/schemas/DiscrepancyReport'
15391              - type: object
15392                  required:
15393                      - problem
15394          properties:
15395              problem:
15396                  type: string
15397                  enum: [CallReceived, EngorgedQ, CallDrought]
```

[MM/DD/YYYY]

Page 614 of 675



```
15398      callId:  
15399          type: string  
15400      incidentId:  
15401          type: string  
15402      pidfLo:  
15403          type: string  
15404      queueName:  
15405          type: string  
15406      AdrDiscrepancyReport:  
15407          allOf:  
15408              - $ref: '#/components/schemas/DiscrepancyReport'  
15409              - type: object  
15410                  required:  
15411                      - problem  
15412                  properties:  
15413                      problem:  
15414                          type: string  
15415                          enum: [ReferenceNotResolved, Malformed, UnknownBlock,  
15416 ReceivedIncorrectData, TooManyUris, OtherAdr]  
15417                      block:  
15418                          type: string  
15419                      location:  
15420                          type: string  
15421                      identity:  
15422                          type: string  
15423                      url:  
15424                          type: string  
15425                          format: uri  
15426                      result:  
15427                          type: string  
15428      NetworkDiscrepancyReport:  
15429          allOf:  
15430              - $ref: '#/components/schemas/DiscrepancyReport'  
15431              - type: object  
15432                  required:  
15433                      - problem  
15434                      - timestamp  
15435                  properties:  
15436                      problem:  
15437                          type: string  
15438                          enum: [ReferenceNotResolved, Malformed, UnknownBlock,  
15439 ReceivedIncorrectData, TooManyUris, OtherAdr]  
15440                      ipAddressLocal:  
15441                          type: string
```

[MM/DD/YYYY]

Page 615 of 675



```
15442      format: ipv4
15443  ipAddressRemote:
15444      type: string
15445      format: ipv4
15446  url:
15447      type: string
15448      format: uri
15449  timestamp:
15450      type: string
15451      format: date-time
15452      example: '2020-03-10T10:00:00-05:00'
15453  ImrDiscrepancyReport:
15454    allOf:
15455      - $ref: '#/components/schemas/DiscrepancyReport'
15456      - type: object
15457        required:
15458          - problem
15459          - callId
15460          - callHeader
15461        properties:
15462          problem:
15463            type: string
15464            enum: [EngorgedQ, ResponseIncorrect, ResponseConfusing,
15465              CallTransferIncorrect, ExcessiveSilence, UnknownScript, InputFailed,
15466              ScriptLogicFailure, OtherImr]
15467          callId:
15468            type: string
15469          incidentId:
15470            type: string
15471          callHeader:
15472            type: string
15473  TestCallDiscrepancyReport:
15474    allOf:
15475      - $ref: '#/components/schemas/DiscrepancyReport'
15476      - type: object
15477        required:
15478          - problem
15479          - callIdUrn
15480          - request
15481          - nbrOfCalls
15482          - successCount
15483          - failCount
15484          - time
15485          - result
```

[MM/DD/YYYY]

Page 616 of 675



```
15486          - mediaOk
15487      properties:
15488          problem:
15489              type: string
15490              enum: [TestInvite, TestMessage, TestOptions, TestMidDialog,
15491      TestMedia, TestLoopbackMedia, TestSignaling, OtherTestCall]
15492          callIdUrn:
15493              type: string
15494              format: uri
15495          request:
15496              type: string
15497          nbrOfCalls:
15498              type: integer
15499              format: int32
15500          successCount:
15501              type: integer
15502              format: int32
15503          failCount:
15504              type: integer
15505              format: int32
15506          time:
15507              type: string
15508              format: date-time
15509              example: '2020-03-10T10:00:00-05:00'
15510          result:
15511              type: integer
15512              format: int32
15513          contact:
15514              type: string
15515          sdp:
15516              type: string
15517          mediaOk:
15518              type: boolean
15519      LogSignatureCertificateDiscrepancyReport:
15520          allOf:
15521              - $ref: '#/components/schemas/DiscrepancyReport'
15522              - type: object
15523                  required:
15524                      - problem
15525                      - logIdentifier
15526          properties:
15527              problem:
15528                  type: string
```

[MM/DD/YYYY]

Page 617 of 675



```
15529          enum: [BadAlgorithm, NoCert, BadURL, BadThumb, BadCertX5c,
15530      BadCertX5u, BadSignature, OtherLogSignature]
15531          logIdentifier:
15532              type: string
15533          result:
15534              type: string
15535          thumbCalc:
15536              type: string
```

15537 **E.2.2 Examples**

15538 **E.3 Dequeue Registration**

15539 **E.3.1 OpenAPI Interface Description**

```
15540 openapi: 3.0.1
15541 info:
15542     title: Dequeue Registration Service
15543     version: "1.0"
15544 servers:
15545     - url: http://localhost/DequeueRegistration/v1
15546 paths:
15547     /Registrations:
15548         put:
15549             tags:
15550                 - DequeueRegistration
15551             summary: Registers or deregisters an entity as a dequeuer
15552             operationId: DequeueRegistration
15553             requestBody:
15554                 description: Registration details
15555                 content:
15556                     application/json:
15557                         schema:
15558                             $ref: '#/components/schemas/Registration'
15559             required: true
15560             responses:
15561                 '200':
15562                     description: Registration successfully updated/created
15563                     content:
15564                         application/json:
15565                             schema:
15566                                 type: object
15567                                 properties:
```

[MM/DD/YYYY]

Page 618 of 675



```
15568           expirationTime:  
15569             type: integer  
15570             format: int32  
15571             description: Time in seconds this registration will  
15572     expire.  
15573       '400':  
15574         description: Bad request  
15575       '454':  
15576         description: Unspecified Error  
15577       '456':  
15578         description: Bad queue  
15579       '457':  
15580         description: Bad dequeuePreference  
15581       '458':  
15582         description: Policy violation  
15583 /Versions:  
15584   servers:  
15585     - url: https://api.example.com/DequeueRegistration  
15586       description: Override base path for Versions query  
15587   get:  
15588     tags:  
15589       - RetrieveVersions  
15590     summary: Retrieves all supported versions, vendor parameter is  
15591 optional.  
15592     operationId: RetrieveVersions  
15593   responses:  
15594     '200':  
15595       description: Versions found  
15596       content:  
15597         application/json:  
15598           schema:  
15599             $ref: 'i3-common.yaml#/components/schemas/VersionsArray'  
15600 components:  
15601   schemas:  
15602     Registration:  
15603       type: object  
15604       required:  
15605         - queueUri  
15606         - dequeuerUri  
15607         - expirationTime  
15608   properties:  
15609     queueUri:  
15610       type: string  
15611       format: uri
```

[MM/DD/YYYY]

Page 619 of 675



```
15612      dequeuerUri:  
15613          type: string  
15614          format: uri  
15615      expirationTime:  
15616          type: integer  
15617          format: int32  
15618          description: Time in seconds this registration will expire.  
15619      expirationTime set to zero is a request to deregister.  
15620      dequeuePreference:  
15621          type: integer  
15622          format: int32  
15623          minimum: 1  
15624          maximum: 5
```

15625 **E.4 MSAG Conversion Service**

15626 **E.4.1 OpenAPI Interface Description**

```
15627  openapi: 3.0.1  
15628  info:  
15629      title: MSAG Conversion Service  
15630      version: "1.0"  
15631  servers:  
15632      - url: http://localhost/Mcs/v1  
15633  paths:  
15634      /PfdfloToMsag:  
15635          post:  
15636              tags:  
15637                  - PIDFLOtoMSAGConversion  
15638              summary: Converts PIDF-LO to MSAG data  
15639              operationId: PIDFLOtoMSAGConversion  
15640              requestBody:  
15641                  description: PIDF-LO data  
15642                  content:  
15643                      application/json:  
15644                          schema:  
15645                              type: string  
15646                          required: true  
15647              responses:  
15648                  '200':  
15649                      description: Data successfully converted  
15650                      content:  
15651                          application/xml:  
15652                          schema:
```

[MM/DD/YYYY]

Page 620 of 675



```
15653                     $ref: '#/components/schemas/MsagData'
15654 '307':
15655     description: Temporary Redirect
15656     headers:
15657         Location:
15658             description: Referral URI of another MCS
15659             schema:
15660                 type: string
15661                 format: uri
15662 '454':
15663     description: Unspecified Error
15664 '468':
15665     description: No Address Found
15666 '469':
15667     description: Unknown MCS/GCS
15668 /MsagToPpdfLo:
15669     post:
15670         tags:
15671             - MSAGtoPIDFLOConversion
15672         summary: Converts MSAG to PIDF-LO data
15673         operationId: MSAGtoPIDFLOConversion
15674         requestBody:
15675             description: MSAG data
15676             content:
15677                 application/json:
15678                     schema:
15679                         type: string
15680             required: true
15681         responses:
15682 '200':
15683     description: Data successfully converted
15684     content:
15685         application/xml:
15686             schema:
15687                 $ref: '#/components/schemas/PidfLoData'
15688 '307':
15689     description: Temporary Redirect
15690     headers:
15691         Location:
15692             description: Referral URI of another MCS
15693             schema:
15694                 type: string
15695                 format: uri
15696 '454':
```

[MM/DD/YYYY]

Page 621 of 675



