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

Abstract

There is no requirement for identities identities asserted by
a SIP message to be anything other than the userÆs desired al
authenticated identity of a user can be obtained using SIP Di
authentication, however it is unlikely that the necessary Pub
Infrastructure to facilitate this for UAs will be available s

A Network Asserted Identity is an identity initially derived
network intermediary as a result of an authentication process
draft describes short term requirements for the exchange of N
Asserted Identities within networks of securely interconnecte
trusted nodes and to User Agents securely connected to such n

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

Table of Contents

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 a 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 Identitied within a Trus Domain.

General requirements for transport of Network Asserted Identi 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 op a Display Name. The URI MUST be meaningful to the domain iden in the URI when used as a SIP Request-URI.

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

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

2.2 Network Asserted Identity

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

The authentication process used, or at least itÆs reliability/strength, is a known feature of the Trust Domain the Network Asserted Identity mechanism i.e. in the language 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 intermediari
are trusted to exchange Network Asserted Identity informatio
sense described below.

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

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

Such simple Trust Domains may be joined into larger Trust Dom
bi-lateral agreements between the owners/operators of the dev

We say a node is ætrustedÆ (with respect to a given Trust Dom
and only if it is a member of that domain.

We say that one node in the domain is ætrusted byÆ another if
only if:

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

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

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

We say that a node, A, in the domain is ætrusted byÆ a node,
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 m
the Trust Domain.

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

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

With the definition above, statements such as æA trusted node
...Æ are just shorthand for æA node compliant to this specifi
SHALL...Æ.

Statements such as æWhen a node receives information from a t
node...Æ are NOT valid, because one node does not have comple
knowledge about all the other nodes in the trust domain.

Statements such as æWhen a node receives information from ano
node that it trusts...Æ ARE valid, and should be interpreted
according to the criteria (i) and (ii) above.

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

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

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

3. Generation of Network Asserted Identity

A Network Asserted Identity is generated by a network interme

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 prefered 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 trus

4.2 Receiving of Network Asserted Identity withing a Trust Domai

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

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 conside
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 authenti
integrity because it is not known that the procedures of Spec
followed to generate and transport the information. Such info
MUST NOT be used. i.e. it shall not be displayed to the user,
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
in which it was received.

For example,

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

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

- o a Network Asserted Identity received in a 200 response t
  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

7. Privacy of Network Asserted Identity

The means by which any privacy requirements in respect of the
Asserted Identity are determined are outside the scope of thi

It shall be possible to indicate that a Network Asserted Iden
subject to a privacy requirement which prevents it being pass
other users.

In this case, the Network Asserted Identity specification sha
require that the mechanism of 3.2 SHALL NOT be used i.e. a tr
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 ide
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
another reason.

Note that æanonymityÆ requests from users or subscribers may
require functionality in addition to the above handling of Ne
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 im
the requirements of this draft.

9. Security considerations

The requirements in this draft are NOT intended to result in
mechanism with general applicability between arbitrary hosts
Internet.

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

The requirements on the mechanisms used for security and to i
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 fro
within the Trust Domain, via a secure connection to a node ou
the Trust Domain.

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

10. IANA Considerations

This document does not have any implications for IANA.

11. References

[1] J. Rosenberg et al, ôSIP: Session initiation protocol," d
ietf-sip-rfc2543bis-09.txt, February 27th, 2002.

[2] C.Jennings, ôNetwork Asserted Identity headerö, draft-jen
sipping-nai-00, May 2002, work in progress.

12. Acknowledgments

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

13. AuthorsÆ Addresses

Mark Watson
Nortel Networks (UK)
Maidenhead Office Park (Bray House)
Westacott Way
Maidenhead,
Berkshire Tel: +44 (0)1628-434456
England Email: mwatson@nortelnetworks.

14. Full Copyright Statement