

Short Term Requirements for Network Asserted Identity

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

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

A Network Asserted Identity is an identity initially derived by a Session Initiation Protocol (SIP) network intermediary as a result of an authentication process. This document describes short term requirements for the exchange of Network Asserted Identities within networks of securely interconnected trusted nodes and to User Agents securely connected to such networks.

There is no requirement for identities asserted by a UA in a SIP message to be anything other than the user's desired alias.

Table of Contents

1.	Introduction	2
2.	Definitions	3
2.1	Identity	3
2.2	Network Asserted Identity	3
2.3	Trust Domains	4
2.4	Spec(T)	7
3.	Generation of Network Asserted Identity	7
4.	Transport of Network Asserted Identity	7
4.1	Sending of Networks Asserted Identity within a Trust Domain	7
4.2	Receiving of Network Asserted Identity within a Trust Domain	7
4.3	Sending of Network Asserted Identity to entities outside a Trust Domain	7
4.4	Receiving of Network Asserted Identity by a node outside the Trust Domain	8
5.	Parties with Network Asserted Identities	8
6.	Types of Network Asserted Identity	8
7.	Privacy of Network Asserted Identity	9
8.	Security Considerations	9
9.	IANA Considerations	10
10.	Acknowledgments	10
	Normative References	10
	Author's Address	10
	Full Copyright Statement	11

1. Introduction

SIP [1] allows users to assert their identity in a number of ways e.g., using the From: header. However, there is no requirement for these identities to be anything other than the users desired alias.

An authenticated identity of a user can be obtained using SIP Digest Authentication (or by other means). However, UAs do not always have the necessary key information to authenticate another UA.

A Network Asserted Identity is an identity initially derived by a SIP network intermediary as a result of an authentication process. This may or may not be based on SIP Digest authentication. This document describes short term requirements for the exchange of Network Asserted Identities within networks of securely interconnected trusted nodes and also to User Agents with secure connections to such networks.

Such a network is described in this document as a Trust Domain and we present a strict definition of trust and Trust Domain for the purposes of this document. These short-term requirements provide only for the exchange of Network Asserted Identity within a Trust Domain and to an entity directly connected to the trust domain.

General requirements for transport of Network Asserted Identities on the Internet are out of scope of this document.

2. Definitions

2.1 Identity

An Identity, for the purposes of this document, is a sip:, sips: or tel: URI, and optionally a Display Name.

The URI MUST be meaningful to the domain identified in the URI (in the case of sip: or sips: URIs) or the owner of the E.164 number (in the case of tel: URIs), in the sense that when used as a SIP Request-URI in a request sent to that domain/number range owner, it would cause the request to be routed to the user/line that is associated with the identity, or to be processed by service logic running on that user's behalf.

If the URI is a sip: or sips: URI, then depending on the local policy of the domain identified in the URI, the URI MAY identify some specific entity, such as a person.

If the URI is a tel: URI, then depending on the local policy of the owner of the number range within which the telephone number lies, the number MAY identify some specific entity, such as a telephone line. However, it should be noted that identifying the owner of the number range is a less straightforward process than identifying the domain which owns a sip: or sips: URI.

2.2 Network Asserted Identity

A Network Asserted Identity is an identity derived by a SIP network entity as a result of an authentication process, which identifies the authenticated entity in the sense defined in Section 2.1.

In the case of a sip: or sips: URI, the domain included in the URI MUST be within the Trust Domain.

In the case of a tel: URI, the owner of the E.164 number in the URI MUST be within the Trust Domain.

The authentication process used, or at least it's reliability/strength, is a known feature of the Trust Domain using the Network Asserted Identity mechanism i.e., in the language of 2.3 below, it is defined in Spec(T).

2.3 Trust Domains

A Trust Domain for the purposes of Network Asserted Identity is a set of SIP nodes (UAC, UAS, proxies or other network intermediaries) that are trusted to exchange Network Asserted Identity information in the sense described below.

A node can be a member of a Trust Domain, T, only if the node is known to be compliant to a certain set of specifications, Spec(T), which characterize the handling of Network Asserted Identity within the Trust Domain, T.

Trust Domains are constructed by human beings who know the properties of the equipment they are using/deploying. In the simplest case, a Trust Domain is a set of devices with a single owner/operator who can accurately know the behaviour of those devices.

Such simple Trust Domains may be joined into larger Trust Domains by bi-lateral agreements between the owners/operators of the devices.

We say a node is 'trusted' (with respect to a given Trust Domain) if and only if it is a member of that domain.

We say that a node, A, in the domain is 'trusted by' a node, B, (or 'B trusts A') if and only if:

1. there is a secure connection between the nodes, AND
2. B has configuration information indicating that A is a member of the Trust Domain.

Note that B may or may not be a member of the Trust Domain. For example, B may be a UA which trusts a given network intermediary, A (e.g., its home proxy).

