          Private Extensions to the Session Initiation Protocol (SIP) for
                    Asserted Identity within Trusted Networks

Status of this Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

Abstract

   This document describes private extensions to the Session Initiation
   Protocol (SIP) that enable a network of trusted SIP servers to assert
   the identity of authenticated users, and the application of existing
   privacy mechanisms to the identity problem. The use of these
   extensions is only applicable inside an administrative domain with
   previously agreed-upon policies for generation, transport and usage
   of such information. This document does NOT offer a general privacy
   or identity model suitable for use between different trust domains,
   or use in the Internet at large.

Table of Contents

1. Applicability Statement

   This document describes private extensions to SIP [1] that enable a
   network of trusted SIP servers to assert the identity of end users or
   end systems, and to convey indications of end-user requested privacy.
   The use of these extensions is only applicable inside a 'Trust
   Domain' as defined in Short term requirements for Network Asserted
   Identity [5]. Nodes in such a Trust Domain are explicitly trusted by
   its users and end-systems to publicly assert the identity of each
   party, and to be responsible for withholding that identity outside of
   the Trust Domain when privacy is requested. The means by which the
   network determines the identity to assert is outside the scope of
   this document (though it commonly entails some form of
   authentication).

   A key requirement of [5] is that the behavior of all nodes within a
   given Trust Domain 'T' is known to comply to a certain set of
   specifications known as 'Spec(T)'. Spec(T) MUST specify behavior for
   the following:

   1. The manner in which users are authenticated

   2. The mechanisms used to secure the communication among nodes within
      the Trust Domain

   3. The mechanisms used to secure the communication between UAs and
      nodes within the Trust Domain

4. The manner used to determine which hosts are part of the Trust
   Domain

5. The default privacy handling when no Privacy header field is
   present

6. That nodes in the Trust Domain are compliant to SIP [1]

7. That nodes in the Trust Domain are compliant to this document

8. Privacy handling for identity as described in Section 7.

An example of a suitable Spec(T) is shown in Section 11.

This document does NOT offer a general privacy or identity model
suitable for inter-domain use or use in the Internet at large. Its
assumptions about the trust relationship between the user and the
network may not apply in many applications. For example, these
extensions do not accommodate a model whereby end users can
independently assert their identity by use of the extensions defined
here. Furthermore, since the asserted identities are not
cryptographically certified, they are subject to forgery, replay, and
falsification in any architecture that does not meet the requirements
of [5].

The asserted identities also lack an indication of who specifically
is asserting the identity, and so it must be assumed that the Trust
Domain is asserting the identity. Therefore, the information is only
meaningful when securely received from a node known to be a member of
the Trust Domain.

Despite these limitations, there are sufficiently useful specialized
deployments that meet the assumptions described above, and can accept
the limitations that result, to warrant informational publication of
this mechanism. An example deployment would be a closed network
which emulates a traditional circuit switched telephone network.

2. Conventions

   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 [3].

   Throughout this document requirements for or references to proxy
   servers or proxy behavior apply similarly to other intermediaries
   within a Trust Domain (ex: B2BUAs).

The terms Identity, Network Asserted Identity and Trust Domain in
this document have meanings as defined in [5].

3. Introduction

Various providers offering a telephony service over IP networks have
selected SIP as a call establishment protocol. Their environments
require a way for trusted network elements operated by the service
providers (for example SIP proxy servers) to communicate the identity
of the subscribers to such a service, yet also need to withhold this
information from entities that are not trusted when necessary. Such
networks typically assume some level of transitive trust amongst
providers and the devices they operate.

These networks need to support certain traditional telephony services
and meet basic regulatory and public safety requirements. These
include Calling Identity Delivery services, Calling Identity Delivery
Blocking, and the ability to trace the originator of a call. While
baseline SIP can support each of these services independently,
certain combinations cannot be supported without the extensions
described in this document. For example, a caller that wants to
maintain privacy and consequently provides limited information in the
SIP From header field will not be identifiable by recipients of the
call unless they rely on some other means to discover the identity of
the caller. Masking identity information at the originating user
agent will prevent certain services, e.g., call trace, from working
in the Public Switched Telephone Network (PSTN) or being performed at
intermediaries not privy to the authenticated identity of the user.