```
15697         description: Unspecified Error
15698     '468':
15699         description: No Address Found
15700     '469':
15701         description: Unknown MCS/GCS
15702 /Versions:
15703     servers:
15704         - url: https://api.example.com/Mcs
15705             description: Override base path for Versions query
15706     get:
15707         tags:
15708             - RetrieveVersions
15709         summary: Retrieves all supported versions, vendor parameter is
15710 optional.
15711         operationId: RetrieveVersions
15712         responses:
15713             '200':
15714                 description: Versions found
15715                 content:
15716                     application/json:
15717                         schema:
15718                             $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
15719     components:
15720     schemas:
15721         PidfLoData:
15722             type: object
15723             required:
15724                 - pidfLoAddress
15725             properties:
15726                 pidfLoAddress:
15727                     type: string
15728         MsagData:
15729             type: object
15730             required:
15731                 - msagAddress
15732             properties:
15733                 msagAddress:
15734                     type: string
```

15735 **E.4.2 Examples**

15736 **E.5 Geocode Conversion Service**

15737 **E.5.1 OpenAPI Interface Description**

```
15738     openapi: 3.0.1
15739     info:
15740         title: Geocode Conversion Service
15741         version: "1.0"
15742     servers:
15743         - url: http://localhost/Gcs/v1
15744     paths:
15745         /Geocode:
15746             post:
15747                 tags:
15748                     - GeocodeRequest
15749                 summary: Converts civic address to geodetic representation of the
15750                 location in PIDF-LO format
15751                 operationId: GeocodeRequest
15752                 requestBody:
15753                     description: PIDF-LO data
15754                     content:
15755                         application/json:
15756                             schema:
15757                                 type: string
15758                                 required: true
15759                 responses:
15760                     '200':
15761                         description: Data successfully converted
15762                         content:
15763                             application/xml:
15764                             schema:
15765                                 $ref: '#/components/schemas/GeodeticData'
15766                     '307':
15767                         description: Temporary Redirect
15768                         headers:
15769                             Location:
15770                             description: Referral URI of another GCS
15771                             schema:
15772                                 type: string
15773                                 format: uri
15774                     '454':
```

[MM/DD/YYYY]

Page 623 of 675



```
15775      description: Unspecified Error
15776      '468':
15777          description: No Address Found
15778      '469':
15779          description: Unknown MCS/GCS
15780  /ReverseGeocode:
15781      post:
15782          tags:
15783              - ReverseGeocodeRequest
15784          summary: Converts geodetic representation of the location to civic
15785          address in PIDF-LO format
15786          operationId: ReverseGeocodeRequest
15787          requestBody:
15788              description: PIDF-LO data
15789          content:
15790              application/json:
15791                  schema:
15792                      type: string
15793          required: true
15794  responses:
15795      '200':
15796          description: Data successfully converted
15797          content:
15798              application/xml:
15799                  schema:
15800                      $ref: '#/components/schemas/CivicAddress'
15801      '307':
15802          description: Temporary Redirect
15803          headers:
15804              Location:
15805                  description: Referral URI of another GCS
15806          schema:
15807              type: string
15808              format: uri
15809      '468':
15810          description: No Address Found
15811      '469':
15812          description: Unknown MCS/GCS
15813  /Versions:
15814      servers:
15815          - url: https://api.example.com/Gcs
15816              description: Override base path for Versions query
15817  get:
15818      tags:
```

[MM/DD/YYYY]

Page 624 of 675



```
15819      - RetrieveVersions
15820      summary: Retrieves all supported versions, vendor parameter is
15821      optional.
15822      operationId: RetrieveVersions
15823      responses:
15824      '200':
15825          description: Versions found
15826          content:
15827              application/json:
15828                  schema:
15829                      $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
15830      components:
15831      schemas:
15832          GeodeticData:
15833              type: object
15834              required:
15835                  - pidfLoGeo
15836              properties:
15837                  pidfLoGeo:
15838                      type: string
15839          CivicAddress:
15840              type: object
15841              required:
15842                  - pidfLoAddress
15843              properties:
15844                  pidfLoAddress:
15845                      type: string
```

15846 **E.5.2 Examples**

15847 **E.6 Test Call**

15848 **E.6.1 OpenAPI Interface Description**

```
15849     openapi: 3.0.1
15850     info:
15851         title: Test Call Service
15852         version: "1.0"
15853     servers:
15854         - url: http://localhost/TestCall/v1
15855     paths:
15856         /SendCallRequests/{psapId}:
15857             put:
```

[MM/DD/YYYY]

Page 625 of 675



```
15858      tags:
15859          - SendCallRequests
15860      summary: Updates an existing send call request identified by the
15861      PSAP ID or creates a new one if the request does not exist
15862      operationId: SendCallRequests
15863      parameters:
15864          - name: psapId
15865              in: path
15866              description: ID of the PSAP which wishes to have test calls sent
15867      to it
15868          required: true
15869          schema:
15870              type: string
15871      requestBody:
15872          description: Request to update/create
15873          content:
15874              application/json:
15875                  schema:
15876                      $ref: '#/components/schemas/SendCallRequests'
15877          required: true
15878      responses:
15879          '200':
15880              description: Request successfully updated/created
15881          '442':
15882              description: Unacceptable Parameters
15883          '454':
15884              description: Unspecified Error
15885          '458':
15886              description: Policy violation
15887      /Versions:
15888      servers:
15889          - url: https://api.example.com/TestCall
15890              description: Override base path for Versions query
15891      get:
15892          tags:
15893              - RetrieveVersions
15894          summary: Retrieves all supported versions, vendor parameter is
15895      optional.
15896          operationId: RetrieveVersions
15897          responses:
15898              '200':
15899                  description: Versions found
15900                  content:
15901                      application/json:
```

[MM/DD/YYYY]

Page 626 of 675



```
15902          schema:
15903              $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
15904      components:
15905          schemas:
15906              SendCallRequests:
15907                  type: object
15908                  required:
15909                      - psapId
15910                      - location
15911                      - frequency
15912                      - discrepancyRateLimit
15913                      - startDate
15914                      - endDate
15915              properties:
15916                  psapId:
15917                      type: string
15918                      readOnly: true
15919                  location:
15920                      type: string
15921                  frequency:
15922                      type: integer
15923                      format: int32
15924                  discrepancyRateLimit:
15925                      type: integer
15926                      format: int32
15927                  startDate:
15928                      type: string
15929                      format: date-time
15930                      example: '2020-03-10T10:00:00-05:00'
15931                  endDate:
15932                      type: string
15933                      format: date-time
15934                      example: '2020-03-11T10:00:00-05:00'
15935              testConditions:
15936                  $ref: '#/components/schemas/PrrTest'
15937          PrrTest:
15938              type: object
15939              required:
15940                  - hostName
15941                  - nominalNextHop
15942                  - conditions
15943              properties:
15944                  hostName:
15945                      type: string
```

[MM/DD/YYYY]

Page 627 of 675



```
15946           description: ESRP Hostname that test conditions are specified  
15947   for.  
15948     nominalNextHop:  
15949       type: string  
15950       format: uri  
15951       description: URI of for nominal next hop that rule set  
15952   conditions are applied to.  
15953     conditions:  
15954       type: array  
15955       items:  
15956         type: object  
15957         required:  
15958           - name  
15959           - value  
15960       properties:  
15961         name:  
15962           $ref: 'i3-common.yaml#/components/schemas/ConditionType'  
15963           description: Condition name  
15964         value:  
15965           type: string  
15966           description: Condition value
```

15967 **E.6.2 Examples**

15968 **E.7 Additional Data Repository**

15969 **E.7.1 OpenAPI Interface Description**

```
15970   openapi: 3.0.1  
15971   info:  
15972     title: IS-ADR Service  
15973     version: "1.0"  
15974   servers:  
15975     - url: http://localhost/Adr/v1  
15976   paths:  
15977     /AdditionalData:  
15978       get:  
15979         tags:  
15980           - RetrieveCallerAdditionalData  
15981         summary: Retrieves Additional Data of the caller in XML format or a  
15982   reference to the Additional Data. Provides ADR search capability by  
15983   identity (Identity-Searchable).  
15984         operationId: RetrieveCallerAdditionalData
```

[MM/DD/YYYY]

Page 628 of 675



```
15985     parameters:
15986         - name: callerUri
15987             in: query
15988             description: Caller URI (taken from From or PAI)
15989             required: true
15990             schema:
15991                 type: string
15992     responses:
15993         '200':
15994             description: Additional Data found
15995             content:
15996                 application/xml:
15997                     schema:
15998                         $ref: '#/components/schemas/AdditionalDataValue'
15999                 application/json:
16000                     schema:
16001                         $ref: '#/components/schemas/AdditionalDataReference'
16002         '307':
16003             description: Temporary Redirect
16004             headers:
16005                 Location:
16006                     description: Referral URI of ADR
16007                     schema:
16008                         type: string
16009                         format: uri
16010         '404':
16011             description: Not found
16012         '454':
16013             description: Unspecified Error
16014     /Versions:
16015         servers:
16016             - url: https://api.example.com/Adr
16017                 description: Override base path for Versions query
16018         get:
16019             tags:
16020                 - RetrieveVersions
16021                 summary: Retrieves all supported versions, vendor parameter is
16022                     optional.
16023                 operationId: RetrieveVersions
16024             responses:
16025                 '200':
16026                     description: Versions found
16027                     content:
16028                         application/json:
```



