Scenario #2(Manual Transfer & Conference)

[**1 Scenario Description**](#_jhk1o5nzsgs1) **1**

[1.1 Test Bench retool](#_hkmq8z9m0du0) 2

[**2 Prerequisites**](#_l7xm3kdv4629) **3**

[2.1 Location(s) & Layers](#_s0hixgsdub22) 3

[2.1.1 ECRF Layers](#_7c4l71oyqtr7) 3

[2.1.2 IMS Locations used](#_1uhswgwbjguj) 4

[2.2.1 Static County ECRF Mapping & LDB/LNG Interworking](#_synxet7l9cg) 4

[2.2.1.1 Device Based](#_9ocad4y5iqjt) 4

[2.2.2 ECRF County Layer to URI mappings.](#_bcyyi8u8pcq5) 5

[2.3 Configure for loggers & recorders](#_73c1v3fh6ztf) 5

[**3 Detailed Steps**](#_z6l84uoyu434) **6**

[3.1 SIP](#_a5fljmxwnopy) 6

# 1 Scenario Description

Standard i3 call where a different agency better serves the location of the incident than where the call was delivered. Also known as a misroute, this scenario's goal is to manually select the correct agency and transfer the media sessions to them.

This call will come from the OSP/LNG into the iBCF position of the test bench. The iBCF will forward the call to the appropriate ESRP. The ESRP will use the provided geolocation information, received by-value or by-reference, to query the configured ECRF w/URN of sos using the findService method. The returned URI will route the call to the appropriate Emergency Queue for the location provided. This ESRPs Queue processing will forward to the appropriate URI pointing to the eBCF and subsequently the CHE used by the current answering agency.

The Called Agent answering the initial queue to which the call was routed will verify the proper connectivity for the media used. At this time the Original Queue CHFE will simulate a misrouted or other transfer/conference call that needs to have another agency involved.

The agency used for the transfer-to-agency is based on the random test run plan generated for ICE 10. These URIs can be preprogrammed into the CHFE or typed in during the test run. This scenario is a Manual operation to point to where the transfer or conference is needed.

## 1.1 Test Bench retool

1. OSPs point to iBCF
2. iBCFs point to ESRP
3. Between subsequent test runs the lab is retooled at the ECRF in test by changing the URI for which the appropriate location routes.
4. ESRP Queue points to eBCF/CHFE

# 2 Prerequisites

1. SBCs and iBCFs are pointed to the appropriate ESRPs in test.
2. ECRF(s) in test have been pre-provisioned with the proper URIs pointing to the queue used for the CHE in test.
3. CAD systems have pre-subscribed to CHE in test.
4. ESRPs have the required Queues and URIs pointed to the appropriate eBCFs.
5. eBCF is pointed to the appropriate CHE in test.

## 2.1 Location(s) & Layers

The following location information will be used to route calls to the appropriate PSAP for each test run. Calls made from IL addresses will force the ECRF in the test to either redirect or recurse to the FG. FG will either forward or redirect to the ecrf.il.ng911test.iit.edu for the PSAP URI pointed to by the location.

See the ICE 10 Location spreadsheet for details, currently at ***[Redacted link, see document provided in package]***

### 2.1.1 ECRF Layers

We will have two regions. The first region will be used to exercise all ECRF vendors during the event. These ECRFs are authoritative for KS, WA, NJ, and TX. These ECRFs will resolve locations provided by the OSPs to specific CHEs using the mapping/retoolings(s) detailed in later sections of this document. These retoolings are used to point the different locations to each OSP, routing to different CHEs during the tests.

The second region will be used to exercise the Forest Guide. When a request for IL location is received by an ECRF provisioned with Region 1 boundaries, they will not have coverage for IL. They will need to redirect or recurse to the FG. The FG will either return a location or redirect to the ECRF for region #2.

1. **Regional #1 ECRFs** -
   1. **States** - Combination of KS, WA, NJ, and TX only
2. **Regional #2 ECRF** -
   1. **States** - IL
3. **Forest Guide ECRP** -

### 2.1.2 IMS Locations used

* [Redacted]
  + **C1\_OSP1\_WA** -

A2: KING

1759 135TH PL NE

BELLEVUE WA 98005

* + **C2\_OSP1\_KS** -

A2: JOHNSON

6220 SPRINT PKWY

OVERLAND PARK KS 66251

* [Redacted]
  + **C1\_OSP2\_NJ** -   
    A2: SOMERSET  
    180 WASHINGTON VALLEY RD  
    BEDMINSTER NJ 07921
  + **C2\_OSP2\_TX** -   
    A2: TARRANT  
    1600 SOLANA BLVD  
    WESTLAKE TX 76262
  + **C3\_OSP2\_TX** -A2: DALLAS  
    700 HIDDEN RIDGE  
    IRVING TX 75038

### 2.2.1 Static County ECRF Mapping & LDB/LNG Interworking

We will assign static civic locations to Device Identifiers using tel: and sip schema URIs in each vendor’s LIS for interworking with Held.

