Network Working Group
Request for Comments: 3603
Category: Informational

W. Marshall, Ed.
AT&T
F. Andreasen, Ed.
Cisco
October 2003

Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture

Status of this Memo

Copyright Notice

Abstract

In order to deploy a residential telephone service at very large scale across different domains, it is necessary for trusted elements owned by different service providers to exchange trusted information that conveys customer-specific information and expectations about the parties involved in the call. This document describes private extensions to the Session Initiation Protocol (SIP) (RFC3261) for supporting the exchange of customer information and billing information between trusted entities in the PacketCable Distributed Call Signaling Architecture. These extensions provide mechanisms for access network coordination to prevent theft of service, customer originated trace of harassing calls, support for operator services and emergency services, and support for various other regulatory issues. The use of the extensions is only applicable within closed administrative domains, or among federations of administrative domains with previously agreed-upon policies where coordination of charging and other functions is required.

Table of Contents

1. Applicability Statement

The SIP extensions described in this document make certain assumptions regarding network topology, linkage between SIP and lower layers, and the availability of transitive trust. These assumptions are generally not applicable in the Internet as a whole. The use of these headers is only applicable within closed administrative domains, or among federations of administrative domains with previously agreed-upon policies where coordination of charging and other functions is required, as in for example the architecture presented in [6]. Use outside such a domain could result in the leakage of potentially sensitive or private information. User consent to the privacy implications of the policies in [6] is strongly encouraged in those domains as well.

Although RFC 2119 language is used in this document, the scope of the normative language is only for the area of applicability of the document and, like the technology, it does not apply to the general Internet.

2. Introduction

In order to deploy a SIP-based [2] residential telephone service at very large scale across different domains, it is necessary for trusted elements owned by different service providers to exchange trusted information that conveys billing information and expectations about the parties involved in the call.

There are many billing models used in deriving revenue from telephony services today. Charging for telephony services is tightly coupled to the use of network resources. It is outside the scope of this document to discuss the details of these numerous and varying methods.

A key motivating principle of the DCS architecture described in [6] is the need for network service providers to be able to control and monitor network resources; revenue may be derived from the usage of these resources as well as from the delivery of enhanced services such as telephony. Furthermore, the DCS architecture recognizes the need for coordination between call signaling and resource management. This coordination ensures that users are authenticated and authorized before receiving access to network resources and billable enhanced services.

DCS Proxies, as defined in [6], have access to subscriber information and act as policy decision points and trusted intermediaries along the call signaling path. Edge routers provide the network connectivity and resource policy enforcement mechanism and also capture and report network connectivity and resource usage information. Edge routers need to be given billing information that can be logged with Record Keeping or Billing servers. The DCS Proxy, as a central point of coordination between call signaling and resource management, can provide this information based on the authenticated identity of the calling and called parties. Since there is a trust relationship among DCS Proxies, they can be relied upon to exchange trusted billing information pertaining to the parties involved in a call. See [6] for a description of the trust boundary and trusted versus untrusted entities.

For these reasons, it is appropriate to consider defining SIP header extensions to allow DCS Proxies to exchange information during call setup. It is the intent that the extensions would only appear on trusted network segments, should be inserted upon entering a trusted network region, and removed before leaving trusted network segments.

Significant amounts of information is retrieved by an originating DCS Proxy in its handling of a connection setup request from a user agent. Such information includes location information about the subscriber (essential for emergency services calls), billing information, and station information (e.g., coin operated phone). In addition, while translating the destination number, information such as the local-number-portability office code is obtained and will be needed by all other proxies handling this call.

For Usage Accounting records, it is necessary to have an identifier that can be associated with all the event records produced for the call. The SIP Call-ID header field cannot be used as such an identifier since it is selected by the originating user agent, and may not be unique among all past calls as well as current calls. Further, since this identifier is to be used by the service provider, it should be chosen in a manner and in a format that meets the service provider's needs.

Billing information may not necessarily be unique for each user (consider the case of calls from an office all billed to the same account). Billing information may not necessarily be identical for all calls made by a single user (consider prepaid calls, credit card calls, collect calls, etc). It is therefore necessary to carry billing information separate from the calling and called party identification. Furthermore, some billing models call for split-charging where multiple entities are billed for portions of the call.

The addition of a SIP General Header Field allows for the capture of billing information and billing identification for the duration of the call.

It is the intent that the billing extensions would only appear on trusted network segments, and MAY be inserted by a DCS Proxy in INVITE and REFER requests and INVITE responses in a trusted network segment, and removed before leaving trusted network segments.

In addition to support for billing, current residential telephone service includes the need for customer originated trace (of harassing or obscene calls), for operator services such as busy line verification and emergency interrupt (initiated by an operator from an Operator Services Position System (OSPS)), for emergency services such as 9-1-1 calls to a Public Service Access Point (PSAP) and the subsequent call handling, and support for Electronic Surveillance and Law Enforcement access as required by applicable legislation and court orders. In all of these cases, additional information about the call and about the subscribers involved in the call needs to be exchanged between the proxies.

3. Trust Boundary

The DCS architecture [6] defines a trust boundary around the various systems and servers that are owned, operated by, and/or controlled by the service provider. These trusted systems include the proxies and various servers such as bridge servers, voicemail servers, announcement servers, etc. Outside of the trust boundary lie the customer premises equipment, and various application and media servers operated by third-party service providers.

Certain subscriber-specific information, such as billing and accounting information, stays within the trust boundary. Other subscriber-specific information, such as endpoint identity, may be presented to untrusted endpoints or may be withheld based on subscriber profiles.