```
16029          schema:
16030            $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
16031      components:
16032        schemas:
16033          AdditionalDataValue:
16034            type: string
16035          AdditionalDataReference:
16036            type: string
```

16037 **E.7.2 Examples**

16038 **E.8 Logging Service**

16039 **E.8.1 OpenAPI Interface Description**

```
16040    openapi: 3.0.1
16041    info:
16042      title: Logging Service
16043      version: "1.0"
16044    servers:
16045      - url: https://api.example.com/Logging/v1
16046    paths:
16047      /LogEvents:
16048        get:
16049          tags:
16050            - RetrieveLogEvents, ListLogEventsByEventTypeAndDateRange
16051          summary: Retrieves LogEvents. Use limit and start parameters for
16052            pagination.
16053          operationId: RetrieveLogEvents
16054          parameters:
16055            - name: limit
16056              in: query
16057              description: Maximum number of results to return
16058              required: false
16059              schema:
16060                type: integer
16061                format: int32
16062            - name: start
16063              in: query
16064              description: First item in the page of results, as an ordinal 1-
16065              based integer
16066              required: false
16067              schema:
```

[MM/DD/YYYY]

Page 630 of 675



```
16068      type: integer
16069      format: int32
16070      minimum: 1
16071      - name: logEventType
16072          in: query
16073          description: LogEvent type
16074          required: false
16075          schema:
16076              $ref: '#/components/schemas/LogEventType'
16077      - name: startTime
16078          in: query
16079          description: Start time
16080          required: false
16081          schema:
16082              type: string
16083              format: date-time
16084              example: '2020-03-10T11:00:01-05:00'
16085      - name: endTime
16086          in: query
16087          description: End time
16088          required: false
16089          schema:
16090              type: string
16091              format: date-time
16092              example: '2020-03-15T11:00:01-05:00'
16093      responses:
16094          '200':
16095              description: LogEvents found
16096              content:
16097                  application/json:
16098                      schema:
16099                          $ref: '#/components/schemas/LogEventContainerArray'
16100          '404':
16101              description: Not found
16102      post:
16103          tags:
16104              - LogEvent
16105          summary: Logs a new event into the Logging Service
16106          operationId: LogEvent
16107          requestBody:
16108              description: LogEvent data to add (JWS using flattened JSON
16109          serialization)
16110              content:
16111                  application/json:
```

[MM/DD/YYYY]

Page 631 of 675



```
16112      schema:
16113          $ref: 'i3-common.yaml#/components/schemas/Jws'
16114      required: true
16115      responses:
16116          '201':
16117              description: LogEvent successfully logged
16118              content:
16119                  application/json:
16120                      schema:
16121                          type: string
16122                          description: logEventId of the new logEvent
16123          '434':
16124              description: Signature Verification Failure
16125          '438':
16126              description: Unacceptable Algorithm
16127          '454':
16128              description: Unspecified Error
16129          '460':
16130              description: Bad LogEvent
16131          '461':
16132              description: LogEvent too big
16133          '462':
16134              description: LogEvent extension not on approved list
16135          '463':
16136              description: LogEvent extension on disallowed list
16137 /LogEvents/{logEventId}:
16138     get:
16139         tags:
16140             - RetrieveLogEvent
16141         summary: Retrieves a LogEvent based on logEventId. LogEvent is
16142             returned in JWS using flattened JSON serialization
16143         operationId: RetrieveLogEvent
16144         parameters:
16145             - name: logEventId
16146                 in: path
16147                 description: ID of the logEvent
16148                 required: true
16149                 schema:
16150                     type: string
16151         responses:
16152             '200':
16153                 description: LogEvent found
16154                 content:
16155                     application/json:
```

[MM/DD/YYYY]

Page 632 of 675



```
16156          schema:
16157              $ref: 'i3-common.yaml#/components/schemas/Jws'
16158      '404':
16159          description: Not found
16160  /Conversations:
16161      get:
16162          tags:
16163              - RetrieveConversationText
16164          summary: Returns an HTML formatted record suitable for human
16165          consumption of the text portion of a call, including all text sent by all
16166          parties.
16167          operationId: RetrieveConversationText
16168          parameters:
16169              - name: callId
16170                  in: query
16171                  description: Call ID of the call
16172                  required: true
16173                  schema:
16174                      type: string
16175          responses:
16176      '200':
16177          description: Conversation found
16178          content:
16179              application/json:
16180                  schema:
16181                      type: string
16182      '404':
16183          description: Not found
16184      '454':
16185          description: Unspecified Error
16186      '464':
16187          description: No Text in this Call
16188  /LogEventIds:
16189      get:
16190          tags:
16191              - ListLogEventsByCallId, ListLogEventsByIncidentId
16192          summary: Retrieves LogEvents IDs. Use limit and start parameters for
16193          pagination.
16194          operationId: ListLogEventsById
16195          parameters:
16196              - name: limit
16197                  in: query
16198                  description: Maximum number of results to return
16199                  required: false
```



```
16200      schema:
16201          type: integer
16202          format: int32
16203      - name: start
16204          in: query
16205          description: First item in the page of results, as an ordinal 1-
16206          based integer
16207          required: false
16208          schema:
16209              type: integer
16210              format: int32
16211              minimum: 1
16212      - name: callId
16213          in: query
16214          description: Call ID of the call
16215          required: false
16216          schema:
16217              type: string
16218      - name: incidentId
16219          in: query
16220          description: Incident ID of the call
16221          required: false
16222          schema:
16223              type: string
16224      responses:
16225          '200':
16226              description: LogEvents found
16227              content:
16228                  application/json:
16229                      schema:
16230                          $ref: '#/components/schemas/LogEventIdArray'
16231          '404':
16232              description: Not found
16233          '454':
16234              description: Unspecified Error
16235      /CallIds:
16236          get:
16237              tags:
16238                  - ListCallsByIncidentId, ListCallsByDateRange, ListCallsByLocation
16239              summary: Returns a list of Call Identifiers associated with a
16240              specific Incident Tracking Identifier, occurred within a time range or
16241              within a specified geographic region.
16242          operationId: ListCalls
16243          parameters:
```

[MM/DD/YYYY]

Page 634 of 675



```
16244      - name: limit
16245          in: query
16246          description: Maximum number of results to return
16247          required: false
16248          schema:
16249              type: integer
16250              format: int32
16251      - name: start
16252          in: query
16253          description: First item in the page of results, as an ordinal 1-
16254          based integer
16255          required: false
16256          schema:
16257              type: integer
16258              format: int32
16259              minimum: 1
16260      - name: incidentId
16261          in: query
16262          description: Incident ID of the call
16263          required: false
16264          schema:
16265              type: string
16266      - name: startTime
16267          in: query
16268          description: Start time
16269          required: false
16270          schema:
16271              type: string
16272              format: date-time
16273              example: '2020-03-10T11:00:01-05:00'
16274      - name: endTime
16275          in: query
16276          description: End time
16277          required: false
16278          schema:
16279              type: string
16280              format: date-time
16281              example: '2020-03-15T11:00:01-05:00'
16282      - name: area
16283          in: query
16284          description: Area of interest
16285          required: false
16286          schema:
16287              type: string
```

[MM/DD/YYYY]

Page 635 of 675



```
16288     responses:
16289       '200':
16290         description: Calls found
16291         content:
16292           application/json:
16293             schema:
16294               $ref: '#/components/schemas/CallIdArray'
16295       '404':
16296         description: Not found
16297       '454':
16298         description: Unspecified Error
16299       '465':
16300         description: Bad Timestamp
16301       '466':
16302         description: endTime occurs before startTime
16303       '467':
16304         description: Bad Geoshape
16305   /IncidentIds:
16306     get:
16307       tags:
16308         - ListIncidentsByDateRange, ListIncidentsByLocation
16309       summary: Returns a list of Incident Tracking Identifiers occurring
16310       within a time/date range. Returns a list of Incidents that occurred within
16311       a specified geographic region.
16312       operationId: ListIncidents
16313       parameters:
16314         - name: limit
16315           in: query
16316           description: Maximum number of results to return
16317           required: false
16318           schema:
16319             type: integer
16320             format: int32
16321         - name: start
16322           in: query
16323           description: First item in the page of results, as an ordinal 1-
16324           based integer
16325           required: false
16326           schema:
16327             type: integer
16328             format: int32
16329             minimum: 1
16330         - name: startTime
16331           in: query
```

[MM/DD/YYYY]

Page 636 of 675



```
16332      description: Start time
16333      required: false
16334      schema:
16335          type: string
16336          format: date-time
16337          example: '2020-03-10T11:00:01-05:00'
16338      - name: endTime
16339          in: query
16340          description: End time
16341          required: false
16342          schema:
16343              type: string
16344              format: date-time
16345              example: '2020-03-15T11:00:01-05:00'
16346      - name: area
16347          in: query
16348          description: Area of interest
16349          required: false
16350          schema:
16351              type: string
16352      responses:
16353          '200':
16354              description: Incidents found
16355              content:
16356                  application/json:
16357                      schema:
16358                          $ref: '#/components/schemas/IncidentIdArray'
16359          '404':
16360              description: Not found
16361          '454':
16362              description: Unspecified Error
16363          '465':
16364              description: Bad Timestamp
16365          '466':
16366              description: endTime occurs before startTime
16367          '467':
16368              description: Bad Geoshape
16369      /AgencyIds:
16370          get:
16371              tags:
16372                  - ListAgenciesByCallId, ListAgenciesByIncidentId
16373              summary: Returns a list of agencies involved in a Call or an
16374              Incident.
16375          operationId: ListAgenciesById
```

[MM/DD/YYYY]

Page 637 of 675



