SIP Extensions for Caller Identity, Privacy and Operator Services

Status of this Memo

This document is an Internet-Draft and is NOT offered in accordance with Section 10 of RFC2026[1], and the author does not provide the IETF with any rights other than to publish as an Internet-Draft.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

DCS Group Internet Draft - Expiration 9/30/00 1
SIP Extensions for Caller Privacy March 2000

The list of Internet-Draft Shadow Directories can be accessed at
The Session Initiation Protocol (SIP) [4] is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. In the current PSTN, call signaling messages travel through switches which act as trusted intermediaries. The signaling messages typically include calling party identification information which may be delivered to the called party. The calling party is able to suppress the delivery of such information to the called party in order to maintain privacy.

In a Voice over IP environment using SIP user agents as the equivalent of telephones and SIP proxies as trusted intermediaries, there may still be requirements to provide calling party identification information, yet communicating parties may also desire to maintain their privacy. In this document, we describe three proposed SIP extensions. The first one may be used to support calling and called party, i.e. remote party, identification including a remote party-type to identify special types of callers such as operators. The second extension allows a party to request privacy in the above mentioned environment and includes a recognition that privacy in a VoIP environment extends beyond simply hiding SIP level user information, to potentially hiding the parties IP address information as well. The third extension allows a user agent to be requested to extend special operation to some calls such as operator services.

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. Introduction

In the telephone network, calling identity information is needed to support the Calling Number Delivery and Calling Name Delivery services which provide the called party with identity information about the calling party prior to the called party answering the call; 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. Consider for example a telemarketer presenting himself with the identity of one of your co-workers, or, even worse, an automated credit-card activation system
using calling identity information as an authentication check. In order for the calling identity information to be trustworthy, the information must come from a trusted source.

Calling identity information may also be needed to support regulatory requirements for a public telephony service. An example of this is the Customer Originated Trace service, which enables a called party to have the identity of a calling party recorded by the telephony service provider. This enables, e.g., the receiver of harassing phone calls to make the identity of the originator of such calls available to the proper authority. Again, in order for this service to be useful, the Calling Identity information recorded must be trustworthy.

One scenario for establishing such trust is for a SIP user agent to require that all incoming SIP invitations arrive through a trusted SIP proxy. For simplicity we will assume that each SIP user agent is associated with a single SIP proxy, which we will refer to as a DCS-proxy in this document. DCS-proxies are interconnected with other DCS-proxies which may or may not trust each other. When a SIP user agent originates a call through its DCS-proxy, it trusts that the DCS-proxy will carry out the service requested, even if other DCS-proxies are involved. The DCS-proxy however does not trust the SIP user agent since it will typically reside at the customer premise.

When a call is placed, the calling identity delivery services reveal privacy information to the called party, and the calling party therefore has the option to block the delivery of this information to the called party. In the PSTN, this is typically achieved by subscribing to a Calling Identity Delivery Blocking service but can be done on an individual call basis as well. When the Calling Identity Delivery Blocking Service is invoked, information about the calling party is still passed through the trusted intermediaries, however presentation restriction indicators are set in the signaling messages to signal the far-end side, that the calling identity information is not to be provided to the called party.

More generally, we may say that the service provided is that of preventing the called party from obtaining information about the calling party that may either be used to identify the party or reveal location information about the party. In an IP environment, IP addressing information may provide the other party with information to reach or identify the calling party. IP addressing information may reveal some level of location information, for instance if one has knowledge of which addresses are deployed where, or by revealing that a given caller is using a different IP-address or address block than usual.

When such a privacy service is to be provided in a SIP environment, it leads to two requirements. First, calling identity information present in SIP messages must not be delivered in an intelligible form to the called party, yet it must be possible to determine the identity of the call originator even in the case where the call is routed through one or more untrusted intermediaries. Secondly, when using SIP in an IP environment, IP addressing information must be
able to be hidden from the other party. Furthermore, in an IP environment, these requirements apply equally well in the opposite direction, i.e. the calling party may wish to identify the called party and the called party may have privacy concerns as well.