The User Agent (UA) may be either within the trust boundary or outside the trust boundary, depending on exactly what function is being performed and exactly how it is being performed. Accordingly, the procedures followed by a User Agent are different depending on whether the UA is within the trust boundary or outside the trust boundary.

The following sections giving procedures for User Agents therefore are subdivided into trusted user agents and untrusted user agents.

4. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

The term "private-URL" used in this document refers to a SIP URI that is generated by a proxy, contains a "hostport" that identifies the proxy, and contains a "userinfo" string that is generated by the proxy. The "userinfo" typically contains (or points to) information that is not to be disclosed outside the trusted domain of the proxies, such as billing account numbers, electronic surveillance indication, electronic surveillance parameters, and call redirection information. Consequently, the information is either stored locally by the proxy, or encrypted with a private key known only to the proxy and encoded in a character string in the "userinfo" portion of the URL. A checksum is included in the "userinfo" data to detect tampering. The mechanism by which a proxy recognizes a "userinfo" as a private-URL and decodes and recovers the original information is local to the proxy and is not subject to standardization. Some possible implementations include an initial magic cookie (e.g., z9hG4Bk followed by the pointer/information), or use of a reserved "user" name (e.g., "private") with the optional "password" containing the pointer/information.

5. P-DCS-TRACE-PARTY-ID

In the telephone network, calling identity information is used to support regulatory requirements such as the Customer Originated Trace service, which provide the called party with the ability to report obscene or harassing phone calls to law enforcement. This service is provided independently of caller-id, and works even if the caller requested anonymity. The calling party is here identified as the station originating the call. In order for this service to be dependable, the called party must be able to trust that the calling identity information being presented is valid. One way to achieve this is described in [10].

To initiate a customer-originated-trace from an untrusted UAC, an additional header is defined for the INVITE request. This header is called P-DCS-Trace-Party-ID, and does not appear in any other request or response. The entity addressed by the Request-URI performs the service-provider-specific functions of recording and reporting the caller identity in the P-DCS-Trace-Party-ID for law enforcement action. It then forwards the call to either an announcement server or to the service-provider's business office to collect further information about the complaint. A trusted UAC does not use this header, as it initiates this action locally.

5.1. Syntax

The ABNF description of this header is (some terms used in this ABNF are defined in [2]):

```
P-DCS-Trace-Party-ID = "P-DCS-Trace-Party-ID" HCOLON
                                  name-addr
```

This document adds the following entry to Table 2 of [2]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-DCS-Trace-Party-ID	R	dr	-	-	-	o	-	-

SUB	NOT	REF	INF	UPD	PRA
-	-	-	-	-	-

The addr-spec contained in name-addr contains a URL that identifies the remote endpoint. Addr-spec typically contains a tel: URL or SIP URI giving the identity of the remote endpoint, as provided in the signaling messages that established the session to be traced.

5.2. Procedures at an Untrusted User Agent Client (UAC)

The UAC MUST insert a P-DCS-Trace-Party-ID header into the initial INVITE message for a customer-originated-trace request. The UAC MUST use a SIP URI in the Request-URI with userinfo set to "call-trace" and hostport identifying the call tracing entity for the untrusted UA.

5.3. Procedures at a Trusted User Agent Client (UAC)

A trusted UAC performs the customer-originated-trace in a manner similar to the trusted UAS, described below. A trusted UAC MUST NOT include this header in any request.

5.4. Procedures at an Untrusted User Agent Server (UAS)

This header MUST NOT appear in any response sent by a UAS.

5.5. Procedures at a Trusted User Agent Server (UAS)

If the P-DCS-Trace-Party-ID header is present in the initial INVITE request from a UAC, and the Request-URI of the INVITE has userinfo set to "call-trace" and hostport set to the UAS, the UAS MUST perform the service-provider-specific functions of recording and reporting

the caller identity for law enforcement action. The UAS then MUST redirect the call, via a 3xx response, to either an announcement server or to the service-provider's business office to collect further information about the complaint.

This header MUST NOT appear in any response sent by a UAS.

5.6. Procedures at Proxy

Two sets of proxy procedures are defined: (1) the procedures at an originating proxy, and (2) the procedures at a terminating proxy. The originating proxy is a proxy that received the INVITE request from a non-trusted endpoint.

The terminating proxy is a proxy that sends the INVITE request to a non-trusted endpoint.

A proxy that both receives the INVITE request from an untrusted endpoint, and sends the INVITE request to an untrusted endpoint, performs both sets of procedures.

5.6.1. Procedures at Originating Proxy

If the P-DCS-Trace-Party-ID header is present in the initial INVITE request from the UAC, and the Request-URI of the INVITE has userinfo other than "call-trace" and hostport set to other than a potentially provisioned call tracing entity, then the Proxy MAY reject the request, or MAY remove the P-DCS-Trace-Party-ID header from the request. If the header is present in a valid request, and contains a private-URL that identifies the Proxy in the hostport, then the Originating Proxy SHOULD replace the private-URL with its original contents (i.e., the verified identity of the caller of the session that is being traced).

5.6.2. Procedures at Terminating Proxy

This header MUST NOT appear in any request or response sent by a terminating proxy to an untrusted endpoint.

6. P-DCS-OSPS

Some calls have special call processing requirements that may not be satisfied by normal user agent call processing. For example, when a user is engaged in a call and another call arrives, such a call might be rejected with a busy indication. However, some PSTN operator services require special call processing. In particular, the Busy Line Verification (BLV) and Emergency Interrupt (EI) services initiated by an operator from an Operator Services Position System

(OSPS) on the PSTN network have such a need. Similarly, emergency calls to a 9-1-1 Public Service Access Point (PSAP) may result in trunk signaling causing operator ringback using a howling tone or sustained ring on the originating line (country-specific variations may exist).