```
16376     parameters:
16377         - name: limit
16378             in: query
16379             description: Maximum number of results to return
16380             required: false
16381             schema:
16382                 type: integer
16383                 format: int32
16384         - name: start
16385             in: query
16386             description: First item in the page of results, as an ordinal 1-
16387             based integer
16388             required: false
16389             schema:
16390                 type: integer
16391                 format: int32
16392                 minimum: 1
16393         - name: incidentId
16394             in: query
16395             description: Incident ID of the call
16396             required: false
16397             schema:
16398                 type: string
16399         - name: callId
16400             in: query
16401             description: Incident ID of the call
16402             required: false
16403             schema:
16404                 type: string
16405     responses:
16406         '200':
16407             description: Agencies found
16408             content:
16409                 application/json:
16410                     schema:
16411                         $ref: '#/components/schemas/AgencyIdArray'
16412         '404':
16413             description: Not found
16414         '454':
16415             description: Unspecified Error
16416     /Versions:
16417         servers:
16418             - url: https://api.example.com/Logging
16419             description: Override base path for Versions query
```

```
16420      get:
16421          tags:
16422              - RetrieveVersions
16423          summary: Retrieves all supported versions, vendor parameter is
16424          optional.
16425          operationId: RetrieveVersions
16426          responses:
16427              '200':
16428                  description: Versions found
16429                  content:
16430                      application/json:
16431                          schema:
16432                              $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
16433          components:
16434              schemas:
16435                  LogEventContainerArray:
16436                      type: object
16437                      required:
16438                          - count
16439                          - totalCount
16440                          - logEventContainers
16441          properties:
16442              count:
16443                  type: integer
16444                  format: int32
16445                  description: Number of items in the array
16446              totalCount:
16447                  type: integer
16448                  format: int32
16449                  description: Total number of items found
16450              logEventContainers:
16451                  type: array
16452                  items:
16453                      $ref: '#/components/schemas/LogEventContainer'
16454                      description: Array of LogEvent Container objects
16455          LogEventContainer:
16456              type: object
16457              required:
16458                  - logEventId
16459                  - logEvent
16460          properties:
16461              logEventId:
16462                  type: string
16463                  readOnly: true
```

[MM/DD/YYYY]

Page 639 of 675



```
16464      rtsp:
16465          type: array
16466          items:
16467              type: string
16468      logEvent:
16469          $ref: 'i3-common.yaml#/components/schemas/Jws'
16470  LogEventIdArray:
16471      type: object
16472      required:
16473          - count
16474          - totalCount
16475          - logEventIds
16476      properties:
16477          count:
16478              type: integer
16479              format: int32
16480              description: Number of items in the array
16481          totalCount:
16482              type: integer
16483              format: int32
16484              description: Total number of items found
16485          logEventIds:
16486              type: array
16487              items:
16488                  type: string
16489                  description: Array of LogEvent IDs
16490  CallIdArray:
16491      type: object
16492      required:
16493          - count
16494          - totalCount
16495          - callIds
16496      properties:
16497          count:
16498              type: integer
16499              format: int32
16500              description: Number of items in the array
16501          totalCount:
16502              type: integer
16503              format: int32
16504              description: Total number of items found
16505          callIds:
16506              type: array
16507              items:
```

[MM/DD/YYYY]

Page 640 of 675



```
16508      type: string
16509      description: Array of Call IDs
16510  IncidentIdArray:
16511      type: object
16512      required:
16513          - count
16514          - totalCount
16515          - incidentIds
16516  properties:
16517      count:
16518          type: integer
16519          format: int32
16520          description: Number of items in the array
16521  totalCount:
16522      type: integer
16523      format: int32
16524      description: Total number of items found
16525  logEventIds:
16526      type: array
16527      items:
16528          type: string
16529          description: Array of Incident IDs
16530  AgencyIdArray:
16531      type: object
16532      required:
16533          - count
16534          - totalCount
16535          - agencyIds
16536  properties:
16537      count:
16538          type: integer
16539          format: int32
16540          description: Number of items in the array
16541  totalCount:
16542      type: integer
16543      format: int32
16544      description: Total number of items found
16545  agencyIds:
16546      type: array
16547      items:
16548          type: string
16549          description: Array of Agency IDs
16550  LogEventType:
16551      type: string
```

[MM/DD/YYYY]

Page 641 of 675



```
16552     enum: [CallProcessLogEvent, CallStartLogEvent, CallEndLogEvent,
16553     RecCallStartLogEvent, RecCallEndLogEvent, CallTransferLogEvent,
16554     RouteLogEvent, MediaStartLogEvent, MediaEndLogEvent,
16555     RecMediaStartLogEvent, RecMediaEndLogEvent,
16556         RecordingFailedLogEvent, MessageLogEvent,
16557     AdditionalAgencyLogEvent, IncidentMergeLogEvent, IncidentUnMergeLogEvent,
16558     IncidentLinkLogEvent, IncidentUnLinkLogEvent, IncidentClearLogEvent,
16559     IncidentReopenLogEvent, LostQueryLogEvent,
16560         LostResponseLogEvent, CallSignalingMessageLogEvent,
16561     SipRecMetadataLogEvent, NonRtpMediaMessageLogEvent,
16562     AliLocationQueryLogEvent, AliLocationResponseLogEvent,
16563     MalformedMessageLogEvent, IncidentSplitLogEvent, EidoLogEvent,
16564         DiscrepancyReportLogEvent, ElementStateChangeLogEvent,
16565     ServiceStateChangeLogEvent, AdditionalDataQueryLogEvent,
16566     AdditionalDataResponseLogEvent, LocationQueryLogEvent,
16567     LocationResponseLogEvent, CallStateChangeLogEvent,
16568         GatewayCallLogEvent, HookflashLogEvent, LegacyDigitsLogEvent,
16569     AgentStateChangeLogEvent, QueueStateChangeLogEvent,
16570     KeepAliveFailureLogEvent, RouteRuleMsgLogEvent, PolicyChangeLogEvent,
16571         VersionsLogEvent, SubscribeLogEvent]
16572     LogEvent:
16573         type: object
16574         required:
16575             - logEventType
16576             - timestamp
16577             - agencyId
16578             - elementId
16579         properties:
16580             clientAssignedIdentifier:
16581                 type: string
16582             logEventType:
16583                 $ref: '#/components/schemas/LogEventType'
16584             timestamp:
16585                 type: string
16586                 format: date-time
16587                 example: '2020-03-10T11:00:01-05:00'
16588             elementId:
16589                 type: string
16590             agencyId:
16591                 type: string
16592             agencyAgentId:
16593                 type: string
16594             agencyPositionId:
16595                 type: string
```

[MM/DD/YYYY]

Page 642 of 675



```
16596      callId:  
16597          type: string  
16598      incidentId:  
16599          type: string  
16600      callIdSip:  
16601          type: string  
16602      ipAddressPort:  
16603          type: string  
16604      extension:  
16605          type: object  
16606      discriminator:  
16607          propertyName: logEventType  
16608  CallProcessLogEvent:  
16609      allOf:  
16610          - $ref: '#/components/schemas/LogEvent'  
16611  CallStartLogEvent:  
16612      allOf:  
16613          - $ref: '#/components/schemas/LogEvent'  
16614          - $ref: '#/components/schemas/CallLogEvent'  
16615  CallEndLogEvent:  
16616      allOf:  
16617          - $ref: '#/components/schemas/LogEvent'  
16618          - $ref: '#/components/schemas/CallLogEvent'  
16619  RecCallStartLogEvent:  
16620      allOf:  
16621          - $ref: '#/components/schemas/LogEvent'  
16622          - $ref: '#/components/schemas/CallLogEvent'  
16623  RecCallEndLogEvent:  
16624      allOf:  
16625          - $ref: '#/components/schemas/LogEvent'  
16626          - $ref: '#/components/schemas/CallLogEvent'  
16627  CallTransferLogEvent:  
16628      allOf:  
16629          - $ref: '#/components/schemas/LogEvent'  
16630          - type: object  
16631          required:  
16632              - target  
16633              - targetCallIdSip  
16634          properties:  
16635              target:  
16636                  type: string  
16637                  format: uri  
16638              targetCallIdSip:  
16639                  type: string
```

[MM/DD/YYYY]

Page 643 of 675



```
16640     RouteLogEvent:  
16641         allOf:  
16642             - $ref: '#/components/schemas/LogEvent'  
16643             - type: object  
16644                 required:  
16645                     - recipientUri  
16646                     - ruleId  
16647                     - policyOwner  
16648                     - policyType  
16649                 properties:  
16650                     recipientUri:  
16651                         type: string  
16652                         format: uri  
16653                     ruleId:  
16654                         type: string  
16655                     policyOwner:  
16656                         type: string  
16657                     policyType:  
16658                         type: string  
16659                     description: Values limited to those in the policyType  
16660             registry  
16661                 policyQueueName:  
16662                     type: string  
16663                     format: uri  
16664                     policyId:  
16665                         type: string  
16666                     cause:  
16667                         type: string  
16668             MediaStartLogEvent:  
16669                 allOf:  
16670                     - $ref: '#/components/schemas/LogEvent'  
16671                     - type: object  
16672                     required:  
16673                         - sdp  
16674                         - mediaLabel  
16675                         - direction  
16676                     properties:  
16677                         sdp:  
16678                             type: string  
16679                         mediaLabel:  
16680                             type: array  
16681                             items:  
16682                                 type: string  
16683                     direction:
```

[MM/DD/YYYY]

Page 644 of 675



