SIP Working Group
Internet Draft
Document: <draft-dcsgroup-sip-proxy-proxy-06.txt>

Category: Informational

W. Marshall
AT&T

K. Ramakrishnan
TeraOptic Networks

E. Miller
Terayon Networks

G. Russell
CableLabs

B. Beser
Juniper Networks

M. Mannette
K. Steinbrenner
3Com

D. Oran
F. Andreasen
Cisco

J. Pickens
Com21

P. Lalwaney
Nokia

J. Fellows
Copper Mountain Networks

D. Evans
D. R. Evans Consulting

K. Kelly
NetSpeak

February 28, 2002

SIP proxy-to-proxy extensions for supporting DCS

Status of this Memo

1. 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 extensions to the Session Initiation Protocol (RFC2543) for supporting the exchange of customer information and billing information between trusted entities in the architecture described in <draft-dcsgroup-sip-arch-02.txt>.

2. 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 RFC-2119 [2].

3. Table of Contents

4. Introduction

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 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 [3] 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 [3], have access to subscriber information and act as policy decision points and trusted intermediaries along the call signaling path. Edge routers provide the policy enforcement mechanism and also capture and report 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.

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. Rules for inserting and removing headers exchanged only between proxies are for further study.

Significant amounts of information is retrieved by an originating 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. Call-ID 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 two SIP General Header Fields allows for the capture of billing information and billing identification for the duration of the call. Alternative techniques such as multi-part attachments will not coexist with encrypted messages.

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 requests entering a trusted network segment, and removed before leaving trusted network segments.

5. Trust Boundary

The DCS architecture 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 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. A trusted user agent is, in almost all cases, equivalent to the combination of an untrusted user agent and a proxy.

6. Requires and Supported Option Tag Values

UACs which support one or more of the extensions defined here include a Supported header in all requests, except ACK, with the option tag according to the following table:

Extension Headers Supported	Option tag
DCS-Trace-Party-ID	DCS.Trace
DCS-Gate	DCS.Gate
DCS-OSPS	DCS.OSPS
DCS-Billing-ID and DCS-Billing-Info	DCS.Billing
DCS-LAES and DCS-Redirect	DCS.Laes
All of the above	DCS

Proxies on the signaling path may have their own requirements for

the extensions defined in this document. If the Supported header in the request lists the option tag value given above, a proxy can be certain the UAC understands the extension headers corresponding to that tag value. If, however, the Supported header was absent, or was present but didn't include the desired tag value, the proxy MAY reject the request with a 421, and indicate in the Require header that one or more of the features are needed. As an alternative, the proxy MAY forward the request, but MUST NOT add any extensions defined in this document. This will allow the call to proceed without the extensions.

If a proxy wishes to ensure that the UAS understands the extensions described in this document, it MAY add a Requires header to the request with the option tag value as given above. If a proxy wishes to ensure that other proxies understand the extensions described in this document, it MAY add a Proxy-Requires header to the request with the option tag value as given above.

If a proxy receives a request with a Proxy-Requires header with an option tag value given above, but does not support the extensions described in this document for that tag value, it MUST reject the request with a 421.

If the UAS receives a request with a Requires header with an option tag value given above, but does not support the extensions described in this document for that tag value, it MUST reject the request with a 421.

If a proxy or UAS receives a request with a Supported header with an option tag value given above, and uses the extensions described in this document in the response, it MUST include a Require header in the response, with the appropriate tag value, indicating that the feature was applied to the response.

7. 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 independent of caller-id, and operates 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.

To initiate a customer-originated-trace from an untrusted UAC, an additional header is defined for the INVITE request sent from the untrusted UAC to its proxy. This header is called Dcs-Trace-Party-ID, and does not appear in any other request or response. The proxy receiving a properly formed INVITE request with this header performs the service-provider-specific functions of recording and reporting the caller identity for law enforcement action. The proxy then completes 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.

7.1 Syntax

The BNF description of this header is:

```
Dcs-Trace-Party-ID = "Dcs-Trace-Party-ID" ":" "<" addr-spec ">"
```

Addr-spec contains a URL that identifies the remote endpoint. Addr-spec typically contains a tel: URL giving the identity of the remote endpoint, or a DCS-URL with a private-param when privacy was requested by the remote endpoint. This URL SHOULD be the value received in the Remote-Party-ID header of the harassing call.