In order to inform the SIP user agent that special treatment should be given to a call, we use a new P-DCS-OSPS header field, which may be set to a value indicating when a special type of call processing is requested. We define three values in this header, namely "BLV" for busy line verification, "EI" for emergency interrupt, and "RING" for operator ringback (e.g., howling/sustained tone ring in the US).

If the user agent decides to honor such a request, the response of the user agent to an INVITE with either "BLV" or "EI" will not be a busy indication. Since "EI" and "RING" only occur on established dialogs, they may also appear in UPDATE requests.

6.1. Syntax

The ABNF description of the P-DCS-OSPS header is as follows (some terms used in this ABNF are defined in [2]):

```
P-DCS-OSPS      = "P-DCS-OSPS" HCOLON OSPS-Tag
OSPS-Tag        = "BLV" / "EI" / "RING" / token
```

This document adds the following entry to Table 2 of [2]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-DCS-OSPS	R	dr	-	-	-	o	-	-

SUB	NOT	REF	INF	UPD	PRA
-	-	-	-	o	-

The OSPS-Tag value of "token" is defined for extensibility, and is reserved for future use.

6.2. Procedures at an Untrusted User Agent Client (UAC)

The P-DCS-OSPS header MUST NOT be sent in a request from an untrusted UAC.

6.3. Procedures at a Trusted User Agent Client (UAC)

This header is typically only inserted by a Media Gateway Controller [6] that is controlling a Media Gateway with special trunks to a PSTN OSPS system or PSAP. This trunk group is usually referred to as a BLV-trunk group and employs special signaling procedures that prevent inadvertent use. Calls originating at the PSTN OSPS system are sent over this trunk group, and result in an INVITE request with the P-DCS-OSPS header.

This header MAY be sent in an INVITE request, and MUST NOT appear in any message other than those listed below.

OSPS-Tag value "BLV" MUST NOT appear in any request or response other than an initial INVITE request establishing a new dialog.

OSPS-Tag value "EI" MUST NOT appear in any request or response other than (1) a subsequent INVITE within a pre-existing dialog established with the OSPS-Tag value of "BLV", or (2) an UPDATE request within a pre-existing dialog established with the OSPS-Tag value of "BLV".

OSPS-Tag value "RING" MUST NOT appear in any request or response other than (1) a subsequent INVITE within a pre-existing dialog established by a UAC to an operator or PSAP, or (2) an UPDATE request within a pre-existing dialog established by a UAC to an operator or PSAP.

6.4. Procedures at an Untrusted User Agent Server (UAS)

If the UAS receives an INVITE request with an OSPS-Tag of "BLV", dialog identification that matches an existing dialog, and the existing call was not established with the OSPS-Tag, it MUST reject the request with a 403-Forbidden error code.

If the UAS receives an INVITE/UPDATE request with an OSPS-Tag value of "EI" or "RING", with dialog identification that does not match an existing dialog, it MUST reject the request with a 403-Forbidden response code.

If the UAS receives an INVITE that contains an OSPS-Tag value of "BLV" and is not willing to cooperate in offering this service, it MUST reject the request with a 403-Forbidden response code.

The UAS SHOULD NOT reject an INVITE with a BLV OSPS-Tag due to a busy condition. The UAS MUST NOT respond with a 3xx-Redirect response code to an INVITE with a BLV OSPS-Tag. The UAS SHOULD NOT alert the user of the incoming call attempt if the BLV OSPS-Tag is present in the INVITE.

If an INVITE with OSPS-Tag of "BLV" is accepted (e.g., meeting all QoS pre-conditions, etc.), the UAS MUST send an audio stream on this connection to the address and port given in the SDP of the INVITE. The UAS MAY perform a mixing operation between the two ends of an existing active call and send the resulting media stream to the address and port indicated. Alternatively, the UAS MAY send a copy of the local voice stream, and (if no activity on the local voice stream) send a copy of the received voice stream of an existing call. If the state of the UAS is idle, the UAS SHOULD send a stream of silence packets to OSPS. If the state of the UAS is ringing or ringback, the UAS SHOULD send a ringback stream to OSPS.

If an INVITE/UPDATE with OSPS-Tag of "EI" is accepted, the UAS MUST enable communication between the UAC and the local user. The UAS MAY put any existing call on hold, or initiate an ad-hoc conference.

If an INVITE/UPDATE with OSPS-Tag of "RING" is accepted, the UAS MUST perform operator ringback in accordance with local procedures, e.g., generate a 3-second howling tone or a sustained ring, depending on the state of the user equipment.

6.5. Procedures at a Trusted User Agent Server (UAS)

The procedures at a trusted UAS MUST be identical to those described in 6.4.

6.6. Procedures at Proxy

In the DCS architecture, the OSPS is considered a trusted UAC. If a proxy receives a P-DCS-OSPS header in a request from an untrusted source, it MUST either remove the header or reject the request with a 403-Forbidden response.

A proxy that implements a call-forwarding service MUST NOT respond to an INVITE request with a 3xx response, if the request contained the P-DCS-OSPS header.

7. P-DCS-BILLING-INFO

There are many billing models used in deriving revenue from telephony services today. Charging for telephony services is tightly coupled to the use of network resources. It is outside the scope of this document to discuss the details of these numerous and varying methods.