```
16684           $ref: '#/components/schemas/Direction'  
16685 MediaEndLogEvent:  
16686     allOf:  
16687       - $ref: '#/components/schemas/LogEvent'  
16688       - type: object  
16689         required:  
16690           - mediaLabel  
16691         properties:  
16692           mediaLabel:  
16693             type: array  
16694             items:  
16695               type: string  
16696             mediaQualityStats:  
16697               type: string  
16698 RecMediaStartLogEvent:  
16699   allOf:  
16700     - $ref: '#/components/schemas/LogEvent'  
16701     - type: object  
16702       required:  
16703         - sdp  
16704         - mediaLabel  
16705       properties:  
16706         sdp:  
16707           type: string  
16708         mediaLabel:  
16709           type: array  
16710           items:  
16711             type: string  
16712         direction:  
16713           $ref: '#/components/schemas/Direction'  
16714         mediaTranscodeFrom:  
16715           type: string  
16716 RecMediaEndLogEvent:  
16717   allOf:  
16718     - $ref: '#/components/schemas/LogEvent'  
16719     - type: object  
16720       required:  
16721         - mediaLabel  
16722       properties:  
16723         mediaLabel:  
16724           type: array  
16725           items:  
16726             type: string  
16727             mediaQualityStats:
```

[MM/DD/YYYY]

Page 645 of 675



```
16728          type: string
16729      mediaTranscodeFrom:
16730          type: string
16731  RecordingFailedLogEvent:
16732      allOf:
16733          - $ref: '#/components/schemas/LogEvent'
16734          - type: object
16735              required:
16736                  - sdp
16737                  - reasonCode
16738                  - reasonText
16739          properties:
16740              sdp:
16741                  type: string
16742              reasonCode:
16743                  type: string
16744                  description: Values limited to those in the ReasonCode
16745      registry
16746          reasonText:
16747              type: string
16748  MessageLogEvent:
16749      allOf:
16750          - $ref: '#/components/schemas/LogEvent'
16751          - type: object
16752              required:
16753                  - text
16754                  - direction
16755          properties:
16756              text:
16757                  type: string
16758              direction:
16759                  $ref: '#/components/schemas/Direction'
16760  AdditionalAgencyLogEvent:
16761      allOf:
16762          - $ref: '#/components/schemas/LogEvent'
16763          - type: object
16764              required:
16765                  - agencyId
16766          properties:
16767              agencyId:
16768                  type: string
16769  IncidentMergeLogEvent:
16770      allOf:
16771          - $ref: '#/components/schemas/LogEvent'
```

[MM/DD/YYYY]

Page 646 of 675



```
16772      - type: object
16773      required:
16774          - incidentId
16775          - mergeIncidentId
16776      properties:
16777          incidentId:
16778              type: string
16779          mergeIncidentId:
16780              type: string
16781 IncidentUnMergeLogEvent:
16782      allOf:
16783          - $ref: '#/components/schemas/LogEvent'
16784          - type: object
16785      required:
16786          - incidentId
16787          - unmergedFromIncidentId
16788      properties:
16789          incidentId:
16790              type: string
16791          unmergedFromIncidentId:
16792              type: string
16793 IncidentLinkLogEvent:
16794      allOf:
16795          - $ref: '#/components/schemas/LogEvent'
16796          - type: object
16797      required:
16798          - incidentId
16799          - linkedIncidentId
16800          - relationship
16801      properties:
16802          incidentId:
16803              type: string
16804          linkedIncidentId:
16805              type: string
16806          relationship:
16807              type: string
16808              enum: [parent, child, unspecified]
16809 IncidentUnLinkLogEvent:
16810      allOf:
16811          - $ref: '#/components/schemas/LogEvent'
16812          - type: object
16813      required:
16814          - incidentId
16815          - unlinkedFromIncidentId
```

[MM/DD/YYYY]

Page 647 of 675



```
16816      properties:  
16817          incidentId:  
16818              type: string  
16819          unlinkedFromIncidentId:  
16820              type: string  
16821      IncidentClearLogEvent:  
16822          allOf:  
16823              - $ref: '#/components/schemas/LogEvent'  
16824      IncidentReopenLogEvent:  
16825          allOf:  
16826              - $ref: '#/components/schemas/LogEvent'  
16827      LostQueryLogEvent:  
16828          allOf:  
16829              - $ref: '#/components/schemas/LogEvent'  
16830              - type: object  
16831                  required:  
16832                      - queryAdapter  
16833                      - direction  
16834                      - queryId  
16835                  properties:  
16836                      queryAdapter:  
16837                          type: string  
16838                      direction:  
16839                          $ref: '#/components/schemas/Direction'  
16840                      queryId:  
16841                          type: string  
16842                      malformedQuery:  
16843                          type: string  
16844      LostResponseLogEvent:  
16845          allOf:  
16846              - $ref: '#/components/schemas/LogEvent'  
16847              - type: object  
16848                  required:  
16849                      - responseAdapter  
16850                      - direction  
16851                      - responseId  
16852                  properties:  
16853                      responseAdapter:  
16854                          type: string  
16855                      direction:  
16856                          $ref: '#/components/schemas/Direction'  
16857                      responseStatus:  
16858                          type: string  
16859                      responseId:
```

[MM/DD/YYYY]

Page 648 of 675



```
16860           type: string
16861       malformedResponse:
16862           type: string
16863   CallSignalingMessageLogEvent:
16864       allOf:
16865           - $ref: '#/components/schemas/LogEvent'
16866           - type: object
16867               required:
16868                   - text
16869                   - direction
16870               properties:
16871                   text:
16872                       type: string
16873                   direction:
16874                       $ref: '#/components/schemas/Direction'
16875               protocol:
16876                   type: string
16877   SipRecMetadataLogEvent:
16878       allOf:
16879           - $ref: '#/components/schemas/LogEvent'
16880           - type: object
16881               required:
16882                   - text
16883               properties:
16884                   text:
16885                       type: string
16886   NonRtpMediaMessageLogEvent:
16887       allOf:
16888           - $ref: '#/components/schemas/LogEvent'
16889           - type: object
16890               required:
16891                   - text
16892                   - direction
16893               properties:
16894                   text:
16895                       type: string
16896                   direction:
16897                       $ref: '#/components/schemas/Direction'
16898               protocol:
16899                   type: string
16900   AliLocationQueryLogEvent:
16901       allOf:
16902           - $ref: '#/components/schemas/LogEvent'
16903           - type: object
```

[MM/DD/YYYY]

Page 649 of 675



```
16904     required:
16905         - text
16906         - direction
16907         - queryId
16908     properties:
16909         text:
16910             type: string
16911         direction:
16912             $ref: '#/components/schemas/Direction'
16913         queryId:
16914             type: string
16915     AliLocationResponseLogEvent:
16916     allOf:
16917         - $ref: '#/components/schemas/LogEvent'
16918         - type: object
16919             required:
16920                 - text
16921                 - direction
16922                 - responseId
16923             properties:
16924                 text:
16925                     type: string
16926                 direction:
16927                     $ref: '#/components/schemas/Direction'
16928                 responseStatus:
16929                     type: string
16930                     description: Values limited to those in the Status Codes
16931     registry
16932         responseId:
16933             type: string
16934     MalformedMessageLogEvent:
16935     allOf:
16936         - $ref: '#/components/schemas/LogEvent'
16937         - type: object
16938             required:
16939                 - text
16940                 - ipAddress
16941             properties:
16942                 text:
16943                     type: string
16944                 ipAddress:
16945                     type: string
16946                 explanationText:
16947                     type: string
```

[MM/DD/YYYY]

Page 650 of 675



```
16948    IncidentSplitLogEvent:  
16949        allOf:  
16950            - $ref: '#/components/schemas/LogEvent'  
16951            - type: object  
16952                required:  
16953                    - incidentId  
16954                    - type  
16955                properties:  
16956                    incidentId:  
16957                        type: string  
16958                    type:  
16959                        type: string  
16960                        enum: [old, new]  
16961    EidoLogEvent:  
16962        allOf:  
16963            - $ref: '#/components/schemas/LogEvent'  
16964            - type: object  
16965                required:  
16966                    - direction  
16967                properties:  
16968                    body:  
16969                        type: string  
16970                    reference:  
16971                        type: string  
16972                    direction:  
16973                        $ref: '#/components/schemas/Direction'  
16974    DiscrepancyReportLogEvent:  
16975        allOf:  
16976            - $ref: '#/components/schemas/LogEvent'  
16977            - type: object  
16978                required:  
16979                    - contents  
16980                    - direction  
16981                    - type  
16982                properties:  
16983                    contents:  
16984                        type: string  
16985                    direction:  
16986                        $ref: '#/components/schemas/Direction'  
16987                    type:  
16988                        type: string  
16989    ElementStateChangeLogEvent:  
16990        allOf:  
16991            - $ref: '#/components/schemas/LogEvent'
```

[MM/DD/YYYY]

Page 651 of 675



