SIP WG
Internet-Draft
Expires: December 27, 2003

J. Peterson
NeuStar
June 28, 2003

SIP Authenticated Identity Body (AIB) Format
draft-ietf-sip-authid-body-02

Status of this Memo

Copyright Notice

Abstract

RFC3261 introduces the concept of adding an S/MIME body to a SIP request or response in order to provide reference integrity over its headers. This document provides a more specific mechanism to derive integrity and authentication properties from an 'authenticated identity body', a digitally-signed SIP message or message fragment. A standard format for such bodies (known as Authenticated Identity Bodies, or AIBs) is given in this document. Some considerations for the processing of AIBs by recipients of SIP messages with such bodies are also given.

Table of Contents

1. Introduction

Section 23.4 of RFC3261 [1] describes an integrity mechanism that relies on signing tunneled 'message/sip' MIME bodies within SIP requests. The purpose of this mechanism is to replicate the headers of a SIP request within a body carried in that request in order to provide a digital signature over these headers. The signature on this body also provides authentication.

The core requirement that motivates this mechanism is the problem of providing a cryptographically verifiable identity within a SIP request. The baseline SIP protocol allows a user agent to express the identity of its user in any of a number of headers. The primary place for identity information asserted by the sender of a request is the From header. The From header field contains a URI (like 'sip:alice@atlanta.com') and an optional display-name (like "Alice") that identifies the originator of the request. A user may have many identities that are used in different contexts.

Typically, this URI is an address-of-record that can be dereferenced in order to contact the originator of the request; specifically, it is usually the same address-of-record under which a user registers their devices in order to receive incoming requests. This address-of-record is assigned and maintained by the administrator of the SIP service in the domain identified by the host portion of the address-of-record. However, the From field of a request can usually be set arbitrarily by the user of a SIP user agent; the From header of a message provides no internal assurance that the originating user can legitimately claim the given identity. Nevertheless, many SIP user agents will obligingly display the contents of the From field as the identity of the originator of a received request (as a sort of caller identification function), much as email implementations display the From field as the sender's identity

In order to provide the recipient of a SIP message with greater assurance of the identity of the sender, a cryptographic signature can be provided over the headers of the SIP request, which allows the signer to assert a verifiable identity. Unfortunately, a signature over the From header alone is insufficient because it could be cut-and-pasted into a replay or forwarding attack, and more headers are therefore needed to correlated a signature with a request. RFC3261 therefore recommends copying all of the headers from the request into a signed MIME body; however, SIP messages can also be large, and many of the headers in a SIP message would not be relevant to determining the identity of the sender or assuring reference integrity with the request, and moreover some headers may change in transit. It is therefore desirable to find a happy medium - to provide a way of signing just enough headers that the identity of the sender can be

ascertained and correlated with the request. 'message/sipfrag' [3] provides a way for a subset of SIP headers to be included in a MIME body; the AIB format described in Section 2 is based on 'message/sipfrag'.

For reasons of end-to-end privacy, it may also be desirable to encrypt AIBs; procedures for this encryption are given in Section 8.

2. AIB Format

As a way of sharing authenticated identity among parties in the network, a special type of MIME body format, the Authenticated Identity Body (AIB) format, is defined in this section. AIBs allow a party in a SIP transaction to cryptographically sign the headers that assert the identity of the originator of a message, and provide some other headers necessary for reference integrity.

An AIB is a MIME body of type 'message/sip' or 'message/sipfrag' (see [3]). This body MUST have a Content-Disposition disposition-type of 'aib', a new value defined in this document specifically for authenticated identity bodies. The Content-Disposition header SHOULD also contain a 'handling' parameter indicating that this MIME body is optional (i.e. if this mechanism is not supported by the user agent server, it can still attempt to process the request).

AIBs using the 'message/sipfrag' MIME type MUST contain the following headers when providing identity for an INVITE request: From, Date and Contact; they SHOULD also contain the To, Call-ID and CSeq header. AIBs MAY contain any other headers that help to uniquely identify the transaction or provide related reference integrity. An example of the AIB format for an INVITE is:

```
Content-Type: message/sipfrag
Content-Disposition: aib; handling=optional

From: Alice <sip:alice@atlanta.com>
To: Bob <sip:bob@biloxi.com>
Contact: <sip:alice@pc33.atlanta.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
```

Unsigned AIBs MUST NOT be honored by any recipients. After the AIB has been signed, it SHOULD be added to any existing MIME bodies in the request (such as SDP), if necessary by transitioning the outermost MIME body to a 'multipart/mixed' format.

3. Example of a Request with AIB

The following shows a full SIP INVITE request with an AIB:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: multipart/mixed; boundary=unique-boundary-1

--unique-boundary-1

Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 pc33.atlanta.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--unique-boundary-1
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 608

--boundary42
Content-Type: message/sipfrag
Content-Disposition: aib; handling=optional

From: Alice <sip:alice@atlanta.com>
To: Bob <sip:bob@biloxi.com>
Contact: <sip:alice@pc33.atlanta.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--