Proxies have access to subscriber information and act as policy decision points and trusted intermediaries along the call signaling path. Edge routers provide the network connection and resource

policy enforcement mechanism and also capture and report network connection and resource usage information. Edge routers need to be given billing information that can be logged with Record Keeping or Billing servers. The proxy, as a central point of coordination between call signaling and resource management, can provide this information based on the authenticated identity of the calling and called parties. Since there is a trust relationship among proxies, they can be relied upon to exchange trusted billing information pertaining to the parties involved in a call.

For Usage Accounting records, it is necessary to have an identifier that can be associated with all the event records produced for the call. The SIP Call-ID header field cannot be used as such an identifier since it is selected by the originating user agent, and may not be unique among all past calls as well as current calls. Further, since this identifier is to be used by the service provider, it should be chosen in a manner and in a format that meets the service provider's needs.

Billing information may not necessarily be unique for each user (consider the case of calls from an office all billed to the same account). Billing information may not necessarily be identical for all calls made by a single user (consider prepaid calls, credit card calls, collect calls, etc). It is therefore necessary to carry billing information separate from the calling and called party identification. Furthermore, some billing models call for split-charging where multiple entities are billed for portions of the call.

The addition of a SIP General Header Field allows for the capture of billing information and billing identification for the duration of the call.

It is the intent that the billing extensions would only appear on trusted network segments, and MAY be inserted by a proxy or trusted UA in INVITE requests in a trusted network segment, and removed before leaving trusted network segments. The P-DCS-Billing-Info header extension is used only on requests and responses between proxies and trusted User Agents. It is never sent to, nor sent by, an untrusted UA.

7.1. Syntax

The DCS-Billing-Info header is defined by the following ABNF (some terms used in this ABNF are defined in [2]):

```
P-DCS-Billing-Info      = "P-DCS-Billing-Info" HCOLON
                           Billing-Correlation-ID "/" FEID
                           *(SEMI Billing-Info-param)
Billing-Correlation-ID  = 1*48(HEXDIG)
FEID                    = 1*16(HEXDIG) "@" host
Billing-Info-param      = RKS-Group-ID-param / Charge-param /
                          Calling-param / Called-param /
                          Routing-param / Loc-Routing-param /
                          generic-param
RKS-Group-ID-param      = "rksgroup" EQUAL RKS-Group-ID
RKS-Group-ID            = token
Charge-param            = "charge" EQUAL Acct-Charge-URI
Acct-Charge-URI         = LDQUOT addr-spec RDQUOT
Calling-param           = "calling" EQUAL Acct-Calling-URI
Acct-Calling-URI        = LDQUOT addr-spec RDQUOT
Called-param            = "called" EQUAL Acct-Called-URI
Acct-Called-URI         = LDQUOT addr-spec RDQUOT
Routing-param           = "routing" EQUAL Acct-Routing-URI
Acct-Routing-URI        = LDQUOT addr-spec RDQUOT
Loc-Routing-param       = "locroute" EQUAL Acct-Loc-Routing-URI
Acct-Loc-Routing-URI    = LDQUOT addr-spec RDQUOT
```

This document adds the following entry to Table 2 of [2]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-DCS-Billing-Info		admr	-	-	-	o	-	-

SUB	NOT	REF	INF	UPD	PRA
-	-	-	-	-	-

The P-DCS-Billing-Info extension contains an identifier that can be used by an event recorder to associate multiple usage records, possibly from different sources, with a billable account. It further contains the subscriber account information, and other information necessary for accurate billing of the service. This header is only used between proxies and trusted User Agents.

The Billing-Correlation-ID is specified in [9] as a 24-byte binary structure, containing 4 bytes of NTP timestamp, 8 bytes of the unique identifier of the network element that generated the ID, 8 bytes

giving the time zone, and 4 bytes of monotonically increasing sequence number at that network element. This identifier is chosen to be globally unique within the system for a window of several months. This MUST be encoded in the P-DCS-Billing-Info header as a hexadecimal string of up to 48 characters. Leading zeroes MAY be suppressed.

The Financial-Entity-ID (FEID) is specified in [9] as an 8-byte structure, containing the financial identifier for that domain, followed by a domain name. FEID can be associated with a type of service and could be assigned to multiple domains by the same provider. A domain could contain multiple assigned FEIDs. This 8-byte structure MUST be encoded in the P-DCS-Billing-Info header as a hexadecimal string of up to 16 characters. Trailing zeroes MAY be suppressed. "Host" contains the domain name.

The RKS-Group-ID specifies a record keeping server (or group of cooperating servers) for event messages relating to this call. It is used to control certain optimizations of procedures when multiple event message streams are being sent to the same Record Keeping Server.

Additional parameters contain the information needed for generation of event message records. Acct-Charge-URI, Acct-Calling-URI, Acct-Called-URI, Acct-Routing-URI, and Acct-Location-Routing-URI are each defined as URLs; they should all contain tel: URLs with E.164 formatted addresses. These fields are further defined in [9] under the element identifiers "Charge_Number" (element ID 16), "Calling_Party_Number" (element ID 4), "Called_Party_Number" (element ID 5), "Routing Number" (element ID 25), and "Location_Routing_Number" (element ID 22).

7.2. Procedures at an Untrusted User Agent Client (UAC)

This header is never sent to an untrusted UAC, and is never sent by an untrusted UAC.

7.3. Procedures at a Trusted User Agent Client (UAC)

The UAC MUST generate the Billing-Correlation-ID for the call, and insert it into the P-DCS-Billing-Info header in the initial INVITE message sent to the terminating proxy, along with the charging information for the call. The UAC MUST include its FEID, and the RKS-Group-ID for the Record-Keeping-Server being used by the UAC. If the UAC performed a Local Number Portability (LNP) query, it MUST include the Routing Number and Location Routing Number returned by the query.