4. SIP Extensions

In the following we present our proposed SIP extensions for Calling and Called Identity Delivery, and Privacy as well as an extension for requesting special call processing, e.g. for operator services. We then present an example of how the privacy extensions may be used to provide the privacy service.

The syntax specification in the following uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [3].

4.1 CALLING AND CALLED PARTY IDENTITY DELIVERY

For the Calling and Called Identity Delivery, we assume that a SIP user agent can determine if invitations are arriving through its DCS-proxy, and thereby can be trusted, or not. Furthermore, as in the current telephone network, the trusted DCS-proxy is assumed to either receive or possess calling party information that enables it to determine the identity of the calling party. In the following, we will use the term remote party to refer to calling and called party, where a distinction is not important.

The calling party identity information could be provided to the called party’s DCS-proxy as the "display-name" in the "name-addr" part of a From header field [4]. Even though the "display-name" is part of the "From" header, it is not considered part of the call leg identifier. SIP user agents and DCS-proxies would therefore be able to manipulate the value of this parameter, including adding, modifying, and deleting Calling Identity information. This was in fact suggested in a previous version of this document, but based on Working Group feedback, it was preferred to introduce a separate header field for this.

The header field suggested is called Remote-Party-ID, which is added to an INVITE message to identify the caller and provides a long-lived identification of the caller. The header field may also be added to the response to provide a long-lived identification of the called party. The Remote-Party-ID header field is inserted by the originating SIP user agent, and is verified and possibly modified by its DCS Proxy. The DCS-proxy authenticates the information provided, for example by digitally signing the Remote-Party-ID or simply providing a Message Authentication Code (MAC); the details depend on the authentication scheme used. Whenever the call originator requests privacy and the message crosses a trust boundary, the Remote-Party-ID must be encrypted to ensure that its confidentiality is maintained while still enabling the call originator to be identified (by the encrypting proxy).
The terminating DCS Proxy forwards the Remote-Party-ID header to the destination SIP user agent in an intelligible form (if possible) only if the user agent has subscribed to Caller ID/Calling Name delivery service, and the originator has not requested privacy. Similar operation may be performed in the reverse direction. The proposed header syntax follows:

```
Remote-Party-ID    = "Remote-Party-ID" "::" [display-name] 
                   "<" addr-spec ">
                   *(":"" rpi-token)

rpi-token        = rpi-id | rpi-type | rpi-auth | 
                   other-rpi-token

rpi-id           = "rpi-id" "=" 
                   ("private" | "unavailable" 
                   | "na")

rpi-type         = "rpi-type" "=" 
                   ("operator" | token)

rpi-auth         = "auth" "=" auth-scheme 
                   #auth-param

auth-scheme      = token

auth-param      = token "=" (token | quoted-string)

other-rpi-token = token ["=" (token | quoted-string)]
```

Furthermore, we define the value "private" for "other-param" in an "addr-spec", to indicate that the user part of an "addr-spec" is in a non-intelligible form. The syntax for "other-param" is therefore refined to:

```
other-param     = (token | (token "=" (token | quoted-string))) 
                   | "private"
```

The "display-name" in Remote-Party-ID is a text string that identifies the account name of the party. The "addr-spec" contains information identifying the party either in clear-text or encrypted form. In the latter case, the "user" part of the "addr-spec" contains the encrypted party information, whereas the "hostport" identifies the entity that can decrypt the information. Furthermore, an "other-param" value of "private" will be present to indicate that the "addr-spec" is encrypted.

The following example illustrates this:

```
Remote-Party-ID: <sip: e(555-1212)@myproxy; private>
```

where e(x) indicates that x is encrypted.
identity delivery services, the value "na" may be provided.

The "rpi-type" token allows the SIP user agent to identify different types of callers which may be used to determine if special privileges should be extended to a given party. The string "operator" is a reserved identifier indicating that a telephony service provider operator is the remote party. The SIP user agent may for instance decide to honor a request for Busy-Line Verification or Emergency Interrupt by an operator; a request it might otherwise refuse.

