Session Initiation Protocol Private Extension for an OSP Authorization Token

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document discusses a private extension to the Session Initiation Protocol (SIP) for carrying OSP (Open Settlements Protocol) authorization tokens in applications such as clearinghouses.
The problem of interdomain IP telephony calls with QoS is an important problem being addressed using AAA protocols. The new private SIP [1] header field proposed here is part of an approach to solving this problem, which is summarized briefly here.

Interdomain IP telephony is accomplished today using clearinghouse services and a mix of proprietary and standard AAA protocols. Making calls with AAA support between service providers that are affiliated to different clearinghouses is a difficult problem.

Beyond IP telephony it is also desirable to have a consistent AAA approach for all applications on the Internet.

Work on a general architecture for AAA is proceeding in the IETF AAAarch research group. A framework and examples have been developed for various Internet applications. At the same time, Internet telephone calls can be set up with QoS and security. Since QoS is a valuable network resource, it requires AAA and possibly payments.

This draft documents a proprietary SIP extension header field that may be used to exchange open settlements protocol [4] information in the context of a SIP session establishment. The approach outlined here may be useful later for developing a uniform AAA architecture and protocols for other application layer services.

Figure 1 shows the model for an interdomain phone call across the Internet with the various entities having business relationships, but not necessarily trust relationships with their correspondents:
While this approach to interdomain authorization is not a complete one, it is currently used today by IP telephony carriers and is useful in limited applications such as in a clearinghouse. As such, it is appropriate for the header field extension to SIP be registered as a private SIP header field per the SIP change process [5]. Note that while RSVP [6] is shown, its use is not required by this extension.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [2] and indicate requirement levels for compliant SIP caller preferences implementations.

3. Design Alternatives

The OSP Token is an opaque string to SIP which must be carried in the INVITE passed between domains. As such, the Token could be carried as a MIME attachment. However, there are three issues with this:

- Since the Token must be carried with the SDP, the INVITE would
need to have a multipart MIME message body. If either User Agents do not support multipart MIME, the call will fail.

- The Token is used by both proxies and User Agents. As such, the proxy would have to decode the multipart MIME message body to extract the token. The general design of SIP is for message bodies to contain information of interest to end-points only, with information needed by proxies contained in header fields.

- Multipart MIME encoding/decoding adds more delay to an already lengthy call setup procedure, as compared to header field processing.

For these reasons, a new SIP header field is proposed instead of a new MIME type for OSP authorization tokens.

Note that since OSP tokens are commonly constructed according to Cryptographic Message Syntax [3], their size may depend on the size of X.509 certificates embedded in the CMS format. For this reason, entities using this header field MUST NOT use UDP for transport. Instead TLS SHOULD be used. In addition, it is recommended that systems use the abbreviated token format described in Annex D of [4].

4. Header Field Definition

The table below specifies an extension of Table 2 in RFC 3261 [1] for the new header field defined here.

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Where</th>
<th>proxy</th>
<th>ACK</th>
<th>BYE</th>
<th>CAN</th>
<th>INV</th>
<th>OPT</th>
<th>REG</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-OSP-Auth-Token</td>
<td>R ad</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>P-OSP-Auth-Token</td>
<td>18x,2xx ad</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

The "where" column describes the request and response types with which the header field can be used. "R" indicates a request header field, a numeric value in the "where" column indicates the status code the header field is used with. The "proxy" column describes whether this message header field MAY be added, "a", or deleted, "d", by a proxy server. In the method columns, "o" means optional and "-" means not applicable.

The Augmented BNF for the header field (using the form and definitions in Section 25 of RFC 3261) is:

```plaintext
P-OSP-Auth-Token = "P-OSP-Auth-Token" HCOLON token *(SEMI osp-param)
osp-param       = realm / generic-param
realm           = "realm" EQUAL realm-value
realm-value     = quoted-string
```
5. Protocol Semantics

The OSP Token is always encoded per base64 and only allowed in INVITE requests, 200 OK responses to INVITES, and reliable provisional responses to INVITEs.

5.1 User Agents

A UAC MAY include the header field an INVITE requesting QoS using AAA.

If present in an INVITE, an AAA/QoS UAS MAY validate the token.

If it is absent or present in the INVITE, an AAA/QoS UAS MAY include the header field in a reliable provisional response or 200 OK answer.

A UAC MAY validate the token received in a response to an INVITE.

5.2 Proxies

A proxy participating in the AAA exchange may add, delete, examine or validate the token.

Otherwise, the header field is ignored.

6. Example Message

This SIP INVITE message is an example exchange between the two domains as shown in Figure 1:

```
INVITE sips:+1-972-555-5555@domain2.example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS proxy.domain1.example.com:5061;branch=z9hG4bK3a5d3.1
Via: SIP/2.0/TLS phone1.domain1.example.com:5061;branch=z9hG4bK3a5654
 ;received=192.0.2.1
Max-Forward: 69
From: Alice <sips:alice@phone1.domain1.example.com>;tag=3
To: <sips:+1-972-555-5555@domain2.example.com;user=phone>
Call-ID: 123456@domain1.example.com
CSeq: 1 INVITE
Contact: <sips:alice@phone1.domain1.example.com>
Record-Route: <sips:proxy.domain1.example.com;lr>
P-OSP-Auth-Token: "YT64VqpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tHGTrfvbnj88HHTrfrvHhjHj776tbB9HG4VQbnj7567GhIGfH6ghyHhHUujpfyF47GhIGfHfYT64VQbnj";realm="domain1.example.com"
Content-Type: application/sdp
Content-Length: 184
```

```txt
v=0
o=alice 9735285123 9721273312 IN IP4 phone1.domain1.example.com
s=-
```
IANA Considerations

Registration of "P-OSP-Auth-Token" SIP header field

This document defines a new private SIP header field, "P-OSP-Auth-Token". As recommended by the policy of the Transport Area [5], this header field should be registered by the IANA in the SIP header field registry, using the RFC number of this document as its reference.

Name of Header field: P-OSP-Auth-Token
Short form: None
Registrant: Alan Johnston
alan.johnston@mci.com
Normative description: This document

Security Considerations

The security and handling of OSP tokens is covered in [4] which includes encryption and use of IPSec.

The P-OSP-Auth-Token header field may be protected using standard SIP mechanisms such as TLS transport and/or S/MIME encryption as detailed in [1].

Since the threats analyzed in the OSP document include ones in which the token is carried in plain text and available to an attacker, carrying the token in SIP does not introduce any new attacks.

Normative References


Informative References


Authors’ Addresses

Alan Johnston
MCI
100 S. 4th Street
St. Louis, Missouri 63102
USA
alan.johnston@mci.com

Henry Sinnreich
MCI
400 International Parkway
Richardson, Texas 75081
USA
henry.sinnreich@mci.com

Diana Rawlins
MCI
901 International Parkway
Richardson, Texas 75081
USA
diana.rawlins@mci.com

Stephen Thomas
Wave7 Optics
1075 Windward Ridge Parkway
Alpharetta, GA 30005
USA
stephen.thomas@wave7optics.com

Richard Brennan
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.
Acknowledgment

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