This document attempts to provide a network asserted identity service
using a very limited, simple mechanism, based on requirements in [5].
This work is derived from a previous attempt, [6], to solve several
problems related to privacy and identity in Trust Domains. A more
comprehensive mechanism, [7] which uses cryptography to address this
problem is the subject of current study by the SIP working group.

Providing privacy in a SIP network is more complicated than in the
PSTN. In SIP networks, the participants in a session are typically
able to exchange IP traffic directly without involving any SIP
service provider. The IP addresses used for these sessions may
themselves reveal private information. A general purpose mechanism
for providing privacy in a SIP environment is discussed in [2]. This
document applies that privacy mechanism to the problem of network
asserted identity.

4. Overview

   The mechanism proposed in this document relies on a new header field
   called 'P-Asserted-Identity' that contains a URI (commonly a SIP URI)
   and an optional display-name, for example:

       P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

   A proxy server which handles a message can, after authenticating the
   originating user in some way (for example: Digest authentication),
   insert such a P-Asserted-Identity header field into the message and
   forward it to other trusted proxies. A proxy that is about to
   forward a message to a proxy server or UA that it does not trust MUST
   remove all the P-Asserted-Identity header field values if the user
   requested that this information be kept private. Users can request
   this type of privacy as described in Section 7.

   The formal syntax for the P-Asserted-Identity header is presented in
   Section 9.

5. Proxy Behavior

   A proxy in a Trust Domain can receive a message from a node that it
   trusts, or a node that it does not trust. When a proxy receives a
   message from a node it does not trust and it wishes to add a P-
   Asserted-Identity header field, the proxy MUST authenticate the
   originator of the message, and use the identity which results from
   this authentication to insert a P-Asserted-Identity header field into
   the message.

   If the proxy receives a message (request or response) from a node
   that it trusts, it can use the information in the P-Asserted-Identity
   header field, if any, as if it had authenticated the user itself.

   If there is no P-Asserted-Identity header field present, a proxy MAY
   add one containing at most one SIP or SIPS URI, and at most one tel
   URL. If the proxy received the message from an element that it does
   not trust and there is a P-Asserted-Identity header present which
   contains a SIP or SIPS URI, the proxy MUST replace that SIP or SIPS
   URI with a single SIP or SIPS URI or remove this header field.
   Similarly, if the proxy received the message from an element that it
   does not trust and there is a P-Asserted-Identity header present
   which contains a tel URI, the proxy MUST replace that tel URI with a
   single tel URI or remove the header field.

   When a proxy forwards a message to another node, it must first
   determine if it trusts that node or not. If it trusts the node, the
   proxy does not remove any P-Asserted-Identity header fields that it

generated itself, or that it received from a trusted source. If it
does not trust the element, then the proxy MUST examine the Privacy
header field (if present) to determine if the user requested that
asserted identity information be kept private.

6. Hints for Multiple Identities

If a P-Preferred-Identity header field is present in the message that
a proxy receives from an entity that it does not trust, the proxy MAY
use this information as a hint suggesting which of multiple valid
identities for the authenticated user should be asserted. If such a
hint does not correspond to any valid identity known to the proxy for
that user, the proxy can add a P-Asserted-Identity header of its own
construction, or it can reject the request (for example, with a 403
Forbidden). The proxy MUST remove the user-provided P-Preferred-
Identity header from any message it forwards.

A user agent only sends a P-Preferred-Identity header field to proxy
servers in a Trust Domain; user agents MUST NOT populate the P-
Preferred-Identity header field in a message that is not sent
directly to a proxy that is trusted by the user agent. Were a user
agent to send a message containing a P-Preferred-Identity header
field to a node outside a Trust Domain, then the hinted identity
might not be managed appropriately by the network, which could have
negative ramifications for privacy.

7. Requesting Privacy

Parties who wish to request the removal of P-Asserted-Identity header
fields before they are transmitted to an element that is not trusted
may add the "id" privacy token defined in this document to the
Privacy header field. The Privacy header field is defined in [6].
If this token is present, proxies MUST remove all the P-Asserted-
Identity header fields before forwarding messages to elements that
are not trusted. If the Privacy header field value is set to "none"
then the proxy MUST NOT remove the P-Asserted-Identity header fields.