--unique-boundary-1--
```

4. AIBs for Identifying Third-Parties

There are special-case uses of the INVITE method in which some SIP messages are exchanged before an INVITE is sent, and the identity of a party from the prior exchange needs to be carried in the subsequent INVITE. Such information might be carried in one or more supplemental AIBs. The presence of these supplemental AIBs does not preclude the use of a 'regular' AIB as specified in this document to protect messages in which they appear.

The use of the REFER [4] method, for example, has a requirement for the recipient of an INVITE to ascertain the identity of the referrer who caused the INVITE to be sent. In this instance, the From header of the INVITE would indicate the referee, whereas a separate header would indicate the referrer.

Third-party call control (3PCC [5]) has an even more complicated identity problem. A central controller INVITEs one party, gathers identity information (and session context) from that party, and then uses this information to INVITE another party. Ideally, the controller would also have a way to share a cryptographic identity signature given by the first party INVITEd by the controller to the second party invited by the controller.

In both of these cases, the Call-ID and CSeq of the original request (3PCC INVITE or REFER) will not correspond with that of the request in by the subsequent INVITE, nor would the To and From. In both the REFER case and the 3PCC case, the Call-ID and CSeq cannot be used to determine reference integrity, and it is therefore much harder to correlate an AIB to a subsequent INVITE request. Some other special headers MAY be used to provide reference integrity between the headers in an AIB with the headers of a 3PCC or REFER-generated INVITE, but this usage is outside of the scope of this document.

5. Identity in non-INVITE Requests

The requirements for populating an AIB in requests within a dialog generally parallel those of the INVITE: From, Call-ID and Date are REQUIRED.

Some non-INVITE requests, however, may have different identity requirements. New methods should identify any special identity requirements in the Security Considerations of their specification.

6. Identity in Responses

Many of the practices described in the preceding sections can be applied to responses as well as requests. Note that a new set of headers must be generated to populate the AIB in a response. The From header field of the AIB in the response to an INVITE SHOULD correspond to the address-of-record of the responder, NOT to the From header field received in the request. The To header field of the request MUST NOT be included. A new Date header field and Contact header field should be generated for the AIB in a response. The Call-ID and CSeq should, however, be copied from the request.

Generally, the To header field of the request will correspond to the address-of-record of the responder. In some architectures where redirection is used, however, this need not be the case. Some recipients of response AIBs may consider it a cause for security concern if the To header field of the request is not the same as the address-of-record in the From header field of the AIB in a response.

7. Receiving an AIB

When a user agent receives a request containing an AIB, it should verify the signature, including validating the certificate of the signer, and compare the identity of the signer (the subjectAltName) with, in the INVITE case, the From header field of the request (for non-INVITE requests, other headers may be used). The two should correspond exactly; if they do not, the user agent should report this condition to its user before proceeding. User agents may distinguish between plausibly minor variations (the difference between 'atlanta.com' and 'sip.atlanta.com') and major variations ('atlanta.com' vs. 'evil.tv') when reporting these discrepancies in order to give the user some idea of how to handle this situation. Similar comparison of the Call-ID header is necessary for INVITE requests. The freshness of the Date header should also be evaluated, following the guidance in RFC3261.

When the originating user agent of a request receives a response containing an AIB, it SHOULD compare the identity in the To header

field of the AIB of the response with the original value of the To header field in the request. If these represent different identities, the user agent SHOULD render the identity in the AIB of the response to its user. Note that a discrepancy in these identity fields is not necessary an indication of a security breach; normal retargeting may simply have directed the request to a different final destination.

8. Encryption of Identity

Many SIP entities that support the use of S/MIME for signatures also support S/MIME encryption, as described in RFC3261 Section 23.4.3.

While encryption of AIBs entails that only the holder of a specific key can decrypt the body, that single key could be distributed throughout a network of hosts that exist under common policies. The security of the AIB is therefore predicated on the secure distribution of the key. However, for some networks (in which there are federations of trusted hosts under a common policy), the widespread distribution of a decryption key could be appropriate. Some telephone networks, for example, might require this model.

When an AIB is encrypted, the AIB SHOULD always be encrypted before it is signed. Note that this means that the recipients of the request, even if they are unable to inspect the AIBF, will still be able to see who signed that body (although it will not necessarily be obvious that the body contains an AIB).

9. Example of Encryption

The following is an example of an encrypted and signed AIB (without any of the preceding SIP headers). In a rendition of this body sent over the wire, the text wrapped in asterisks would be in ciphertext.

```
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568

--boundary42

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
  handling=required
Content-Length: 231

************************************************************
* Content-Type: message/sipfrag                            *
* Content-Disposition: aib; handling=optional              *
*                                                          *
* From: sip:alice@atlanta.com                              *
* Call-ID: a84b4c76e66710                                  *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                     *
************************************************************

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

10. Security Considerations

This document recommends the inclusion of the Call-ID, CSeq and To headers in AIBs when 'message/sipfrag' is used to represent the identity of a request's sender. If these headers are omitted, some important security properties of AIB are lost. For example, recipients of AIBs might keep a dictionary of received Call-IDs for some duration of time (perhaps until two hours after the Date header in the AIB), and compare the Call-ID received in AIBs of new requests to those in the dictionary in order to detect replays of AIBs.

Caching CSeqs can also assist in the detection of replays.

11. IANA Considerations

This document defines a new MIME Content-Disposition disposition-type value of 'aib'. This value is reserved for MIME bodies that contain an authenticated identity, as described in section Section 2.

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, May 2002.

[2] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[3] Sparks, R., "Internet Media Type message/sipfrag", RFC 3420, September 2002.

Informative References

[4] Sparks, R., "The SIP Refer Method", draft-ietf-sip-refer-07 (work in progress), November 2002.

[5] Rosenberg, J., Peterson, J., Schulzrinne, H. and G. Camarillo, "Best Current Practices for Third-Party Call Control in the Session Initiation Protocol", draft-ietf-sipping-3pcc-02 (work in progress), June 2002.

Author's Address

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US

Phone: +1 925/363-8720
EMail: jon.peterson@neustar.biz
URI: http://www.neustar.biz/

Appendix A. Acknowledgements

The author would like to thank Robert Sparks, Jonathan Rosenberg, and Mary Watson for their comments. Rohan Mahy also provided some

valuable guidance.

Full Copyright Statement

Acknowledgement

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