If the response to the initial INVITE is a 3xx-Redirect, the UAC generates a new initial INVITE request to the destination specified in the Contact: header, as per standard SIP. If a UAC receives a 3xx-Redirect response to an initial INVITE, the new INVITE generated by the UAC MUST contain the P-DCS-Billing-Info header from the 3xx-Redirect response. If the UAC is acting as a B2BUA, instead of generating a new INVITE it MAY generate a private-URL and place it in the Contact header of a 3xx-Redirect response sent to the originating endpoint. This private-URL MUST contain (or contain a pointer to) the P-DCS-Billing-Info value, which indicates the charging arrangement for the new call, and an expiration time very shortly in the future, to limit the ability of the originator to re-use this private-URL for multiple calls.

A UAC that includes a Refer-to header in a REFER request MUST include a P-DCS-Billing-Info header in the Refer-to's URL. This P-DCS-Billing-Info header MUST include the accounting information of the initiator of the REFER.

7.4. Procedures at an Untrusted User Agent Server (UAS)

This header is never sent to an untrusted UAS, and is never sent by an untrusted UAS.

7.5. Procedures at a Trusted User Agent Server (UAS)

The UAS MUST include a P-DCS-Billing-Info header in the first reliable 1xx (except 100) or 2xx response to an initial INVITE message. This P-DCS-Billing-Info header MUST include the Billing-Correlation-ID generated by the UAS, the FEID of the UAS, and the RKS-Group-ID of the Record-Keeping-Server being used by the UAS. The UAS MAY change the values of Acct-Charge-URI if it wishes to override the billing information that was present in the INVITE (e.g., for a toll-free call). The decision to do this and the contents of the new Acct-Charge-URI MUST be determined by service provider policy provisioned in the UAS. If the UAS performed a LNP query, it MUST include the Routing Number and Location Routing Number returned by the query.

The UAS MUST add a P-DCS-Billing-Info header to a 3xx-redirect response to an initial INVITE, giving the accounting information for the call forwarder, for the call segment from the destination to the forwarded-to destination.

7.6. Procedures at Proxy

Three sets of proxy procedures are defined: (1) the procedures at an originating proxy, (2) the procedures at a terminating proxy, and (3) the procedures at a tandem proxy.

The originating proxy is a proxy that received the INVITE request from a non-trusted endpoint.

The terminating proxy is a proxy that sends the INVITE request to a non-trusted endpoint.

A proxy that is neither an originating proxy, nor a terminating proxy, is a tandem proxy.

For purposes of mid-call changes, such as call transfers, the proxy that receives the request from a non-trusted endpoint is considered the initiating proxy; the proxy that sends the request to a non-trusted endpoint is considered the recipient proxy. Procedures for the initiating proxy are included below with those for originating proxies, while procedures for the recipient proxy are included with those for terminating proxies.

A proxy that both receives the INVITE request from an untrusted endpoint, and sends the INVITE request to a non-trusted endpoint, performs both sets of procedures.

7.6.1. Procedures at Originating Proxy

The originating proxy MUST generate the Billing-Correlation-ID for the call, and insert it into the P-DCS-Billing-Info header in the initial INVITE message sent to the terminating proxy, along with the charging information for the call. The originating proxy MUST include its FEID, and the RKS-Group-ID for the Record-Keeping-Server being used by the originating proxy. If the originating proxy performed a LNP query, it MUST include the Routing Number and Location Routing Number returned by the query. Any P-DCS-Billing-Info header present from an untrusted UA MUST be removed.

If the Request-URI contains a private-URL, and the decoded username contains billing information, the originating proxy MUST generate a P-DCS-Billing-Info header with that decrypted information. Otherwise, the originating proxy MUST determine the accounting information for the call originator, and insert a P-DCS-Billing-Info header including that information.

If the response to the initial INVITE is a 3xx-Redirect, received prior to a 18x, the originating proxy generates a new initial INVITE request to the destination specified in the Contact: header, as per standard SIP. If an originating proxy receives a 3xx-Redirect response to an initial INVITE prior to a 18x response, the INVITE generated by the proxy MUST contain the P-DCS-Billing-Info header from the 3xx-Redirect response.

If the response to the initial INVITE is a 3xx-Redirect, received after a 18x, the originating proxy generates a private-URL and places it in the Contact header of a 3xx-Redirect response sent to the originating endpoint. This private-URL MUST contain (or contain a pointer to) the P-DCS-Billing-Info value, which indicate the charging arrangement for the new call, and an expiration time very shortly in the future, to limit the ability of the originator to re-use this private-URL for multiple calls.

An originating proxy that processes a REFER request from an untrusted UA MUST include a P-DCS-Billing-Info header in the Refer-to's URL. This P-DCS-Billing-Info header MUST include the accounting information of the initiator.

7.6.2. Procedures at Terminating Proxy

The terminating proxy MUST NOT send the P-DCS-Billing-Info header to an untrusted destination.

The terminating proxy MUST include a P-DCS-Billing-Info header in the first reliable 1xx (except 100) or 2xx response to an initial INVITE message. This P-DCS-Billing-Info header MUST include the Billing-Correlation-ID generated by the terminating proxy, the FEID of the terminating proxy, and the RKS-Group-ID of the Record-Keeping-Server being used by the terminating proxy. The terminating proxy MAY change the values of Acct-Charge-URI if it wishes to override the billing information that was present in the INVITE (e.g., for a toll-free call). The decision to do this and the contents of the resulting P-DCS-Billing-Info header MUST be determined by service provider policy provisioned in the terminating proxy. If the terminating proxy performed a LNP query, it MUST include the Routing Number and Location Routing Number returned by the query.