When a proxy is forwarding the request to an element that is not
trusted and there is no Privacy header field, the proxy MAY include
the P-Asserted-Identity header field or it MAY remove it. This
decision is a policy matter of the Trust Domain and MUST be specified
in Spec(T). It is RECOMMENDED that the P-Asserted-Identity header
fields SHOULD NOT be removed unless local privacy policies prevent
it, because removal may cause services based on Asserted Identity to
fail.

However, it should be noted that unless all users of the Trust Domain
have access to appropriate privacy services, forwarding of the P-
Asserted-Identity may result in disclosure of information which the
user has not requested and cannot prevent. It is therefore STRONGLY
RECOMMENDED that all users have access to privacy services as
described in this document.

Formal specification of the "id" Privacy header priv-value is
described in Section 9.3. Some general guidelines for when users
require privacy are given in [2].

If multiple P-Asserted-Identity header field values are present in a
message, and privacy of the P-Asserted-Identity header field is
requested, then all instances of the header field values MUST be
removed before forwarding the request to an entity that is not
trusted.

8. User Agent Server Behavior

Typically, a user agent renders the value of a P-Asserted-Identity
header field that it receives to its user. It may consider the
identity provided by a Trust Domain to be privileged, or
intrinsically more trustworthy than the From header field of a
request. However, any specific behavior is specific to
implementations or services. This document also does not mandate any
user agent handling for multiple P-Asserted-Identity header field
values that happen to appear in a message (such as a SIP URI
alongside a tel URL).

However, if a User Agent Server receives a message from a previous
element that it does not trust, it MUST NOT use the P-Asserted-
Identity header field in any way.

If a UA is part of the Trust Domain from which it received a message
containing a P-Asserted-Identity header field, then it can use the
value freely but it MUST ensure that it does not forward the
information to any element that is not part of the Trust Domain, if
the user has requested that asserted identity information be kept
private.

If a UA is not part of the Trust Domain from which it received a
message containing a P-Asserted-Identity header field, then it can
assume this information does not need to be kept private.

9. Formal Syntax

The following syntax specification uses the augmented Backus-Naur
Form (BNF) as described in RFC-2234 [4].

9.1 The P-Asserted-Identity Header

   The P-Asserted-Identity header field is used among trusted SIP
   entities (typically intermediaries) to carry the identity of the user
   sending a SIP message as it was verified by authentication.

      PAssertedID = "P-Asserted-Identity" HCOLON PAssertedID-value
                     *(COMMA PAssertedID-value)
      PAssertedID-value = name-addr / addr-spec

   A P-Asserted-Identity header field value MUST consist of exactly one
   name-addr or addr-spec. There may be one or two P-Asserted-Identity
   values. If there is one value, it MUST be a sip, sips, or tel URI.
   If there are two values, one value MUST be a sip or sips URI and the
   other MUST be a tel URI. It is worth noting that proxies can (and
   will) add and remove this header field.

   This document adds the following entry to Table 2 of [1]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-Asserted-Identity	adr		-	o	-	o	o	-

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

9.2 The P-Preferred-Identity Header

   The P-Preferred-Identity header field is used from a user agent to a
   trusted proxy to carry the identity the user sending the SIP message
   wishes to be used for the P-Asserted-Header field value that the
   trusted element will insert.

      PPreferredID = "P-Preferred-Identity" HCOLON PPreferredID-value
                     *(COMMA PPreferredID-value)
      PPreferredID-value = name-addr / addr-spec

   A P-Preferred-Identity header field value MUST consist of exactly one
   name-addr or addr-spec. There may be one or two P-Preferred-Identity
   values. If there is one value, it MUST be a sip, sips, or tel URI.
   If there are two values, one value MUST be a sip or sips URI and the
   other MUST be a tel URI. It is worth noting that proxies can (and
   will) remove this header field.

This document adds the following entry to Table 2 of [1]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
P-Preferred-Identity	adr		-	o	-	o	o	-

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

9.3 The "id" Privacy Type

   This specification adds a new privacy type ("priv-value") to the
   Privacy header, defined in [2]. The presence of this privacy type in
   a Privacy header field indicates that the user would like the Network
   Asserted Identity to be kept private with respect to SIP entities
   outside the Trust Domain with which the user authenticated. Note
   that a user requesting multiple types of privacy MUST include all of
   the requested privacy types in its Privacy header field value.

      priv-value = "id"

   Example:

           Privacy: id

10. Examples

10.1 Network Asserted Identity passed to trusted gateway

   In this example, proxy.cisco.com creates a P-Asserted-Identity header
   field from an identity it discovered from SIP Digest authentication.
   It forwards this information to a trusted proxy which forwards it to
   a trusted gateway. Note that these examples consist of partial SIP
   messages that illustrate only those headers relevant to the
   authenticated identity problem.