```
16992      - type: object
16993      required:
16994          - notificationContents
16995          - direction
16996      properties:
16997          notificationContents:
16998              type: string
16999          affectedElementId:
17000              type: string
17001          direction:
17002              $ref: '#/components/schemas/Direction'
17003  ServiceStateChangeLogEvent:
17004      allOf:
17005          - $ref: '#/components/schemas/LogEvent'
17006          - type: object
17007          required:
17008              - newState
17009              - affectedServiceIdentifier
17010              - direction
17011          properties:
17012              newState:
17013                  type: string
17014              newSecurityPosture:
17015                  type: string
17016              affectedServiceIdentifier:
17017                  type: string
17018          direction:
17019              $ref: '#/components/schemas/Direction'
17020  AdditionalDataQueryLogEvent:
17021      allOf:
17022          - $ref: '#/components/schemas/LogEvent'
17023          - type: object
17024          required:
17025              - uri
17026              - text
17027              - direction
17028              - queryId
17029          properties:
17030              uri:
17031                  type: string
17032                  format: uri
17033              text:
17034                  type: string
17035          direction:
```

[MM/DD/YYYY]

Page 652 of 675



```
17036      $ref: '#/components/schemas/Direction'
17037      queryId:
17038          type: string
17039  AdditionalDataResponseLogEvent:
17040      allOf:
17041          - $ref: '#/components/schemas/LogEvent'
17042          - type: object
17043              required:
17044                  - text
17045                  - direction
17046                  - responseId
17047          properties:
17048              text:
17049                  type: string
17050              direction:
17051                  $ref: '#/components/schemas/Direction'
17052              responseStatus:
17053                  type: string
17054                  description: Values limited to those in the Status Codes
17055  registry
17056      responseId:
17057          type: string
17058  LocationQueryLogEvent:
17059      allOf:
17060          - $ref: '#/components/schemas/LogEvent'
17061          - type: object
17062              required:
17063                  - uri
17064                  - text
17065                  - direction
17066                  - queryId
17067          properties:
17068              uri:
17069                  type: string
17070                  format: uri
17071              text:
17072                  type: string
17073              direction:
17074                  $ref: '#/components/schemas/Direction'
17075              queryId:
17076                  type: string
17077  LocationResponseLogEvent:
17078      allOf:
17079          - $ref: '#/components/schemas/LogEvent'
```

[MM/DD/YYYY]

Page 653 of 675



```
17080      - type: object
17081          required:
17082              - text
17083              - direction
17084              - responseId
17085          properties:
17086              text:
17087                  type: string
17088              direction:
17089                  $ref: '#/components/schemas/Direction'
17090          responseStatus:
17091              type: string
17092              description: Values limited to those in the Status Codes
17093      registry
17094          responseId:
17095              type: string
17096      CallStateChangeEvent:
17097          allOf:
17098              - $ref: '#/components/schemas/LogEvent'
17099              - type: object
17100                  required:
17101                      - state
17102                      - direction
17103                      - legCallId
17104          properties:
17105              state:
17106                  type: string
17107                  description: Values limited to those in the CallStates
17108      registry
17109          direction:
17110              $ref: '#/components/schemas/Direction'
17111          legCallId:
17112              type: string
17113          targetId:
17114              type: string
17115          changeReason:
17116              type: string
17117      GatewayCallLogEvent:
17118          allOf:
17119              - $ref: '#/components/schemas/LogEvent'
17120              - type: object
17121                  properties:
17122                      portTrunkGroup:
17123                          type: string
```

[MM/DD/YYYY]

Page 654 of 675



```
17124    pAni:  
17125        type: integer  
17126        format: int32  
17127    digits:  
17128        type: string  
17129    direction:  
17130        $ref: '#/components/schemas/Direction'  
17131    signallingProtocol:  
17132        type: string  
17133    legacyCallId:  
17134        type: string  
17135    HookflashLogEvent:  
17136        allOf:  
17137            - $ref: '#/components/schemas/LogEvent'  
17138            - type: object  
17139                properties:  
17140                    lineId:  
17141                        type: string  
17142    LegacyDigitsLogEvent:  
17143        allOf:  
17144            - $ref: '#/components/schemas/LogEvent'  
17145            - type: object  
17146                required:  
17147                    - digits  
17148                    - sentReceived  
17149                    - type  
17150                properties:  
17151                    digits:  
17152                        type: string  
17153                sentReceived:  
17154                        type: string  
17155                        enum: [sent, received]  
17156                type:  
17157                        type: string  
17158                        enum: [DTMF, MF]  
17159    AgentStateChangeLogEvent:  
17160        allOf:  
17161            - $ref: '#/components/schemas/LogEvent'  
17162            - type: object  
17163                required:  
17164                    - primaryAgentState  
17165                properties:  
17166                    primaryAgentState:  
17167                        type: string
```

[MM/DD/YYYY]

Page 655 of 675



```
17168      enum: [Available, NotAvailable]
17169      secondaryAgentState:
17170          type: string
17171          description: Values limited to those in the Secondary Agent
17172      State registry
17173          deviceId:
17174              type: string
17175      QueueStateChangeLogEvent:
17176          allOf:
17177              - $ref: '#/components/schemas/LogEvent'
17178              - type: object
17179                  required:
17180                      - notificationContents
17181                      - queueId
17182                      - direction
17183                  properties:
17184                      notificationContents:
17185                          type: string
17186                      queueId:
17187                          type: string
17188                      direction:
17189                          $ref: '#/components/schemas/Direction'
17190      KeepAliveFailureLogEvent:
17191          allOf:
17192              - $ref: '#/components/schemas/LogEvent'
17193              - type: object
17194                  required:
17195                      - responseStatus
17196                  properties:
17197                      responseStatus:
17198                          type: string
17199                          description: Values limited to those in the Status Codes
17200      registry
17201          RouteRuleMsgLogEvent:
17202              allOf:
17203                  - $ref: '#/components/schemas/LogEvent'
17204                  - type: object
17205                      required:
17206                          - ruleId
17207                          - priority
17208                          - message
17209                          - policyOwner
17210                          - policyType
17211                  properties:
```

[MM/DD/YYYY]

Page 656 of 675



```
17212           ruleId:  
17213             type: string  
17214           priority:  
17215             type: integer  
17216             format: int32  
17217           message:  
17218             type: string  
17219           policyOwner:  
17220             type: string  
17221           policyType:  
17222             type: string  
17223             description: Values limited to those in the policyType  
17224       registry  
17225           policyQueueName:  
17226             type: string  
17227             format: uri  
17228           policyId:  
17229             type: string  
17230       PolicyChangeLogEvent:  
17231         allOf:  
17232           - $ref: '#/components/schemas/LogEvent'  
17233           - type: object  
17234             required:  
17235               - policyType  
17236               - owner  
17237               - changeType  
17238               - policyContent  
17239               - policyStoreId  
17240               - policyEditor  
17241         properties:  
17242           policyType:  
17243             type: string  
17244             description: Values limited to those in the policyType  
17245       registry  
17246           owner:  
17247             type: string  
17248           changeType:  
17249             type: string  
17250             enum: [CREATE, UPDATE, DELETE]  
17251           policyContent:  
17252             type: string  
17253           policyStoreId:  
17254             type: string  
17255           policyEditor:
```

[MM/DD/YYYY]

Page 657 of 675



```
17256          type: string
17257  policyQueueName:
17258      type: string
17259      format: uri
17260  policyId:
17261      type: string
17262 VersionsLogEvent:
17263  allOf:
17264      - $ref: '#/components/schemas/LogEvent'
17265      - type: object
17266          required:
17267              - source
17268              - response
17269          properties:
17270              source:
17271                  type: string
17272              response:
17273                  type: string
17274 SubscribeLogEvent:
17275  allOf:
17276      - $ref: '#/components/schemas/LogEvent'
17277      - type: object
17278          required:
17279              - package
17280              - peer
17281              - parameter
17282              - expiration
17283              - response
17284              - purpose
17285              - direction
17286              - subscriptionId
17287          properties:
17288              package:
17289                  type: string
17290                  description: Values limited to those in the Event Package
17291  registry
17292
17293      peer:
17294          type: string
17295      parameter:
17296          type: array
17297          items:
17298              type: object
17299          properties:
              type:
```

```
17300          type: string
17301          value:
17302          type: string
17303          expiration:
17304          type: integer
17305          format: int32
17306          response:
17307          type: string
17308          purpose:
17309          type: string
17310          enum: [initial, refresh, terminate]
17311          direction:
17312          $ref: '#/components/schemas/Direction'
17313          subscriptionId:
17314          type: string
17315 CallLogEvent:
17316          type: object
17317          required:
17318          - direction
17319          properties:
17320          direction:
17321          $ref: '#/components/schemas/Direction'
17322          standardPrimaryCallType:
17323          type: string
17324          description: Values limited to those in the LogEvent CallTypes
17325 registry
17326          standardSecondaryCallType:
17327          type: string
17328          description: Values limited to those in the LogEvent CallTypes
17329 registry
17330          localCallType:
17331          type: string
17332          localUse:
17333          type: object
17334          to:
17335          type: string
17336          from:
17337          type: string
17338          Direction:
17339          type: string
17340          enum: [incoming, outgoing]
```

17341 **E.8.2 Examples**

17342 **E.9 Bad Actor Service**

17343 **E.9.1 OpenAPI Interface Description**