The terminating proxy MUST add P-DCS-Billing-Info headers to a 3xx-redirect response to an initial INVITE, giving the accounting information for the call forwarder, for the call segment from the destination to the forwarded-to destination.

A proxy receiving a mid-call REFER request that includes a Refer-to header generates a private-URL and places it in the Refer-to header sent to the endpoint. This private-URL MUST contain the P-DCS-Billing-Info value, which indicate the charging arrangement for the new call, and an expiration time very shortly in the future, to limit the ability of the endpoint to re-use this private-URL for multiple calls.

7.6.3. Procedures at Tandem Proxy

If the tandem proxy performed a LNP query, it MUST insert the Routing Number and Location Routing Number returned by the query into the P-DCS-Billing-Info header in the first reliable 1xx/2xx/3xx (except 100) response.

8. P-DCS-LAES and P-DCS-REDIRECT

NOTE: According to RFC 2804 [5], the IETF supports documentation of lawful intercept technology if it is necessary to develop it. The following section provides such documentation. The RFC 2119 language, as stated above, describes the requirements of the specification only if implemented, and strictly within the applicability domain described above. See RFC 2804 for description of issues regarding privacy, security, and complexity in relation to this technology.

The P-DCS-LAES extension contains the information needed to support Lawfully Authorized Electronic Surveillance. This header contains the address and port of an Electronic Surveillance Delivery Function for delivery of a duplicate stream of event messages related to this call. The header may also contain an additional address and port for delivery of call content. Security key information is included to enable pairs of Delivery Functions to securely exchange surveillance information. This header is only used between proxies and trusted User Agents.

The P-DCS-Redirect extension contains call identifying information needed to support the requirements of Lawfully Authorized Electronic Surveillance of redirected calls. This header is only used between proxies and trusted User Agents.

Use of P-DCS-LAES and P-DCS-Redirect is controlled by a combination of legislation, regulation, and court orders, which MUST be followed. In certain cases inclusion of these headers will be mandated, and therefore MUST be present in the requests and responses indicated. In other cases inclusion of these headers will be forbidden, and therefore MUST NOT be present in the request and responses indicated. In the sub-sections that follow, use of "SHOULD" is intended to

capture these conflicting situations, e.g., a P-DCS-LAES header SHOULD be included in an initial INVITE means either that it MUST be included or that it MUST NOT be included, based on the applicable court orders.

8.1. Syntax

The formats of the P-DCS-LAES and P-DCS-Redirect headers are given by the following ABNF (some terms used in this ABNF are defined in [2] and [3]):

```
P-DCS-LAES        = "P-DCS-LAES" HCOLON Laes-sig
                    *(SEMI Laes-param)
Laes-sig          = hostport
Laes-param        = Laes-content / Laes-key / generic-param
Laes-content      = "content" EQUAL hostport
Laes-key          = "key" EQUAL token

P-DCS-Redirect    = "P-DCS-Redirect" HCOLON Called-ID
                    *(redir-params)
Called-ID         = LDQUOT addr-spec RDQUOT
redir-params      = redir-uri-param / redir-count-param /
                    generic-param
redir-uri-param   = "redirector-uri" EQUAL Redirector
Redirector        = LDQUOT addr-spec RDQUOT
redir-count-param = "count" EQUAL Redir-count
Redir-count       = 1*DIGIT
```

This document adds the following entry to Table 2 of [2]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-DCS-LAES		adr	-	-	-	o	-	-
P-DCS-Redirect		adr	-	-	-	o	-	-

SUB	NOT	REF	INF	UPD	PRA
-	-	-	-	-	-
-	-	-	-	-	-

The values of Laes-sig and Laes-content are addresses of the Electronic Surveillance Delivery Function, and used as the destination address for call-identifying information and call-content, respectively. Laes-key is a string generated by the proxy that is used by the Delivery Function to securely transfer information between them [8].

The P-DCS-Redirect header contains redirection information. The redir-uri-param indicates the original destination requested by the user (e.g., dialed number), the Redirector indicates the new destination, and the Redir-count indicates the number of redirections that have occurred.

8.2. Procedures at an Untrusted User Agent Client (UAC)

This header MUST NOT be sent to an untrusted UAC, and MUST NOT be sent by an untrusted UAC.

8.3. Procedures at a Trusted User Agent Client (UAC)

The UAC checks for an outstanding lawfully authorized surveillance order for the originating subscriber, and, if present, includes this information in the Authorization for Quality of Service [7] or signals this information to the device performing the intercept (e.g., a Media Gateway).

If the P-DCS-LAES header is present in the first reliable 1xx (except 100), 2xx or 3xx response (indicating surveillance is required on the terminating subscriber, but that the terminating equipment is unable to perform that function), the UAC MUST include this information in the Authorization for Quality of Service, or MUST signal this information to the device performing the intercept (e.g., a Media Gateway).

If a 3xx-Redirect response is received to the initial INVITE request, and if a P-DCS-LAES header is present in the 3xx response, the UAC SHOULD include that header unchanged in the reissued INVITE. The UAC SHOULD also include a P-DCS-Redirect header containing the original dialed number, the new destination number, and the number of redirections that have occurred. Although it is technically possible for the originating equipment to perform this surveillance (or add to its existing surveillance of the call), the design of the surveillance system has the terminating equipment performing the surveillance for all the intermediate forwardings.