   * F1   useragent.cisco.com -> proxy.cisco.com

   INVITE sip:+14085551212@cisco.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Max-Forwards: 70
   Privacy: id

```
   * F2   proxy.cisco.com -> useragent.cisco.com

   SIP/2.0 407 Proxy Authorization
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
   To: <sip:+14085551212@cisco.com>;tag=123456
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Proxy-Authenticate: .... realm="sip.cisco.com"

   * F3   useragent.cisco.com -> proxy.cisco.com

   INVITE sip:+14085551212@cisco.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 70
   Privacy: id
   Proxy-Authorization: .... realm="sip.cisco.com" user="fluffy"

   * F4   proxy.cisco.com -> proxy.pstn.net (trusted)

   INVITE sip:+14085551212@proxy.pstn.net SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 69
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   P-Asserted-Identity: tel:+14085264000
   Privacy: id
```

```
   * F5   proxy.pstn.net -> gw.pstn.net (trusted)

   INVITE sip:+14085551212@gw.pstn.net SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
   Via: SIP/2.0/TCP proxy.pstn.net;branch=z9hG4bK-a1b2
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 68
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   P-Asserted-Identity: tel:+14085264000
   Privacy: id
```

10.2 Network Asserted Identity Withheld

   In this example, the User Agent sends an INVITE that indicates it
   would prefer the identity sip:fluffy@cisco.com to the first proxy,
   which authenticates this with SIP Digest. The first proxy creates a
   P-Asserted-Identity header field and forwards it to a trusted proxy
   (outbound.cisco.com). The next proxy removes the P-Asserted-Identity
   header field and the request for Privacy before forwarding this
   request onward to the biloxi.com proxy server which it does not
   trust.

```
   * F1    useragent.cisco.com -> proxy.cisco.com

   INVITE sip:bob@biloxi.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Max-Forwards: 70
   Privacy: id
   P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

   * F2    proxy.cisco.com -> useragent.cisco.com
   SIP/2.0 407 Proxy Authorization
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
   To: <sip:bob@biloxi.com>;tag=123456
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Proxy-Authenticate: .... realm="cisco.com"
```

```
   * F3    useragent.cisco.com -> proxy.cisco.com

   INVITE sip:bob@biloxi.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 70
   Privacy: id
   P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   Proxy-Authorization: .... realm="cisco.com" user="fluffy"

   * F4    proxy.cisco.com -> outbound.cisco.com (trusted)

   INVITE sip:bob@biloxi SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 69
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@vovida.org>
   Privacy: id

   * F5   outbound.cisco.com -> proxy.biloxi.com (not trusted)

   INVITE sip:bob@biloxi SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
   Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 68
   Privacy: id
```

```
* F6   proxy.biloxi.com -> bobster.biloxi.com

INVITE sip:bob@bobster.biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
Via: SIP/2.0/TCP proxy.biloxi.com;branch=z9hG4bK-d456
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 67
Privacy: id
```

11. Example of Spec(T)

   The integrity of the mechanism described in this document relies on
   one node knowing (through configuration) that all of the nodes in a
   Trust Domain will behave in a predetermined way. This requires the
   predetermined behavior to be clearly defined and for all nodes in the
   Trust Domain to be compliant. The specification set that all nodes
   in a Trust Domain T must comply with is termed 'Spec(T)'.

   The remainder of this section presents an example Spec(T), which is
   not normative in any way.

      1. Protocol requirements

         The following specifications MUST be supported:

         1. RFC 3261

         2. RFC 3325

      2. Authentication requirements

         Users MUST be authenticated using SIP Digest Authentication.

      3. Security requirements

         Connections between nodes within the Trust Domain and between
         UAs and nodes in the Trust Domain MUST use TLS using a cipher
         suite of RSA_WITH_AES_128_CBC_SHA1. Mutual authentication
         between nodes in the trust domain MUST be performed and
         confidentiality MUST be negotiated.