#### 2.2.1.1 Device Based

Using RFC-6155 Device Identifier tel: URIs that mimic an ESRK are used.

The following location mappings are to be made in all ECRFs and LISs.

**Note** - Depending on the vendor’s solution an equivalent model may be used such as a pattern URL for Held.

***[Redacted due to Confidentiality Code of Conduct]***

### 2.2.2 ECRF County Layer to URI mappings.

Each ECRF vendor will be assigned an authoritative boundary set. They will configure this in their ECRF and send all other out of area queries to the FG.

**Note** - See ECRF and FG Location Guide for ECRF County Mapping toolings used throughout the event.

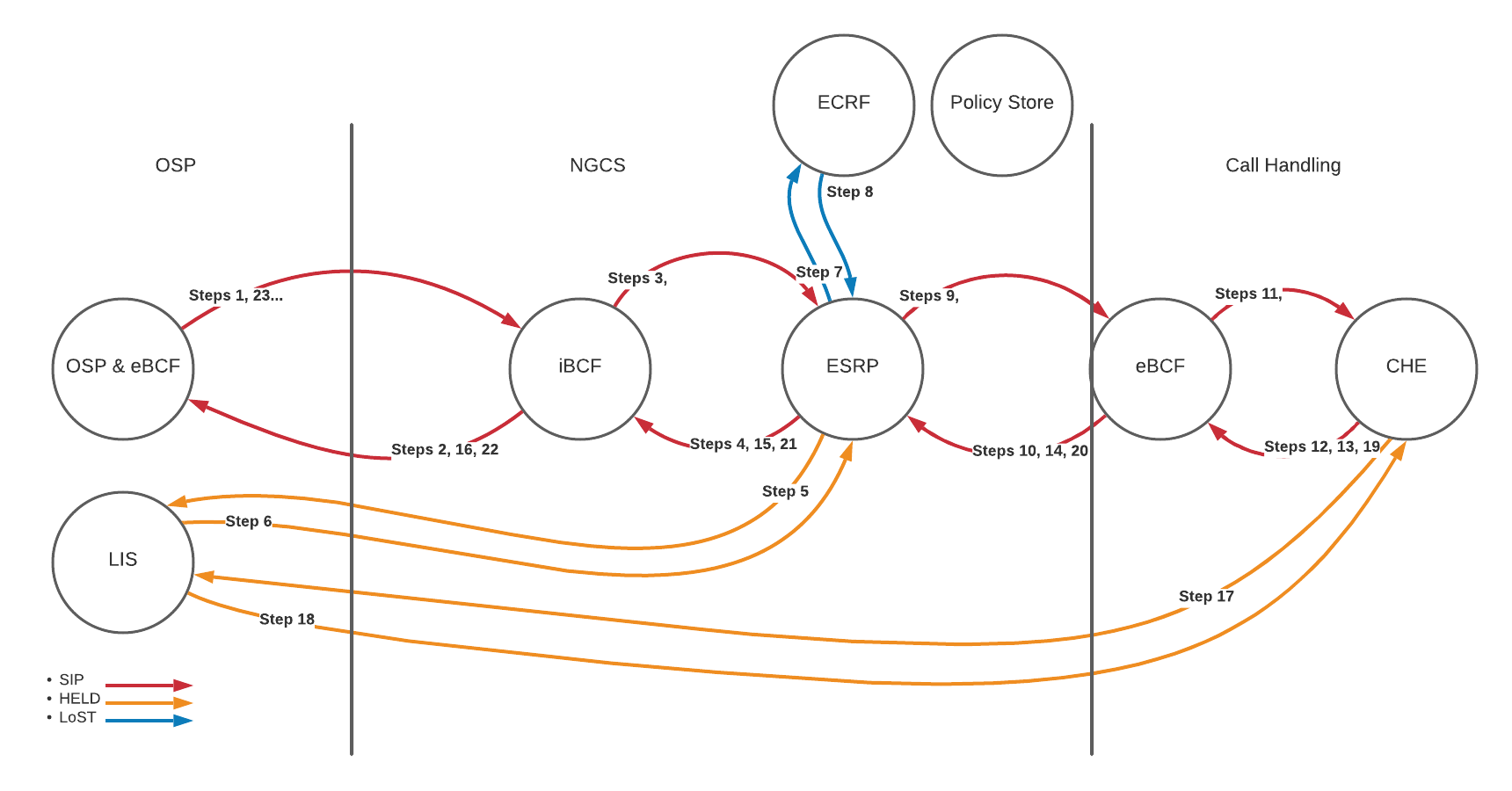
## 2.3 Configure for loggers & recorders