A 'secure connection' in this context means that messages cannot be read by third parties, cannot be modified by third parties without detection and that B can be sure that the message really did come from A. The level of security required is a feature of the Trust Domain i.e., it is defined in Spec(T).

Within this context, SIP signaling information received by one node FROM a node that it trusts is known to have been generated and passed through the network according to the procedures of the particular specification set Spec(T), and therefore can be known to be valid, or at least as valid as specified in the specifications Spec(T).

Equally, a node can be sure that signaling information passed TO a node that it trusts will be handled according to the procedures of Spec(T).

For these capabilities to be useful, Spec(T) must contain requirements as to how the Network Asserted Identity is generated, how its privacy is protected and how its integrity is maintained as it is passed around the network. A reader of Spec(T) can then make an informed judgement about the authenticity and reliability of Network Asserted Information received from the Trust Domain T.

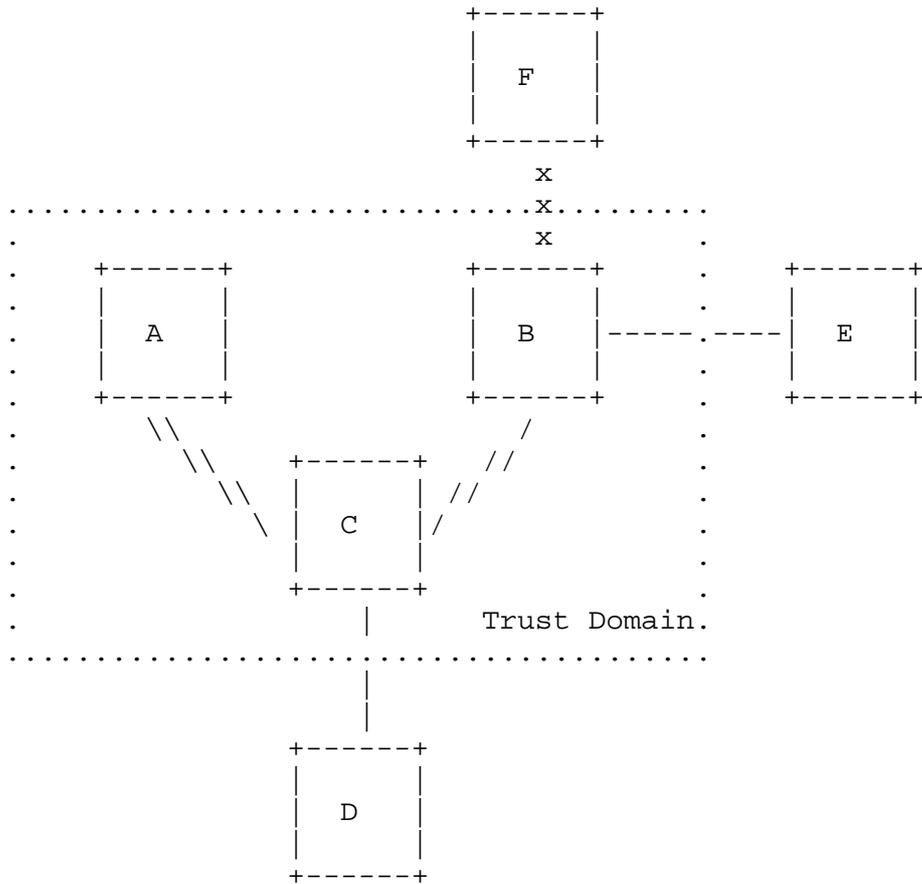
The term 'trusted' (with respect to a given Trust Domain) can be applied to a given node in an absolute sense - it is just equivalent to saying the node is a member of the Trust Domain. However, the node itself does not know whether another arbitrary node is 'trusted', even within the Trust Domain. It does know about certain nodes with which it has secure connections as described above.

With the definition above, statements such as 'A trusted node SHALL ...' are just shorthand for 'A node compliant to this specification SHALL...'.

Statements such as 'When a node receives information from a trusted node...' are NOT valid, because one node does not have complete knowledge about all the other nodes in the trust domain.

Statements such as 'When a node receives information from another node that it trusts...' ARE valid, and should be interpreted according to the criteria (1) and (2) above.

The above relationships are illustrated in the following figure:



xxxxxxx Insecure connection
 ----- Secure connection

.....
 . All boxes within the dotted line
are part of the same Trust Domain

- o A, B and C are part of the same trust domain
- o A trusts C, but A does not trust B
- o since E knows that B is inside of the trust domain, E trusts B, but B does not trust E
- o B does not trust F, F does not trust B

2.4 Spec(T)

An aspect of the definition of a trust domain is that all the elements in that domain are compliant to a set of configurations and specifications generally referred to as Spec(T). Spec(T) is not a specification in the sense of a written document; rather, its an agreed upon set of information that all elements are aware of. Proper processing of the asserted identities requires that the elements know what is actually being asserted, how it was determined, and what the privacy policies are. All of that information is characterized by Spec(T).