A UAC that includes a Refer-to header in a REFER request, when the originating subscriber has an outstanding lawfully authorized surveillance order, SHOULD include a P-DCS-LAES header attached to the Refer-to. The P-DCS-LAES header SHOULD include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, SHOULD include the address and port of the local Electronic Surveillance Delivery Function for the copy of call content if call content is to be intercepted, and SHOULD include a random string for use as a security key between the Delivery Functions.

The trusted UAC MUST NOT send the P-DCS-LAES and P-DCS-Redirect headers to an untrusted entity.

8.4. Procedures at an Untrusted User Agent Server (UAS)

This header MUST NOT be sent to an untrusted UAS, and MUST NOT be sent by an untrusted UAS.

8.5. Procedures at a Trusted User Agent Server (UAS)

The UAS checks for an outstanding lawfully authorized surveillance order for the terminating subscriber, or presence of the P-DCS-LAES header in the INVITE request. If either is present, the UAS includes this information in the authorization for Quality of Service [7].

If the terminating equipment is unable to perform the required surveillance (e.g., if the destination is a voicemail server), the UAS SHOULD include a P-DCS-LAES header in the first reliable non-100 response requesting the originating proxy to perform the surveillance. The P-DCS-LAES header SHOULD include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, SHOULD include the address and port of the local Electronic Surveillance Delivery Function for the copy of call content if call content is to be intercepted, and SHOULD include a random string for use as a security key between the Delivery Functions.

If the response to the initial INVITE request is a 3xx-Redirect response, and there is an outstanding lawfully authorized surveillance order for the terminating subscriber, the UAS SHOULD include a P-DCS-LAES header in the 3xx-Redirect response, with contents as described above.

The trusted UAS MUST NOT send the P-DCS-LAES and P-DCS-Redirect headers to an untrusted entity.

8.6. Procedures at Proxy

Two sets of proxy procedures are defined: (1) the procedures at an originating proxy, and (2) the procedures at a terminating proxy. The originating proxy is a proxy that received the INVITE request from a non-trusted endpoint.

The terminating proxy is a proxy that sends the INVITE request to a non-trusted endpoint.

For purposes of mid-call changes, such as call transfers, the proxy that receives the request from a non-trusted endpoint is considered the initiating proxy; the proxy that sends the request to a non-trusted endpoint is considered the recipient proxy. Procedures for the initiating proxy are included below with those for originating proxies, while procedures for the recipient proxy are included with those for terminating proxies.

A proxy that both receives the INVITE request from an untrusted endpoint, and sends the INVITE request to a non-trusted endpoint, MUST NOT generate P-DCS-LAES nor P-DCS-Redirect headers.

A proxy that is neither an originating proxy nor a terminating proxy SHOULD pass the P-DCS-Laes and P-DCS-Redirect headers in requests and responses.

8.6.1. Procedures at Originating Proxy

The Originating Proxy MUST remove any P-DCS-LAES and P-DCS-Redirect headers in requests or responses to or from an untrusted proxy or untrusted UA.

The originating proxy checks for an outstanding lawfully authorized surveillance order for the originating subscriber, and, if present, includes this information in the Authorization for Quality of Service [7] or signals this information to the device performing the intercept (e.g., a Media Gateway).

If the P-DCS-LAES header is present in the first reliable 1xx (except 100), 2xx or 3xx response (indicating surveillance is required on the terminating subscriber, but that the terminating equipment is unable to perform that function), the originating proxy MUST include this information in the Authorization for Quality of Service, or MUST signal this information to the device performing the intercept (e.g., a Media Gateway).

If the Request-URI in an initial INVITE request contains a private-URL, the originating proxy MUST decrypt the userinfo information to find the real destination for the call, and other special processing information. If electronic surveillance information is contained in the decrypted userinfo, the originating proxy SHOULD generate a P-DCS-LAES header with the surveillance information.

If a 3xx-Redirect response is received to the initial INVITE request prior to a 18x, and if a P-DCS-LAES header is present in the 3xx response, the originating proxy SHOULD include that header unchanged in the reissued INVITE. The originating proxy SHOULD also include a

P-DCS-Redirect header containing the original dialed number, the new destination number, and the number of redirections that have occurred.

If a 3xx-Redirect response is received to the initial INVITE request after a 18x, the originating proxy generates a private-URL and places it in the Contact header of a 3xx-Redirect response sent to the originating endpoint. If a P-DCS-LAES header is present in the 3xx response, this private-URL MUST contain (1) the electronic surveillance information from the 3xx-Redirect response, (2) the original destination number, (3) the identity of the redirecting party, and (4) the number of redirections of this call.

An originating proxy that processes a REFER request [4] from an untrusted UA, when the originating subscriber has an outstanding lawfully authorized surveillance order, becomes a B2BUA for that request. It SHOULD reissue the request with a P-DCS-LAES header added to the Refer-to's URL. The P-DCS-LAES header SHOULD include (1) the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, (2) the address and port of the local Electronic Surveillance Delivery Function for the copy of call content if call content is to be intercepted, and (3) a random string for use as a security key between the Delivery Functions.

An initiating proxy that sends a mid-call REFER request including a Refer-to header, when the initiating subscriber has an outstanding lawfully authorized surveillance order, SHOULD include a P-DCS-LAES header in the Refer-to's URL.

The originating proxy MUST NOT send the P-DCS-LAES and P-DCS-Redirect headers to an untrusted entity.