***[Redacted due to Confidentiality Code of Conduct]***

# 3 Detailed Steps

## 3.1 SIP, Held and LoST

1. INVITE(1) from OSP(BCF) to NGCS(iBCF)
2. 100 Trying from NGCS(iBCF) to OSP(BCF)
3. INVITE(2) from iBCF to ESRP
4. 100 Trying from ESRP to iBCF
5. NGCS(ESRP) queries OSP(LIS) for “emergencyRouting” using Held
6. OSP(LIS) returns PIDF-Lo to NGCS(ESRP) in Held Response
7. ESRP queriesECRF using LoST’s findService and urn:service:sos.
8. ECRF returns a findServiceResponse with queue URI to ESRP.
9. INVITE(3) to eBCF from ESRP
10. 100 Trying from eBCF to(ESRP)
11. INVITE(4) from NGCS(eBCF) to Call Handling(CHE)
    1. If there is an is-focus tag the CHE then
       1. SUBSCRIBE to Conference Event Package from CHE to Contact in INVITE(4).
12. 100 Trying from Call Handling(CHE) to NGCS(eBCF)
13. 18X from Call Handling(CHE) to NGCS(eBCF)
14. 18X from NGCS(eBCF) to ESRP
15. 18X from ESRP to NGCS(iBCF)
16. 18x from NGCS(iBCF) to OSP(BCF)
17. CHE queries OSP(LIS) for “emergencyDispatch” using Held
18. OSP(LIS) returns PIDF-Lo to Call Handling(CHE) in Held Response
19. Eventually, the agent answers and CHE sends 200 OK(4) to NGCS(eBCF)
    1. At this point, EIDO Conveyance NOTIFY(Step #2) is performed.
20. 200 OK(3) from NGCS(eBCF) to ESRP
21. 200 OK(2) from ESRP to NGCS(iBCF)
22. 200 OK(1) from NGCS(iBCF) to OSP(BCF)
23. ACK…
24. **LoST** - PSAP queries ECRF(listServicesByLocation) with Dispatch Location obtained in 18 and Service URN in urn:emergency:service:responder tree to obtain transfer target URI (we need to configure ECRF accordingly to return other CHS URI)
25. **LoST** -ECRF returns mapping for given location and Service URN
26. **Ad Hoc** - If NGCS conference model is ad hoc
    1. PSAP sends INVITE to Conference Factory
    2. Conference Factory returns 302 Moved Temporarily with Contact specifying conference URI to be used
    3. PSAP moves call with 9-1-1 caller to conference URI using re-INVITE
27. PSAP sends REFER to conference controller with Refer-To header specifying the following:
    1. SIP URI of transfer target (as obtained in step 25
    2. A parameter with Method=Call-Info specifying HTTP(S) URI with parameter purpose=emergency-eido specifying where transfer target is to retrieve EIDO for 9-1-1 call and Incident data
    3. A “serviceurn” parameter specifying the Service URN used to query the ECRF
28. Conference controller sends INVITE to transfer target with the following:
    1. Request URI is the Service URN specified in the Refer-To header
    2. Call-Info header with HTTP(S) URI specified in the Refer-To header along with parameter purpose=emergency-eido
    3. Route header specifying the SIP URI specified in the Refer-To header
29. Transfer target returns 200 OK to answer call
30. Conference controller returns ACK
31. (This may occur at INVITE reception time prior to call being answered) Target PSAP establishes TCP (and TLS if HTTPS URI) connection with server specified in URI received in Call-Info header with purpose=emergency-eido
32. Target PSAP sends a GET request with Accept header specifying application/emergency.eido+json and acceptable versions
33. EIDO server returns a 200 OK with a valid EIDO JSON structure in the body, which contains all of the details found in the INVITE received in step 11 above (Call Data Component with contents of Geolocation headers, contents of Call-Info headers with purpose=EmergencyCallData.xxx, Call Identifier, Callback information, etc.)



***[Major Sections Redacted due to Confidentiality Code of Conduct]***