7.2 Procedures at an Untrusted User Agent Client (UAC)

The UAC MUST insert a Dcs-Trace-Party-ID header into the initial INVITE message for a customer-originated-trace request. The UAC MUST use a Request-URI with username of "call-trace" and host identifying the provisioned proxy for the untrusted UA.

7.3 Procedures at a Trusted User Agent Client (UAC)

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

7.4 Procedures at an Untrusted User Agent Server (UAS)

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

7.5 Procedures at a Trusted User Agent Server (UAS)

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

7.6 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.

7.6.1 Procedures at Originating Proxy

If the Dcs-Trace-Party-ID header is present in the initial INVITE request from the UAC, and the Request-URI of the INVITE has username of "call-trace" and host of the originating proxy, the originating proxy MUST perform the service-provider-specific functions of recording and reporting the caller identity for law enforcement action. The proxy then MUST direct the call to either an announcement server or to the service-provider's business office to collect further information about the complaint.

The originating proxy MUST remove the Dcs-Trace-Party-ID header from the INVITE before sending the request to another proxy or UAS.

7.6.2 Procedures at Terminating Proxy

This header MUST NOT appear in any request or response sent by a proxy.

8. DCS-GATE

The Dcs-Gate header extension is used only on requests and responses between proxies. It never is sent to, nor sent by, an untrusted UAC/UAS.

The proxy-proxy signaling establishes a synchronization path that may be required by the PacketCable Dynamic Quality of Service (D-QoS) specification to coordinate the release of resources of the call. As per the D-QoS specification, the CMTS monitors the packet flow, and generates a Gate-Close message in response to either an explicit close request from the MTA/RGW, or when an equipment or facility failure causes the connection to be broken. This Gate-Close message is directed either to the local CMS/Agent, or to the remote CMS/Agent, or to the CMTS serving the remote MTA, depending on the capabilities of the endpoints. When a CMS/Agent receives such a Gate-Close message, it considers it identical to a call termination request.

The Dcs-Gate header is used between proxies, and conveys the location of the remote gate, identity of the gate, and the security key to be used in gate coordination messages.

8.1 Syntax

The BNF description of the Dcs-Gate header is as follows:

```
Dcs-Gate               = "Dcs-Gate" ":" hostport "/" Gate-ID
                          [";" Gate-Key ";" Gate-CipherSuite]
                          [Gate-strength-token]
Gate-ID                = 1*alphanum
Gate-Key               = 1*alphanum
Gate-CipherSuite       = token
Gate-strength-token    = "required" | "optional"
```

Hostport gives the IP address or FQDN of the CMTS/EdgeRouter that enforces the QoS, or the endpoint system that simulates the gate coordination exchange on behalf of an edge router.

Gate-ID is a token used at the system named in the Hostport parameter to identify the particular session. For DCS systems, it is a 32-bit quantity encoded as an 8-character string of digits 0-9 and letters a-f.

Gate-Key is a character string that provides keying information to the system named in the hostport parameter. The method of deriving the actual keys for the gate coordination messages, and the security procedures, are beyond the scope of this document.

Gate-CipherSuite is a character string that gives the type of encryption algorithm that will be used to secure the gate coordination messages.

Gate-Strength-Token specifies whether the gate coordination is required or optional for the current session. Its use is described in the following sections.

8.2 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.

8.3 Procedures at a Trusted User Agent Client (UAC)

A UAC located within the trust boundary of the service provider

performs the functions given in section 7.6.1.

8.4 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.

8.5 Procedures at a Trusted User Agent Server (UAS)

A UAS located within the trust boundary of the service provider performs the functions given in section 7.6.2.

8.6 Procedures at Proxy

The Dcs-Gate header MUST NOT appear in any message other than the initial INVITE request, or in the first non-100 response to that request. The proxy MUST remove the Dcs-Gate header in any request or response sent to an untrusted endpoint.

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 a non-trusted endpoint, does not generate a Dcs-Gate header.

A proxy that is neither an originating proxy nor a terminating proxy has no function in coordinating the commitment of resources.

8.6.1 Procedures at Originating Proxy

The originating proxy MUST insert a Dcs-Gate header in the initial INVITE message for a new call.