   4. Scope of Trust Domain

      The Trust Domain specified in this agreement consists of hosts
      which posses a valid certificate which is a) signed by
      examplerootca.org; b) whose subjectAltName ends with one of the
      following domain names: trusted.div1.carrier-a.net,
      trusted.div2.carrier-a.net, sip.carrier-b.com; and c) whose
      domain name corresponds to the hostname in the subjectAltName
      in the certificate.

   5. Implicit handling when no Privacy header is present

      The elements in the trust domain must support the 'id' privacy
      service therefore absence of a Privacy header can be assumed to
      indicate that the user is not requesting any privacy. If no
      Privacy header field is present in a request, elements in this
      Trust Domain MUST act as if no privacy is requested.

12. Security Considerations

   The mechanism provided in this document is a partial consideration of
   the problem of identity and privacy in SIP. For example, these
   mechanisms provide no means by which end users can securely share
   identity information end-to-end without a trusted service provider.
   Identity information that the user designates as 'private' can be
   inspected by any intermediaries participating in the Trust Domain.
   This information is secured by transitive trust, which is only as
   reliable as the weakest link in the chain of trust.

   When a trusted entity sends a message to any destination with that
   party's identity in a P-Asserted-Identity header field, the entity
   MUST take precautions to protect the identity information from
   eavesdropping and interception to protect the confidentiality and
   integrity of that identity information. The use of transport or
   network layer hop-by-hop security mechanisms, such as TLS or IPSec
   with appropriate cipher suites, can satisfy this requirement.

13. IANA Considerations

13.1 Registration of new SIP header fields

   This document defines two new private SIP header fields, "P-
   Asserted-Identity" and "P-Preferred-Identity". As recommended by the
   policy of the Transport Area, these headers have been registered by
   the IANA in the SIP header registry, using the RFC number of this
   document as its reference.

    Name of Header: P-Asserted-Identity

    Short form: none

    Registrant: Cullen Jennings
                                fluffy@cisco.com

    Normative description:
    Section 9.1 of this document

    Name of Header: P-Preferred-Identity

    Short form: none

    Registrant: Cullen Jennings
                                fluffy@cisco.com

    Normative description:
    Section 9.2 of this document

13.2 Registration of "id" privacy type for SIP Privacy header

    Name of privacy type: id

    Short Description: Privacy requested for Third-Party Asserted
                             Identity

    Registrant: Cullen Jennings
                             fluffy@cisco.com

    Normative description:
    Section 9.3 of this document

14. Acknowledgements

    Thanks to Bill Marshall and Flemming Andreason [6], Mark Watson [5],
    and Jon Peterson [7] for authoring drafts which represent the bulk of
    the text making up this document. Thanks to many people for useful
    comments including Jonathan Rosenberg, Rohan Mahy and Paul Kyzivat.

Normative References

    [1] 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.

    [2] Peterson, J., "A Privacy Mechanism for the Session Initiation
        Protocol (SIP)", RFC 3323, November 2002.

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

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

Informational References

   [5] Watson, M., "Short Term Requirements for Network Asserted
       Identity", RFC 3324, November 2002.

   [6] Andreasen, F., "SIP Extensions for Network-Asserted Caller
       Identity and Privacy within Trusted Networks", Work in Progress.

   [7] Peterson, J., "Enhancements for Authenticated Identity Management
       in the Session Initiation Protocol (SIP)", Work in Progress.

Authors' Addresses

   Cullen Jennings
   Cisco Systems
   170 West Tasman Drive
   MS: SJC-21/3
   San Jose, CA 95134
   USA

   Phone: +1 408 527-9132
   EMail: fluffy@cisco.com

   Jon Peterson
   NeuStar, Inc.
   1800 Sutter Street, Suite 570
   Concord, CA 94520
   USA

   Phone: +1 925/363-8720
   EMail: Jon.Peterson@NeuStar.biz

   Mark Watson
   Nortel Networks
   Maidenhead Office Park (Bray House)
   Westacott Way
   Maidenhead, Berkshire
   England

   Phone: +44 (0)1628-434456
   EMail: mwatson@nortelnetworks.com

Full Copyright Statement

Acknowledgement