3. Generation of Networks Asserted Identity

A Network Asserted Identity is generated by a network intermediary following an Authentication process which authenticates the entity (UA) to be identified.

The Authentication process(es) used are a characteristic feature of the Trust Domain, and MUST be specified in Spec(T).

It shall be possible for a UA to provide a preferred identity to the network intermediary, which MAY be used to inform the generation of the Network Asserted Identity according to the policies of the Trust Domain.

4. Transport of Network Asserted Identity

4.1 Sending of Networks Asserted Identity within a Trust Domain

It shall be possible for one node within a Trust Domain to securely send a Network Asserted Identity to another node that it trusts.

4.2 Receiving of Network Asserted Identity within a Trust Domain

It shall be possible for one node within a Trust Domain to receive a Network Asserted identity from another node that it trusts.

4.3 Sending of Network Asserted Identity to entities outside a Trust Domain

If a node, A, within the Trust Domain, is trusted by a node, B, outside the Trust Domain, then it shall be possible for A to securely send a Network Asserted Identity to B, if allowed by the privacy policies of the user that has been identified, and the trust domain.

This is most often used to pass a Network Asserted Identity directly to a UA.

4.4 Receiving of Network Asserted Identity by a node outside the Trust Domain

It shall be possible for a node outside the Trust Domain to receive a Network Asserted Identity from a node that it trusts.

Network Asserted Identity received in this way may be considered valid, and used for display to the user, input data for services etc.

Network Asserted Identity information received by one node from a node which it does not trust carries no guarantee of authenticity or integrity because it is not known that the procedures of Spec(T) were followed to generate and transport the information. Such information MUST NOT be used. (i.e., it shall not be displayed to the user, passed to other nodes, used as input data for services, etc.)

5. Parties with Network Asserted Identities

A Network Asserted Identity identifies the originator of the message in which it was received.

For example,

a Network Asserted Identity received in an initial INVITE (outside the context of any existing dialog) identifies the calling party.

a Network Asserted Identity received in a 180 Ringing response to such an INVITE identifies the party who is ringing.

a Network Asserted Identity received in a 200 response to such an INVITE identifies the party who has answered.

6. Types of Network Asserted Identity

It shall be possible to assert multiple identities associated with a given party (in a given message), provided that these are of distinct types.

The types of identity supported shall be sip:, sips: and tel: URIs, all of which identify the user as described in Section 2.1. It is not required to transport both a sip: and sips: URI.

It shall be possible for the capability to transport additional types of identity associated with a single party to be introduced in future.

7. Privacy of Network Asserted Identity

The means by which any privacy requirements in respect of the Network Asserted Identity are determined are outside the scope of this document.

It shall be possible to indicate within a message containing a Network Asserted Identity that this Network Asserted Identity is subject to a privacy requirement which prevents it being passed to other users. This indication should not carry any semantics as to the reason for this privacy requirement.

It shall be possible to indicate that the user has requested that the Network Asserted Identity be not passed to other users. This is distinct from the above indication, in that it implies specific user intent with respect to the Network Asserted Identity.

The mechanism shall support Trust Domain policies where the above two indications are equivalent (i.e., the only possible reason for a privacy requirement is a request from the user), and policies where they are not.

In this case, the Network Asserted Identity specification shall require that the mechanism of Section 4.3 SHALL NOT be used i.e., a trusted node shall not pass the identity to a node it does not trust. However, the mechanism of Section 4.3 MAY be used to transfer the identity within the trusted network.

Note that 'anonymity' requests from users or subscribers may well require functionality in addition to the above handling of Network Asserted Identities. Such additional functionality is out of the scope of this document.

8. Security Considerations

The requirements in this document are NOT intended to result in a mechanism with general applicability between arbitrary hosts on the Internet.

Rather, the intention is to state requirements for a mechanism to be used within a community of devices which are known to obey the specification of the mechanism (Spec(T)) and between which there are secure connections. Such a community is known here as a Trust Domain.

The requirements on the mechanisms used for security and to initially derive the Network Asserted Identity must be part of the specification Spec(T).

The requirements also support the transfer of information from a node within the Trust Domain, via a secure connection to a node outside the Trust Domain.

Use of this mechanism in any other context has serious security shortcomings, namely that there is absolutely no guarantee that the information has not been modified, or was even correct in the first place.

9. IANA Considerations

This document does not have any implications for IANA.

10. Acknowledgments

Thanks are due to Jon Peterson, Cullen Jennings, Allison Mankin and Jonathan Rosenberg for comments on this document.

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.

Author's Address

Mark Watson
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead, BERKS SL6 3QH
UK

EMail: mwatson@nortelnetworks.com

Full Copyright Statement

Copyright (C) The Internet Society (2002). 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.

Acknowledgement

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