As noted above, calling identity information must be trustworthy in order to be useful. In the absence of a trust relationship between all the proxies involved in a call, it must therefore be possible to add authenticity information to the Remote-Party-ID as well as specify who authenticated the information.

The "auth" token provides this function by authenticating everything in the Remote-Party-ID that precedes the "auth" token (up until but not including the semi-colon). The actual syntax and semantics depend on the authentication scheme used. Details on usage with pgp is specified later in this document.

Multiple "auth" tokens may be present which allows proxies to state that the Remote-Party-ID information provided is authentic without necessarily claiming that the identity of the remote party is correct. For example, a call between A and B where A is served by Proxy PA and B is served by Proxy PB might have the following Remote-Party-ID:

Remote-Party-ID: <sip:A@mynet.com;user=ip>;  
    auth=pgp signature="abc", signed-by="PA";  
    auth=pgp signature="xyz", signed-by="PB"

which implies that PA certifies that the call was originated by A, whereas PB certifies that PA certifies that the call was originated by A. Had PB trusted PA, then PB could instead have removed the "auth" token from PA, and simply have certified the information itself.

Finally, it should be noted, that when a proxy encrypts the Remote-Party-ID information, the proxy may choose to add additional "url-parameters" (in the form of "other-param") to the "addr-spec" to identify the encryption algorithm used as well as integrity checks for the "addr-spec". These parameters could be useful to the proxy when the "addr-spec" is used for a subsequent call, e.g. call return or call trace, however this would be internal to the proxy and is consequently not specified. This operation should not be confused with the authentication parameters specified above where the authenticating party, e.g. proxy, may differ from the verifying party, e.g. user agent.

4.1.1 Remote-Party-ID Authenticity with PGP
This section details the use of pgp for the rpi-token by refining the auth syntax as follows:

```
   rpi-auth     = "auth" "=" auth-scheme #auth-param
   auth-scheme  = "pgp"
   auth-param   = pgp-response
```

where pgp-response is defined in RFC 2543, Section 15.1.2.

An example was provided in the previous section.

### 4.2 PRIVACY

In support of privacy, the originator of a call must have a way of suppressing the delivery of calling identity information to the called party. One way of achieving that could simply be to omit the information from the Remote-Party-ID field. However, for DCS-proxy to DCS-proxy communication, where the information would still need to be passed, a presentation restriction indicator would then be needed.

Also, in order to maintain complete privacy in an IP environment, calling party IP-address information may have to be concealed from the terminating party as well. The cost and complexity of providing IP address level privacy rather than simply SIP level privacy is likely to differ enough to warrant two separate services. The calling party will thus need to signal the DCS-proxy which privacy service it is requesting.

We therefore propose to extend SIP with a new header field called Anonymity which allows an originating SIP user agent to indicate the degree of privacy that should be provided by the DCS proxy. The value "URI" requests the party’s identity not be provided to the destination. The value "Name" requests the calling name not be provided. The value "IPAddr" requests IP privacy such that the destination is not given the originator’s IP address. The value "Full" requests both URI and Name blocking and IP address privacy. The header field also allows a receiving SIP user agent to indicate its desire for privacy in its response to the first INVITE request.

```
   Anonymity       = "Anonymity" ":" *privacy-tag
   privacy-tag     = "Full" | "URI" | "Name" | "IPAddr" | "Off"
```

If privacy is requested, it MUST be one or more of "Full", "URI", "Name", or "IPAddr". The value "Off" indicates that no privacy is requested, and MUST be the only value if present.
4.3 Operator Services Call Processing

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 propose 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:

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

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 DCS-proxy.

4.4 Example of Use

In this Section, we will illustrate how the request for privacy may work in practice. It should be noted that the privacy service described can be implemented in a number of ways; we merely describe one possible solution in this section.

