

Internet Draft
Document: [draft-ietf-sipping-nai-reqs-00.txt](#)

Mark
Nortel Ne

Category: Informational
Expires November 2002

Ma

Short term requirements for Network Asserted Identity

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

There is no requirement for identities asserted by a SIP message to be anything other than the user's desired authenticated identity of a user can be obtained using SIP Digest authentication, however it is unlikely that the necessary Public Key Infrastructure to facilitate this for UAs will be available soon.

A Network Asserted Identity is an identity initially derived from a network intermediary as a result of an authentication process. This draft 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.

General requirements for transport of Network Asserted Identities over the Internet are out of scope of this draft.

Table of Contents

1.	Introduction.....	
2.	Definitions.....	
2.1	Identity.....	

Network Asserted Identity û short term requirements

Ma

- [2.2](#) Network Asserted Identity.....
- [2.3](#) Trust Domains.....
- [3.](#) Generation of Network Asserted Identity.....
- [4.](#) Transport of Network Asserted Identity.....
 - 4.1 Sending of Network Asserted Identity within a Trust Do
 - [4.2](#) Receiving of Network Asserted Identity withing a Trust
 -
 - 4.3 Sending of Network Asserted Identity to entities outsi
 - Trust Domain.....
 - 4.4 Receiving of Network Asserted Identity by a node outsi
 - Trust Domain.....
- [5.](#) Parties with Network Asserted Identities.....
- [6.](#) Types of Network Asserted Identity.....
- [7.](#) Privacy of Network Asserted Identity.....
- [8.](#) Next steps.....
- [9.](#) Security considerations.....
- [10.](#) IANA Considerations.....
- [11.](#) References.....
- [12.](#) Acknowledgments.....
- [13.](#) AuthorsÆ Addresses.....
- [14.](#) Full Copyright Statement.....

[1.](#) Introduction

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

An authenticated identity of a user can be obtained using SIP Authentication (or by other means). However, it is unlikely t necessary Public Key Infrastructure to globally facilitate th users will be available soon.

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

Such a network is described in this draft as a Trust Domain and present a strict definition of trust and Trust Domain for the purposes of this draft. These short-term requirements provide for the exchange of Network Asserted Identity within a Trust Domain.

Network Asserted Identity - short term requirements

Ma

General requirements for transport of Network Asserted Identity on the Internet are out of scope of this draft.

[2. Definitions](#)

[2.1 Identity](#)

An Identity, for the purposes of this draft, is a URI, and optionally a Display Name. The URI MUST be meaningful to the domain identified in the URI when used as a SIP Request-URI.

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 is a number MAY identify some specific entity, such as a telephone number. However, it should be noted that identifying the owner of the number range is a less straightforward process than identifying the entity which owns a sip: or sips: URI.

[2.2 Network Asserted Identity](#)

A Network Asserted Identity is an identity derived by a SIP endpoint entity as a result of an authentication process.

The authentication process used, or at least its reliability/strength, is a known feature of the Trust Domain in which the Network Asserted Identity mechanism i.e. in the language defined below, it is defined in Spec(T).

[2.3 Trust Domains](#)

A Trust Domain for the purposes of Network Asserted Identity

of SIP nodes (UAC, UAS, proxies or other network intermediaries) 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 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 accurately know the behaviour of those devices.

Watson

Expires - November 2002

[Page

Network Asserted Identity - short term requirements

Ma

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

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

We say that one node in the domain is *trusted by* another if and only if:

- (i) there is a secure connection between the nodes, AND
- (ii) they have configuration information to indicate that they are members of the same Trust Domain.

This most often applies to network intermediaries such as proxies within the Trust Domain.

A *secure connection* in this context means that messages cannot be read by third parties and cannot be modified or inserted by third parties without detection. The level of security required is a feature of the Trust Domain i.e. it is defined in Spec(T).

We say that a node, A, in the domain is *trusted by* a node, B, outside the domain if and only if:

- (i) there is a secure connection between the nodes, AND
- (ii) B has configuration information indicating that A is a member of the Trust Domain.

This most often applies to a UA which trusts a given network intermediary (e.g. its home proxy).

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, a node itself does not know whether another arbitrary node is "trusted" even within the Trust Domain. It does know about certain nodes 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 a node that it trusts..." ARE valid, and should be interpreted according to the criteria (i) and (ii) above.

Watson

Expires - November 2002

[Page

Network Asserted Identity - short term requirements

Ma

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 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 the Network Asserted Information received from the Trust Domain T.

3. Generation of Network Asserted Identity

A Network Asserted Identity is generated by a network intermediary

following an Authentication process which authenticates the e (UA) to be identified.

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

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

[4. Transport of Network Asserted Identity](#)

[4.1 Sending of Network Asserted Identity within a Trust Domain](#)

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

[4.2 Receiving of Network Asserted Identity withing a Trust Domain](#)

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

[4.3 Sending of Network Asserted Identity to entities outside a T Domain](#)

It shall be possible for a node within the Trust Domain to se send a Network Asserted Identity to a node outside the trust

Watson

Expires - November 2002

[Pa

Network Asserted Identity û short term requirements

Ma

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

[4.4 Receiving of Network Asserted Identity by a node outside the Domain](#)

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

Network Asserted Identity received in this way may be consid valid, and used for display to the user, input data for servi

Network Asserted Identity information received by one node fr

node which it does not trust carries no guarantee of authentication integrity because it is not known that the procedures of Specification were followed to generate and transport the information. Such information MUST NOT be used. i.e. it shall not be displayed to the user, nor 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,

- o a Network Asserted Identity received in an initial INVITE (outside the context of any existing dialog) identifies the calling party.
- o a Network Asserted Identity received in a 180 Ringing response to such an INVITE identifies the party who is ringing.
- o a Network Asserted Identity received in a 200 response to an INVITE identifies the party who has answered.

6. Types of Network Asserted Identity

Each party shall have at most one Network Asserted Identity.

It shall be possible for the capability to transport multiple identities associated with a single party to be introduced in the future.

7. Privacy of Network Asserted Identity

Watson

Expires - November 2002

[Page 10]

Network Asserted Identity - short term requirements

Ma

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 that a Network Asserted Identity is subject to a privacy requirement which prevents it being passed to other users.

In this case, the Network Asserted Identity specification shall require that the mechanism of 3.2 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 3.1 MAY be used to transfer the identity within the trusted network.

It shall be possible to indicate whether the Network Asserted Identity is private due to a request from the user/subscriber or another reason.

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

8. Next steps

It is proposed to use [draft-jennings-sipping-nai-00](#) [2] to implement the requirements of this draft.

9. Security considerations

The requirements in this draft 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 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 implement derive the Network Asserted Identity must be part of the specification Spec(T).

Such devices may be hosts on the Internet.

The requirements also support the transfer of information from 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.

10. IANA Considerations

This document does not have any implications for IANA.

11. References

[1] J. Rosenberg et al, "SIP: Session initiation protocol," [draft-ietf-sip-rfc2543bis-09.txt](#), February 27th, 2002.

[2] C.Jennings, "Network Asserted Identity header," [draft-jennings-sipping-nai-00](#), May 2002, work in progress.

12. Acknowledgments

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

13. Authors' Addresses

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

Tel: +44 (0)1628-434456
Email: mwatson@nortelnetworks.com.

14. 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 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, the document itself may not be modified in any way, such as by rewording 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

Network Asserted Identity û short term requirements

Ma

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."

Watson

Expires - November 2002

[Pa