The originating proxy MUST identify the system that will perform gate coordination (either the proxy itself, or the CMTS controlling the media flow to the endpoint), and the identification token used at that system to identify the call. It MUST insert the IP address or FQDN of that system in the hostport parameter of the Dcs-Gate header, and the identification token as the Gate-ID.

The originating proxy MUST pick a security key and cipher suite for the gate coordination message exchange, and insert these values in the Dcs-Gate header.

If the system that will perform gate coordination is a CMTS, the strength token MUST be given as required. If the system that will perform gate coordination is the proxy itself, the strength token MAY be given as optional, or omitted.

8.6.2 Procedures at Terminating Proxy

The terminating proxy MUST identify the system that will perform gate coordination (either the proxy itself, or the CMTS controlling

the media flow to the endpoint), and the identification token used at that system to identify the call. Gate coordination will be required for this call if (1) the strength token in the Dcs-Gate header in the initial INVITE indicates 'required', or (2) the system that will perform gate coordination at the destination is a CMTS.

If gate coordination is required for this call, the terminating proxy MUST include a Dcs-Gate header in the first non-100 response to the initial INVITE request. It MUST insert the IP address or FQDN of the system that will perform gate coordination in the hostport parameter of the Dcs-Gate header, and the identification token as the Gate-ID.

If gate coordination is not required for this call, the terminating proxy SHOULD NOT include a Dcs-Gate header in the first non-100 response to the initial INVITE request.

9. 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.

In order to inform the SIP user agent that special treatment should be given to a call, we use a new OSPS header field, which may be set to a value indicating when a special type of call processing is requested. We define two values in this header, namely "BLV" for

busy line verification and "EI" for emergency interrupt.

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. When such a request is received, the user agent may look at the Remote-Party-ID, and decide only to honor the request if "rpi-type" is "operator" and Remote-Party-ID was authenticated by the user agent's proxy.

9.1 Syntax

```
Dcs-OSPS        = "Dcs-OSPS" ":" OSPS-Tag
OSPS-Tag        = "BLV" | "EI" | token
```

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

9.2 Procedures at an Untrusted User Agent Client (UAC)

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

9.3 Procedures at a Trusted User Agent Client (UAC)

This header is typically only inserted by a Media-Gateway-Controller that is controlling a Media Gateway with special MF trunk connections to a PSTN OSPS system. This trunk group is usually referred to as a BLV-trunk group, and employs special signaling procedures that prevent inadvertant use. Calls originating at the PSTN OSPS system are sent over this trunk group, and result in an INVITE request with the OSPS header.

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

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

OSPS-Tag value "EI" MUST NOT appear in any INVITE request other than a subsequent INVITE within a pre-existing session established with the OSPS-Tag value of "BLV".

9.4 Procedures at an Untrusted User Agent Server (UAS)

If the UAS receives an INVITE request with an OSPS-Tag, call-leg

identification that matches an existing call, and the existing call was not established with the OSPS-Tag, it MUST reject the request with a 409-Conflict error code. If the UAS receives an INVITE request with an OSPS-Tag value of "EI", with call-leg identification that does not match an existing call, it MUST reject the request with a 409-Conflict error 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 error code. Otherwise, the UAS MUST verify the Dcs-Remote-Party-ID header contains a rpi-type token with value "operator." If the call is not from a service-provider-certified operator, it SHOULD be rejected with a 401-Unauthorized error 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 error code to an INVITE with a BLV OSPS-Tag. The UAS SHOULD NOT alert the user of the incomming call attempt if the BLV OSPS-Tag is present in the INVITE.

If an INVITE with OSPS-Tag of "BLV" is accepted (meeting all QoS pre-conditions, etc.), the UAS MUST send an audio stream on this conection 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 active call. 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. 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 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.

9.5 Procedures at a Trusted User Agent Server (UAS)

The procedures at a trusted UAS are identical to those described in 8.4.

9.6 Procedures at Proxy

There is no special processing of this header at proxies.

10. DCS-BILLING-ID and DCS-BILLING-INFO

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 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 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.

Proxies have access to subscriber information and act as policy decision points and trusted intermediaries along the call signaling path. Edge routers provide the policy enforcement mechanism and also capture and report 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 these reasons, it is appropriate to consider defining SIP header extensions to allow 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. Rules for inserting and removing headers exchanged only between proxies are for further study.