```
17344     openapi: 3.0.1
17345     info:
17346         title: Bad Actor Service
17347         version: "1.0"
17348     servers:
17349         - url: http://localhost/BadActor/v1
17350     paths:
17351         /BadActors:
17352             post:
17353                 tags:
17354                     - BadActorRequest
17355                     summary: Identifies a source as a "Bad Actor"
17356                     operationId: BadActorRequest
17357                     requestBody:
17358                         description: Bad actor source Id
17359                         content:
17360                             application/json:
17361                                 schema:
17362                                     type: string
17363                                     required: true
17364                     responses:
17365                         '201':
17366                             description: Bad Actor successfully added
17367                         '401':
17368                             description: Unauthorized
17369                         '432':
17370                             description: Already reported
17371                         '433':
17372                             description: No such sourceId
17373                         '454':
17374                             description: Unspecified Error
17375         /Versions:
17376             servers:
17377                 - url: https://api.example.com/BadActor
17378                     description: Override base path for Versions query
17379             get:
17380                 tags:
```

[MM/DD/YYYY]

Page 660 of 675



```
17381      - RetrieveVersions
17382      summary: Retrieves all supported versions, vendor parameter is
17383      optional.
17384          operationId: RetrieveVersions
17385          responses:
17386              '200':
17387                  description: Versions found
17388                  content:
17389                      application/json:
17390                          schema:
17391                              $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
17392
```

17393 **E.10 Service/Agency Locator Service**

17394 **E.10.1 OpenAPI Interface Description**

```
17395     openapi: 3.0.1
17396     info:
17397         title: Service/Agency Locator
17398         version: "1.0"
17399     servers:
17400         - url: http://localhost/ServiceAgencyLocator/v1
17401     paths:
17402         /LocatorRecordUris:
17403             get:
17404                 tags:
17405                     - SearchByName
17406                 summary: Retrieves Service/Agency Locator Records URIs
17407                 operationId: SearchByName
17408                 parameters:
17409                     - name: limit
17410                         in: query
17411                         description: Maximum number of results to return
17412                         required: false
17413                         schema:
17414                             type: integer
17415                             format: int32
17416                     - name: start
17417                         in: query
17418                         description: First item in the page of results, as an ordinal 1-
17419                         based integer
17420                         required: false
17421                         schema:
```

[MM/DD/YYYY]

Page 661 of 675



```
17422          type: integer
17423          format: int32
17424          minimum: 1
17425          - name: serviceAgencyName
17426          in: query
17427          description: Name of the Service or Agency, wildcards can be
17428      used
17429          required: true
17430          schema:
17431          type: string
17432      responses:
17433      '200':
17434          description: URIs found
17435          content:
17436          application/json:
17437          schema:
17438          $ref: '#/components/schemas/LocatorRecordUriArray'
17439      '404':
17440          description: Not found
17441      '454':
17442          description: Unspecified Error
17443 /NameSets:
17444     get:
17445     tags:
17446     - InterESInetSearchIndex
17447     summary: Retrieves Service/Agency names the Locator is aware of
17448     operationId: InterESInetSearchIndex
17449     parameters:
17450     - name: limit
17451         in: query
17452         description: Maximum number of results to return
17453         required: false
17454         schema:
17455         type: integer
17456         format: int32
17457     - name: start
17458         in: query
17459         description: First item in the page of results, as an ordinal 1-
17460         based integer
17461         required: false
17462         schema:
17463         type: integer
17464         format: int32
17465         minimum: 1
```

[MM/DD/YYYY]

Page 662 of 675



```
17466      responses:
17467        '200':
17468          description: Namesets found
17469          content:
17470            application/json:
17471              schema:
17472                $ref: '#/components/schemas/NameSetArray'
17473        '404':
17474          description: Not found
17475        '411':
17476          description: Index beyond available names
17477        '454':
17478          description: Unspecified Error
17479    /Versions:
17480      servers:
17481        - url: https://api.example.com/ServiceAgencyLocator
17482          description: Override base path for Versions query
17483    get:
17484      tags:
17485        - RetrieveVersions
17486      summary: Retrieves all supported versions, vendor parameter is
17487 optional.
17488      operationId: RetrieveVersions
17489      responses:
17490        '200':
17491          description: Versions found
17492          content:
17493            application/json:
17494              schema:
17495                $ref: 'i3-common.yaml#/components/schemas/VersionsArray'
17496  components:
17497    schemas:
17498      LocatorRecordUriArray:
17499        type: object
17500        required:
17501          - count
17502          - totalCount
17503          - locatorUris
17504        properties:
17505          count:
17506            type: integer
17507            format: int32
17508            description: Number of items in the array
17509          totalCount:
```

[MM/DD/YYYY]

Page 663 of 675



```
17510      type: integer
17511      format: int32
17512      description: Total number of items found
17513  locatorUris:
17514      type: array
17515      items:
17516          $ref: '#/components/schemas/LocatorRecordUri'
17517      description: Array of Locator URI objects
17518  NameSetArray:
17519      type: object
17520      required:
17521          - count
17522          - totalCount
17523          - nameSets
17524  properties:
17525      count:
17526          type: integer
17527          format: int32
17528          description: Number of items in the array
17529  totalCount:
17530      type: integer
17531      format: int32
17532      description: Total number of items found
17533  nameSets:
17534      type: array
17535      items:
17536          $ref: '#/components/schemas/NameSet'
17537      description: Array of Name Sets objects
17538  LocatorRecordUri:
17539      type: object
17540      required:
17541          - locatorRecordUri
17542          - serviceAgencyName
17543          - uriType
17544  properties:
17545      uri:
17546          type: string
17547          format: uri
17548  serviceAgencyName:
17549      type: string
17550  uriType:
17551      type: string
17552      enum: [RecordUri, ReferralUri]
17553  LocatorRecord:
```

[MM/DD/YYYY]

Page 664 of 675



```
17554 type: object
17555 required:
17556   - recordId
17557   - serviceAgencyId
17558   - serviceAgencyName
17559   - serviceAgencyJcard
17560   - serviceAgencyTypes
17561   - loggerUri
17562 properties:
17563   recordId:
17564     type: string
17565   serviceAgencyId:
17566     type: string
17567   serviceAgencyName:
17568     type: string
17569   serviceAgencyJcard:
17570     type: string
17571   serviceAgencyTypes:
17572     type: array
17573     minItems: 1
17574     items:
17575       type: string
17576   emergencySipInterfaceUri:
17577     type: string
17578     format: uri
17579   adminLineUri:
17580     type: string
17581     format: uri
17582   loggerUri:
17583     type: string
17584     format: uri
17585   eidoInterfaceUri:
17586     type: string
17587     format: uri
17588   mdsFeatureInterfaceUri:
17589     type: string
17590     format: uri
17591   mdsImageInterfaceUri:
17592     type: string
17593     format: uri
17594   svcStateUri:
17595     type: string
17596     format: uri
17597   dscRptUri:
```

[MM/DD/YYYY]

Page 665 of 675



```
17598      type: string
17599      format: uri
17600      headJcard:
17601          type: string
17602      onDutySuperJcard:
17603          type: string
17604      NameSet:
17605          type: object
17606          properties:
17607              locatorUri:
17608                  type: string
17609                  format: uri
17610              names:
17611                  type: array
17612                  items:
17613                      type: string
```

17614 **E.11 Notify Bodies**

17615 **E.11.1 ESRP NOTIFY Notify Body**

17616 **E.11.1.1 JSON Schema**

```
17617  {
17618      "$schema": "http://json-schema.org/draft-04/schema#",
17619      "version": "1.0",
17620      "title": "ESRP Notify NOTIFY",
17621      "description": "SIP NOTIFY message body for ESRP Notify notifications",
17622      "type": "object",
17623      "properties": {
17624          "esrpNotify": {
17625              "type": "object",
17626              "properties": {
17627                  "queueUri": {
17628                      "type": "string"
17629                  },
17630                  "eventCode": {
17631                      "type": "string"
17632                  },
17633                  "urgency": {
17634                      "type": "integer"
17635                  },
17636                  "comment": {
```

[MM/DD/YYYY]

Page 666 of 675



```
17637          "type": "string"
17638      },
17639      "callLocation": {
17640          "type": "string"
17641      },
17642      "additionalData": {
17643          "type": "string"
17644      },
17645      "esrpRule": {
17646          "type": "string"
17647      }
17648  },
17649  "required": [
17650      "queueUri",
17651      "eventCode",
17652      "urgency",
17653      "callLocation",
17654      "esrpRule"
17655  ]
17656 }
17657 },
17658  "required": [
17659      "esrpNotify"
17660  ]
17661 }
```

17662 **E.11.1.2 Gap-Overlap Notify Body**

17663 **E.11.1.3 JSON Schema**

```
17664  {
17665      "$schema": "http://json-schema.org/draft-04/schema#",
17666      "version": "1.0",
17667      "title": "Gap Overlap NOTIFY",
17668      "description": "SIP NOTIFY message body for Gap Overlap notifications",
17669      "type": "object",
17670      "properties": {
17671          "gapOverlap": {
17672              "type": "object",
17673              "properties": {
17674                  "agencies": {
17675                      "type": "array",
17676                      "items": {
17677                          "type": "string"
```

[MM/DD/YYYY]

Page 667 of 675