8.6.2. Procedures at Terminating Proxy

The Terminating Proxy MUST remove any P-DCS-LAES and P-DCS-Redirect headers in requests or responses to or from an untrusted proxy or UA.

The terminating proxy checks for an outstanding lawfully authorized surveillance order for the terminating subscriber. If present, the terminating proxy includes this information in the authorization for Quality of Service [7].

The terminating proxy MUST NOT send the P-DCS-LAES and P-DCS-Redirect headers to an untrusted entity, either as headers in the request or response, or as headers attached to URIs in the request or response.

If the terminating equipment is unable to perform the required surveillance (e.g., if the destination is a voicemail server), the terminating proxy SHOULD include a P-DCS-LAES header in the first reliable 1xx/2xx/3xx (except 100) response requesting the originating proxy to perform the surveillance. The P-DCS-LAES header SHOULD include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, SHOULD include the address and port of the local Electronic Surveillance Delivery Function for the copy of call content if call content is to be intercepted, and SHOULD include a random string for use as a security key between the Delivery Functions.

If the response to the initial INVITE request is a 3xx-Redirect response, and there is an outstanding lawfully authorized surveillance order for the terminating subscriber, the terminating proxy SHOULD include a P-DCS-LAES header in the 3xx-Redirect response, with contents as described above.

A proxy receiving a mid-call REFER request [4] that includes a Refer-to header with a P-DCS-LAES header attached becomes a B2BUA for this request. It MUST generate a private-URL and place it in the Refer-to header sent to the endpoint. This private-URL MUST contain the P-DCS-LAES information from the attached header.

9. Security Considerations

QoS gate coordination, billing information, and electronic surveillance information are all considered to be sensitive information that MUST be protected from eavesdropping and furthermore require integrity checking. It is therefore necessary that the trusted UAs and proxies take precautions to protect this information from eavesdropping and tampering. Use of IPsec or TLS between Proxies is REQUIRED. A minimum mandatory-to-implement IPsec configuration for the DCS architecture is given by [8]. Also REQUIRED is mutual authentication (1) between Proxies and (2) between trusted UAs and Proxies, both of which MAY be implemented with administratively pre-shared keys, or through consultation with another trusted third party. If IPsec is to be used, the specification of the security policies and procedures of the administrative domain where these headers are applicable (and all connections between administrative domains in the federation) MUST define an interoperable set of options.

10. IANA Considerations

This document defines a number of SIP extension headers, which have been included in the registry of SIP headers defined in [2]. Registration information for new headers is as follows:

Header Field Name: P-DCS-Trace-Party-ID
RFC Number: 3603
Compact Form: none

Header Field Name: P-DCS-OSPS
RFC Number: 3603
Compact Form: none

Header Field Name: P-DCS-Billing-Info
RFC Number: 3603
Compact Form: none

Header Field Name: P-DCS-LAES
RFC Number: 3603
Compact Form: none

Header Field Name: P-DCS-Redirect
RFC Number: 3603
Compact Form: none

11. Intellectual Property Rights Notice

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

12. References

12.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[3] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[4] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

[5] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

12.2. Informative References

[6] DCS Group, "Architectural Considerations for Providing Carrier Class Telephony Services Utilizing SIP-based Distributed Call Control Mechanisms", Work in Progress.

[7] PacketCable Dynamic Quality of Service Specification, pkt-sp-dqos-i07-030815, August 2003.

[8] PacketCable Security Specification, pkt-sp-sec-i09-030728, July 2003.

[9] PacketCable Event Message Specification, pkt-sp-em-i07-030815, August 2003.

[10] Jennings, C., Peterson, J. and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

13. Acknowledgements

The Distributed Call Signaling work in the PacketCable project is the work of a large number of people, representing many different companies. The authors would like to recognize and thank the following for their assistance: John Wheeler, Motorola; David Boardman, Daniel Paul, Arris Interactive; Bill Blum, Jon Fellows, Jay Strater, Jeff Ollis, Clive Holborow, Motorola; Doug Newlin, Guido Schuster, Ikhlaq Sidhu, 3Com; Jiri Matousek, Bay Networks; Farzi Khazai, Nortel; John Chapman, Bill Guckel, Michael Ramalho, Cisco; Chuck Kalmanek, Doug Nortz, John Lawser, James Cheng, Tung- Hai Hsiao, Partho Mishra, AT&T; Telcordia Technologies; and Lucent Cable Communications.

Previous versions further acknowledged, as co-authors, several people for providing the text of this document. They are:

Bill Marshall (wtm@research.att.com) and K. K. Ramakrishnan (kkrama@research.att.com), AT&T; Ed Miller (edward.miller@terayon.com), Terayon; Glenn Russell (G.Russell@Cablelabs.com), CableLabs; Burcak Beser (burcak@juniper.net) Juniper Networks, Mike Mannette (Michael_Mannette@3com.com) and Kurt Steinbrenner (Kurt_Steinbrenner@3com.com), 3Com; Dave Oran (oran@cisco.com) and

Flemming Andreasen (fandreas@cisco.com), Cisco Systems; John Pickens (jpickens@com21.com), Com21; Poornima Lalwaney (poornima.lalwaney@nokia.com), Nokia; Jon Fellows (jfellows@coppermountain.com), Copper Mountain Networks; Doc Evans (n7dr@arrisi.com) Arris, and Keith Kelly (keith@netspeak.com), NetSpeak.

14. Editors' Addresses

Bill Marshall
AT&T
Florham Park, NJ 07932

EMail: wtm@research.att.com

Flemming Andreasen
Cisco
Edison, NJ

EMail: fandreas@cisco.com

15. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.