Significant amounts of information is retrieved by an originating 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. Call-ID 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 two SIP General Header Fields allows for the capture of billing information and billing identification for the duration of the call. Alternative techniques such as multi-part attachments will not coexist with encrypted messages.

It is the intent that the billing extensions would only appear on trusted network segments, and MAY be inserted by a proxy in INVITE requests entering a trusted network segment, and removed before leaving trusted network segments. The Dcs-Billing-ID and Dcs-Billing-Info header extensions are used only on requests and responses between proxies. They are never sent to, nor sent by, an untrusted UAC/UAS.

10.1 Syntax

The Dcs-Billing-ID and Dcs-Billing-Info headers are defined by the following BNF.

```
Dcs-Billing-ID          = "Dcs-Billing-ID" ":"
                                Billing-Correlation-ID "/" FEID
Dcs-Billing-Info        = "Dcs-Billing-Info" ":"
```

```
                                [hostport] 1#Acct-Entry
     Acct-Entry             = Acct-Charge-URI "/"
                                Acct-Calling-URI  "/"
                                Acct-Called-URI
                                ["/" Acct-Routing-URI
                                "/" Acct-Loc-Routing-URI]

     Acct-Charge-URI        = "<" URI ">"
     Acct-Calling-URI       = "<" URI ">"
     Acct-Called-URI        = "<" URI ">"
     Acct-Routing-URI       = "<" URI ">"
     Acct-Loc-Routing-URI   = "<" URI ">"
     Billing-Correlation-ID = 1*hex
     FEID                   = 1*hex
```

The Dcs-billing-ID 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. Dcs-billing-id is chosen to be globally unique within the system for a window of several months. This header is only used between proxies.

The Billing-Correlation-ID is specified in other PacketCable documents as a 16-byte binary structure, containing 4 bytes of NNTP timestamp, 8 bytes of MAC address of the network element that generated the ID, and 4 bytes of monotonically increasing sequence number at that network element. This MUST be encoded in the Dcs-Billing-ID header as a hex string of up to 32 characters. Leading zeroes may be suppressed.

The Financial Entity ID (FEID) is specified in other PacketCable documents as a 4-byte binary structure, containing the financial identifier for that domain. 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 MUST be encoded in the Dcs-Billing-ID header as a hex string of up to 8 characters. Leading zeroes may be suppressed.

The Dcs-billing-info extension identifies a subscriber account number of the payer, and other information necessary for accurate billing of the service.

The hostport, if present, specifies a record keeping server for event messages relating to this call. If not present, the default record keeping server for each network element is sent the event messages.

Acct-data contains the information needed by the Gate Controller to give to the CMTS 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.

10.2 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.

10.3 Procedures at a Trusted User Agent Client (UAC)

The UAC MUST generate the Billing-Correlation-ID for the call, and insert the Dcs-Billing-ID header into the initial INVITE message sent to the terminating proxy.

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 INVITE generated by the UAC MUST contain the Dcs-Billing-Info headers from the 3xx-Redirect response.

An originating proxy that includes a Refer-to header in a REFER request MUST include a Dcs-Billing-Info header in the Refer-to's URL. This Dcs-Billing-Info header MUST include the accounting information of the initiator.

A UAC that sends a mid-call REFER request including a Refer-to header MUST include a Dcs-Billing-ID header and one or more Dcs-Billing-Info headers attached to the Refer-to. The Dcs-Billing-Info headers MUST include the complete set of Dcs-Billing-Info headers associated with the current call, and MUST include one additional Dcs-Billing-Info header (for the segment from the initiator) with accounting information of the initiator.

10.4 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.

10.5 Procedures at a Trusted User Agent Server (UAS)

The UAS MAY include a Dcs-Billing-Info header in the first non-100 response to an initial INVITE message 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 Dcs-Billing-Info header MUST be determined by service provider policy provisioned in the UAS.

The UAS MUST add Dcs-Billing-Info headers to a 3xx-redirect response to an initial INVITE. All Dcs-Billing-Info headers present in the initial INVITE MUST be copied to the 3xx-redirect response. In addition, the UAS MUST add an additional Dcs-Billing-Info header,

for the segment from the destination to the forwarded-to destination, giving the accounting information for the call forwarder.