The Figure below illustrates a basic privacy example scenario.
Figure 1 - Basic Privacy Example

The originating user agent (MTA-o) sends an INVITE (1) message requesting URI and name privacy to DCS-proxy-o. DCS-proxy-o ensures that valid calling identity information is included in the message before it sends INVITE (2) to DCS-proxy-t, which in this case is trusted. DCS-proxy-t examines the Anonymity header field included in the INVITE and sees that URI and name privacy is requested. DCS-proxy-t therefore encrypts the "addr-spec" in the Remote-Party-ID, puts the result in the "user" part, inserts itself as the "hostport", and adds an "auth" parameter to the end, e.g. using a pgp signature. If MTA-t subscribes to caller-id, DCS-proxy-t also inserts "rpi-id=private" in the Remote-Party-ID. Finally, if a "display-name" was provided in the Remote-Party-ID, DCS-proxy-t simply removes it.

While this illustrates the basic operation of the service, there are additional issues that need to be considered. In SIP, there are additional fields that can reveal the identity of the calling party, either in part or completely. In the cases of calling name and calling number privacy, the "addr-spec", e.g. SIP-URL, as well as "display-name" part of the From header field may contain calling party information. This privacy problem can be overcome by having MTA-o supply a cryptographically random identifier for the userinfo, and a non-identifying hostname, e.g. "localhost". Also, when the session description protocol (SDP) is used to describe the media in the session, the use of SDP fields revealing calling identity information needs to be considered as well. Similar concerns apply to the use of RTCP.

The second example we look at is one where full privacy is requested, i.e. both calling name and number privacy, as well as IP address privacy. The Figure below illustrates how IP address privacy can be achieved by inserting a trusted intermediary, an anonymizer, for the media streams between MTA-o and MTA-t.
For all signaling and media exchange purposes, the anonymizer adds a level of indirection thereby hiding the IP address(es) of MTA-o from MTA-t. This indirection is used both for the media streams and SIP signaling, beyond the initial INVITE, exchanged directly between MTA-o and MTA-t.

Also, the following commonly used header fields may reveal privacy information, which can be remedied as described:

- The From header field must not reveal any calling identity information in the SIP-URL. This can be remedied, e.g. by supplying a cryptographically random identifier for the userinfo, and a non-identifying hostname, e.g. "localhost". The "display-name" must be anonymous.
- A Contact header field must be set to point to the anonymizer to prevent any direct signaling between MTA-o and MTA-t.
- Via header fields identifying either MTA-o or DCS-proxy-o must be hidden, e.g. by encryption or simple stateful removal and re-insertion by DCS-proxy-t.
- Call-ID should not be based on MTA-o’s IP-address.

Furthermore, when SDP is used to describe the media in the session, the session descriptions exchanged by the user agents need to be modified to direct the media streams to the anonymizer. Again, the use of SDP fields revealing calling identity information needs to be considered as well. Similar concerns apply to the use of RTCP.

5. Security Considerations

A user requesting complete privacy must still authenticate himself to the DCS-Proxy, and therefore the SIP messages between MTA-o and DCS-proxy-o must be protected. Likewise, it is necessary that the proxies take precautions to protect the user identification information from eavesdropping and interception. Use of IPSec between MTA and DCS-proxy as well as between proxies is recommended.

6. References

2. Bradner, S., "Key words for use in RFCs to Indicate Requirement
7. Acknowledgments

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, Ikhtlaq 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.

8. Author’s Addresses

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

K. K. Ramakrishnan  
AT&T  
Florham Park, NJ 07932  
Email: kkrama@research.att.com

Ed Miller  
CableLabs  
Louisville, CO 80027  
Email: E.Miller@Cablelabs.com

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

Burcak Beser  
3Com  
Rolling Meadows, IL 60008  
Email: Burcak_Beser@3com.com

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
Motorola
San Diego, CA  92121
Email: plalwaney@gi.com

Jon Fellows
Motorola
San Diego, CA  92121
Email: jfellows@gi.com

Doc Evans
Secure Cable Solutions

DCS Group
Internet Draft – Expiration 9/30/00
SIP Extensions for Caller Privacy
March 2000

Westminster, CO  30120
Email: drevans@securecable.com

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

"Copyright (C) The Internet Society (date). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

Expiration Date This memo is filed as <draft-dcsgroup-sip-privacy-01.txt>, and expires September 30, 2000.