```
17678        }
17679    },
17680    "layers": {
17681        "type": "array",
17682        "items": {
17683            "type": "string"
17684        }
17685    },
17686    "gap": {
17687        "type": "boolean"
17688    },
17689    "dateTime": {
17690        "type": "string"
17691    },
17692    "area": {
17693        "type": "string"
17694    }
17695 },
17696 "required": [
17697     "agencies",
17698     "layers",
17699     "gap",
17700     "dateTime",
17701     "area"
17702     ]
17703   }
17704 },
17705 "required": [
17706     "gapOverlap"
17707   ]
17708 }
```

17709 **E.11.2 Abandoned Call Notify Body**

17710 **E.11.2.1 JSON Schema**

```
17711 {
17712     "$schema": "http://json-schema.org/draft-04/schema#",
17713     "version": "1.0",
17714     "title": "Abandoned Call NOTIFY",
17715     "description": "SIP NOTIFY message body for Abandoned Call
17716     notifications",
17717     "type": "object",
17718     "properties": {
```

[MM/DD/YYYY]

Page 668 of 675



```
17719     "abandonedCall": {  
17720         "type": "object",  
17721         "properties": {  
17722             "invite": {  
17723                 "type": "string"  
17724             },  
17725             "inviteTimestamp": {  
17726                 "type": "string"  
17727             },  
17728             "cancelTimestamp": {  
17729                 "type": "string"  
17730             }  
17731         },  
17732         "required": [  
17733             "invite",  
17734             "inviteTimestamp",  
17735             "cancelTimestamp"  
17736         ]  
17737     }  
17738 },  
17739     "required": [  
17740         "abandonedCall"  
17741     ]  
17742 }
```

17743 **E.11.3 Element State Notify Body**

17744 **E.11.3.1 JSON Schema**

```
17745 {  
17746     "$schema": "http://json-schema.org/draft-04/schema#",  
17747     "version": "1.0",  
17748     "title": "Element State NOTIFY",  
17749     "description": "SIP NOTIFY message body for Element State  
17750     notifications",  
17751     "type": "object",  
17752     "properties": {  
17753         "elementState": {  
17754             "type": "object",  
17755             "properties": {  
17756                 "elementDomain": {  
17757                     "type": "string"  
17758                 },  
17759                 "state": {
```

[MM/DD/YYYY]

Page 669 of 675



```
17760          "type": "string"
17761      },
17762      "reason": {
17763          "type": "string"
17764      }
17765  },
17766  "required": [
17767      "elementDomain",
17768      "state",
17769      "reason"
17770  ]
17771 }
17772 },
17773 "required": [
17774     "elementState"
17775 ]
17776 }
```

17777 **E.11.3.2 Queue State Notify Body**

17778 **E.11.3.3 JSON Schema**

```
17779 {
17780     "$$schema": "http://json-schema.org/draft-04/schema#",
17781     "version": "1.0",
17782     "title": "Queue State NOTIFY",
17783     "description": "SIP NOTIFY message body for Queue State notifications",
17784     "type": "object",
17785     "properties": {
17786         "queueState": {
17787             "type": "object",
17788             "properties": {
17789                 "queueUri": {
17790                     "type": "string"
17791                 },
17792                 "queueLength": {
17793                     "type": "number"
17794                 },
17795                 "queueMaxLength": {
17796                     "type": "integer"
17797                 },
17798                 "state": {
17799                     "type": "string"
17800                 }
17801             }
17802         }
17803     }
17804 }
```

[MM/DD/YYYY]

Page 670 of 675



```
17801      },
17802      "required": [
17803          "queueUri",
17804          "queueLength",
17805          "queueMaxLength",
17806          "state"
17807      ]
17808  }
17809 },
17810 "required": [
17811     "queueState"
17812 ]
17813 {
```

17814 **E.11.3.4 Service State Notify Body**

17815 **E.11.3.5 JSON Schema**

```
17816 {
17817     "$schema": "http://json-schema.org/draft-04/schema#",
17818     "version": "1.0",
17819     "title": "Service State NOTIFY",
17820     "description": "SIP NOTIFY message body for Service State
17821 notifications",
17822     "type": "object",
17823     "properties": {
17824         "service": {
17825             "type": "object",
17826             "properties": {
17827                 "name": {
17828                     "type": "string"
17829                 },
17830                 "domain": {
17831                     "type": "string"
17832                 }
17833             },
17834             "required": [
17835                 "name",
17836                 "domain"
17837             ]
17838         },
17839         "serviceState": {
17840             "type": "object",
17841             "properties": {
```

[MM/DD/YYYY]

Page 671 of 675



```
17842         "state": {
17843             "type": "string"
17844         },
17845         "reason": {
17846             "type": "string"
17847         }
17848     },
17849     "required": [
17850         "state",
17851         "reason"
17852     ]
17853 },
17854 "securityPosture": {
17855     "type": "object",
17856     "properties": {
17857         "posture": {
17858             "type": "string"
17859         },
17860         "reason": {
17861             "type": "string"
17862         }
17863     },
17864     "required": [
17865         "posture",
17866         "reason"
17867     ]
17868 },
17869 },
17870 "required": [
17871     "service",
17872     "serviceState"
17873 ]
17874 }
```

17875 **E.11.4 Common YAML**

17876 **E.11.4.1 OpenAPI Interface Description**

```
17877 components:
17878     schemas:
17879         VersionsArray:
17880             type: object
17881             required:
17882                 - versions
```

[MM/DD/YYYY]

Page 672 of 675



```
17883     properties:  
17884         versions:  
17885             type: array  
17886             items:  
17887                 type: object  
17888                 required:  
17889                     - major  
17890                     - minor  
17891             properties:  
17892                 major:  
17893                     type: integer  
17894                     format: int32  
17895                     description: Version major number  
17896                 minor:  
17897                     type: integer  
17898                     format: int32  
17899                     description: Version minor number  
17900             vendor:  
17901                 type: string  
17902                 description: Vendor extension of the version  
17903             serviceInfo:  
17904                 type: object  
17905                 properties:  
17906                     requiredAlgorithms:  
17907                         type: array  
17908                         items:  
17909                             type: string  
17910                             enum: [EdDSA, none]  
17911                             description: alg Header Parameter Values for JWS  
17912             fingerprint:  
17913                 type: string  
17914                 description: Vendor info  
17915             ConditionType:  
17916                 type: string  
17917                 enum: [TimePeriodCondition, SipHeaderCondition,  
17918                     AdditionalDataCondition, MimeBodyCondition, LocationCondition,  
17919                     CallSuspicionCondition, SecurityPostureCondition,  
17920                     QueueStateCondition, LostServiceUrnCondition,  
17921                     ServiceStateCondition, CallSourceCondition, BodyPartCondition,  
17922                     RequestUriCondition,  
17923                         NormalNextHopCondition, IncomingQueueCondition,  
17924                     SdpOfferCondition, CapCondition, CallingNumberVerificationStatusCondition]  
17925             Jws:  
17926                 type: object
```

[MM/DD/YYYY]

Page 673 of 675



```
17927 required:  
17928     - payload  
17929     - protected  
17930     - signature  
17931 properties:  
17932     payload:  
17933         type: string  
17934         format: byte  
17935     protected:  
17936         type: string  
17937         format: byte  
17938     signature:  
17939         type: string  
17940         format: byte
```

17941 Acknowledgements

17942 The National Emergency Number Association (NENA) 9-1-1 Core Services Committee, i3
17943 Architecture Working Group developed this document.

17944 NENA Board of Directors Approval Date: [MM/DD/YYYY] (Will be added by the CRM.)

17945 NENA recognizes the following industry experts and their employers for their contributions to the
17946 development of this document.

Members	Employer
Steve O'Conor, ENP, 911 Core Services Committee Co-Chair, Working Group Co-Chair	Next Generation 9-1-1 Consulting Services, LLC
Terry Reese, 911 Core Services Committee Co-Chair	Ericsson
Brian Rosen, Working Group Co-Chair	Brian Rosen Technologies LLC
Dan Banks	Digital Data Technologies, Inc.
Marc Berryman, ENP	Mission Critical Partners
Daniel Biage	Solacom Technologies, Inc.
Guy Caron	Bell Canada
Jerry Eisner, ENP	RedSky Technologies
Simon Farrow	Stancil Corporation
Randall Gellens	Core Technology Consulting
Daniel Hagan	Hagan Consulting, Inc.
Jason Horning, ENP	North Dakota Association of Counties
Rafal Kaminski	Motorola Solutions, Inc.
James Kinney	INdigital Telecom

[MM/DD/YYYY]

Page 674 of 675



Members	Employer
Roger Marshall	Comtech Telecommunications Corp.
Dan Mongrain	Motorola Solutions, Inc.
Darrin Morkunas	Intrado, Inc.
Philip Reichl	INdigital Telecom
Matthew Serra, ENP	Rave Mobile Safety
Brooks Shannon	RapidDeploy
Jim Shepard, ENP	911 Datamaster
Bob Sherry, ENP	West Safety Services
Michael Smith	Equature/DSS Corp.
Henry Unger	Pulsiam
Jeffrey Wheeler	Data Technical Services

17947 **Special Acknowledgements:**

17948 Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document
17949 through the prescribed approval process.

17950 The i3 Architecture Working Group is part of the NENA Development Group that is led by:
17951 • Jim Shepard, ENP, and Wendi Rooney, ENP, Development Steering Council Co-Chairs
17952 • Roger Hixson, ENP, 9-1-1 Services Senior Consultant
17953 • Brandon Abley, Technical Issues Director
17954 • April Heinze, Operational Issues Director

[MM/DD/YYYY]

Page 675 of 675