10.6 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, does not generate Dcs-Billing-ID nor Dcs-Billing-Info headers.

A proxy that is neither an originating proxy nor a terminating proxy has no function in manipulating existing calls.

10.6.1 Procedures at Originating Proxy

The originating proxy MUST generate the Billing-Correlation-ID for the call, and insert the Dcs-Billing-ID header into the initial INVITE message sent to the terminating proxy.

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

If the response to the initial INVITE is a 3xx-Redirect, received prior to a 18x-Ringing, 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-Ringing response, the INVITE generated by the proxy MUST contain the Dcs-Billing-Info headers from the 3xx-Redirect response.

If the response to the initial INVITE is a 3xx-Redirect, received after a 18x-Ringing, 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 the sequence of Dcs-Billing-Info values, which indicate the complex 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-param for multiple calls.

An originating proxy that includes a Refer-to header in a REFER request MUST include a Dcs-Billing-Info header in the Refer-to's URL. This Dcs-Billing-Info header MUST include the accounting information of the initiator.

An initiating proxy that sends a REFER request including a Refer-to header MUST include a Dcs-Billing-ID header and one or more Dcs-Billing-Info headers in the Refer-to's URL. The Dcs-Billing-Info headers MUST include the complete set of Dcs-Billing-Info headers associated with the current call, and MUST include one additional Dcs-Billing-Info header (for the segment from the initiator) with accounting information of the initiator.

10.6.2 Procedures at Terminating Proxy

The terminating proxy MUST NOT send the Dcs-Billing-ID nor the Dcs-Billing-Info headers to a non-trusted destination.

The terminating proxy MAY include a Dcs-Billing-Info header in the first non-100 response to an initial INVITE message 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 Dcs-Billing-Info header MUST be determined by service provider policy provisioned in the terminating proxy. The terminating proxy MUST add Dcs-Billing-Info headers to a 3xx-redirect response to an initial INVITE. All Dcs-Billing-Info headers present in the initial INVITE MUST be copied to the 3xx-redirect response. In addition, the terminating proxy MUST add an additional Dcs-Billing-Info header, for the segment from the

destination to the forwarded-to destination, giving the accounting information for the call forwarder.

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 value of Dcs-Billing-ID, the sequence of Dcs-Billing-Info values, which indicate the complex 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-param for multiple calls.

11. DCS-LAES and DCS-REDIRECT

The 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.

The 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.

11.1 Syntax

The format of the Dcs-Laes header is given by the following BNF.

```
Dcs-LAES        = "Dcs-LAES" ":" Laes-sig ["," Laes-content]
                        ";" Laes-key
Laes-sig        = hostport
Laes-content    = hostport
Laes-key        = token
Dcs-Redirect    = "Dcs-Redirect" ":" Called-id  Redirector
                        Num-redir
Called-id       = "<" SIP-URL ">"
Redirector      = "<" SIP-URL ">"
Num-redir       = 1*DIGIT
```

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.

11.2 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.

11.3 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 or signals this information to the device performing the intercept (e.g. a Media Gateway).

If the Dcs-LAES header is present in the 183-Session-Progress 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 Dcs-LAES header is present in the 3xx response, the UAC MUST include that header unchanged in the reissued INVITE. The UAC MUST also include a Dcs-Redirect header containing the original dialed number, the new destination number, and the number of redirections that have occurred.

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

The trusted UAC MUST NOT send the Dcs-Laes and Dcs-Redirect headers to an untrusted entity.

11.4 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.

11.5 Procedures at a Trusted User Agent Server (UAS)

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

If the terminating equipment is unable to perform the required surveillance (e.g. if the destination is a voicemail server), the UAS MUST include a Dcs-LAES header in the 183-Session-Progress response requesting the originating proxy to perform the surveillance. The Dcs-LAES header MUST include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, MUST 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 MUST 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 MUST include a Dcs-Laes header in the 3xx-Redirect response, with contents as described above.

The trusted UAS MUST NOT send the Dcs-Laes and Dcs-Redirect headers to an untrusted entity.

11.6 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, does not generate Dcs-Laes nor Dcs-Redirect headers.

A proxy that is neither an originating proxy nor a terminating proxy has no function in manipulating existing calls.

11.6.1 Procedures at Originating Proxy

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 or signals this information to the device performing the intercept (e.g. a Media Gateway).

If the Dcs-LAES header is present in the 183-Session-Progress 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 the private-param user parameter, the originating proxy MUST decrypt the username information to find the real destination for the call, and other special processing information. If electronic surveillance information is contained in the decrypted username, the originating proxy MUST generate a Dcs-LAES header with the surveillance information.

If a 3xx-Redirect response is received to the initial INVITE request prior to a 18x-Ringing, and if a Dcs-LAES header is present in the

3xx response, the originating proxy MUST include that header unchanged in the reissued INVITE. The originating proxy MUST also include a 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-Ringing, 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 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 includes a Refer-to header in a REFER request, when the originating subscriber has an outstanding lawfully authorized surveillance order, MUST include a Dcs-Laes header in the Refer-to's URL. The Dcs-LAES header MUST include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, MUST 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 MUST include 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, MUST include a Dcs-Laes header in the Refer-to's URL. The Dcs-Laes header MUST include the information listed above.

The originating proxy MUST NOT send the Dcs-Laes and Dcs-Redirect headers to an untrusted entity.

11.6.2 Procedures at Terminating Proxy

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.

The terminating proxy MUST NOT send the Dcs-Laes and Dcs-Redirect headers to an untrusted entity.

If the terminating equipment is unable to perform the required surveillance (e.g. if the destination is a voicemail server), the terminating proxy MUST include a Dcs-LAES header in the 183-Session-Progress response requesting the originating proxy to perform the surveillance. The Dcs-LAES header MUST include the address and port of the local Electronic Surveillance Delivery Function for a copy of the call's event messages, MUST 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 MUST 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 MUST include a Dcs-Laes header in the 3xx-Redirect response, with contents as described above.

A proxy receiving a mid-call REFER request that includes a Refer-to header with a Dcs-laes header attached MUST generate a private URL and place it in the Refer-to header sent to the endpoint. This private URL MUST contain the Dcs-Laes information from the attached header.

12. Security Considerations

Billing information is often considered sensitive and private information to the customers. It is therefore necessary that the Proxies take precautions to protect this information from eavesdropping and interception. Use of IPSec between Proxies is recommended.

13. Notice Regarding Intellectual Property Rights

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.

14. References

1. Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

3 DCS Group, "Architectural Considerations for Providing Carrier Class Telephony Services Utilizing SIP-based Distributed Call Control Mechanisms", draft-dcsgroup-sip-arch-04.txt, February 2001.

15. 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.

16. Author's Addresses

Bill Marshall
AT&T
Florham Park, NJ 07932
Email: wtm@research.att.com

K. K. Ramakrishnan
TeraOptic Networks
Summit, NJ 07901
Email: kk@teraoptic.com

Ed Miller
Terayon
Louisville, CO 80027
Email: edward.miller@terayon.com

Glenn Russell
CableLabs
Louisville, CO 80027
Email: G.Russell@Cablelabs.com

Burcak Beser
Juniper Networks
Sunnyvale, CA
Email: burcak@juniper.net

Mike Mannette
3Com
Rolling Meadows, IL 60008
Email: Michael_Mannette@3com.com

Kurt Steinbrenner
3Com
Rolling Meadows, IL 60008
Email: Kurt_Steinbrenner@3com.com

Dave Oran
Cisco

Acton, MA 01720
Email: oran@cisco.com

Flemming Andreasen
Cisco
Edison, NJ
Email: fandreas@cisco.com

John Pickens
Com21
San Jose, CA
Email: jpickens@com21.com

Poornima Lalwaney
Nokia
San Diego, CA 92121
Email: poornima.lalwaney@nokia.com

Jon Fellows
Copper Mountain Networks
San Diego, CA 92121
Email: jfellows@coppermountain.com

Doc Evans
D. R. Evans Consulting
Boulder, CO 80303
Email: n7dr@arrl.net

Keith Kelly
NetSpeak
Boca Raton, FL 33587
Email: keith@netspeak.com

Full Copyright Statement

This memo is filed as <draft-dcsgroup-sip-proxy-proxy-06.txt>, and expires August 31, 2002.