SIPPING
Internet-Draft
Expires: May 29, 2007

G. Camarillo
Ericsson

November 25, 2006

A Document Format for Requesting Consent
draft-ietf-sipping-consent-format-01.txt

Status of this Memo

Copyright Notice

Abstract

This document defines an Extensible Markup Language (XML) format for a permission document used to request consent. A permission document written in this format is used by a relay to request the permission, of a specific recipient, to perform a particular routing translation.

Table of Contents

1. Introduction

The framework for consent-based communications in the Session Initiation Protocol (SIP) [9] identifies the need for a format to create permission documents. Such permission documents are used by SIP [3] relays to request permission to perform translations. A relay is defined as any SIP server, be it a proxy, B2BUA (Back-to-Back User Agent), or some hybrid, which receives a request and translates the request URI into one or more next hop URIs to which it then delivers a request.

The format for permission documents specified in this document is based on the XML document format for expressing Privacy Preferences [8].

2. Definitions and Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [1] and indicate requirement levels for compliant implementations.

Relay: Any SIP server, be it a proxy, B2BUA (Back-to-Back User Agent), or some hybrid, that receives a request, translates its Request-URI into one or more next-hop URIs (i.e., recipient URIs), and delivers the request to those URIs.

Recipient URI: The Request-URI of an outgoing request sent by an entity (e.g., a user agent or a proxy). The sending of such request may have been the result of a translation operation.

Target URI: The Request-URI of an incoming request that arrives to an entity (e.g., a proxy) that will perform a translation operation.

Translation operation: Operation by which an entity (e.g., a proxy) translates the request URI of an incoming request (i.e., the target URI) into one or more URIs (i.e., recipient URIs) which are used as the request URIs of one or more outgoing requests.

3. Permission Document Structure

A permission document is an XML document, formatted according to the schema defined in [8]. Permission documents inherit the MIME type of common policy documents, 'application/auth-policy+xml'. As described in [8], this type of document is composed of three parts: conditions,

actions, and transformations. However, even though permission documents need to have a transformation part to comply to the common policy syntax, effectively, permission documents do not make any use of transformations.

This section defines the new conditions and actions defined by this specification. This specification does not define any new transformation.

3.1. Conditions

Note that, as discussed in [8], a permission document applies to a translation if all the expressions in its conditions part evaluate to TRUE.

3.1.1. Identity Condition

The identity condition, defined in [8], is matched against the recipient URI of a translation.

When performing a translation, a relay matches the identity condition of the permission document that was used to request permission for that translation against the destination URI of the outgoing request. When receiving a request granting or denying permissions (e.g., a SIP PUBLISH request as described in [9]), the relay matches the identity condition of the permission document that was used to request permission against the identity of the entity granting or denying permissions (i.e., the sender of the PUBLISH request).

The <identity> element is defined in [8], which indicates that the specific usages of the framework document need to define details that are protocol and usage specific. In particular, this section defines acceptable means of authentication.

The 'id' attribute in the elements <one> and <except> MUST contain a scheme when these elements appear in a permission document.

When used with SIP, a recipient granting or denying a relay permissions is considered authenticated if one of the following techniques is used:

SIP Identity [7], as described in [9]. For PUBLISH requests that are authenticated using the SIP Identity mechanism, the identity of the sender of the PUBLISH request is equal to the SIP URI in the From header field of the request, assuming that the signature in the Identity header field has been validated.

P-Asserted-Identity [5], as described in [9]. For PUBLISH requests that are authenticated using the P-Asserted-Identity mechanism, the identity of the sender of the PUBLISH request is equal to the P-Asserted-Identity header field of the request.

Return Routability Test, as described in [9].

SIP digest, as described in [9].

3.1.2. Sender Condition

The sender condition is matched against the URI of the sender of the request that is used as input for a translation. Sender conditions can contain the same elements and attributes as identity conditions.

When performing a translation, a relay matches the sender condition against the identity of the sender of the incoming request.

The following subsections define acceptable means of authentication, the procedure for representing the identity of the sender as a URI, and the procedure for converting an identifier of the form user@domain, present in the 'id' attribute of the <one> and <except> elements, into a URI.

3.1.2.1. Acceptable Means of Authentication

When used with SIP, a request sent by a sender is considered authenticated if one of the following techniques is used:

SIP Digest: the relay authenticates the sender using SIP digest authentication [2]. However, if the anonymous authentication described on page 194 of RFC 3261 [3] is used, the sender is not considered authenticated.

Asserted Identity: if a request contains a P-Asserted-ID header field [5] and the request is coming from a trusted element, the sender is considered authenticated.

Cryptographically Verified Identity: if a request contains an Identity header field as defined in [7], and it validates the From header field of the request, the request is considered to be authenticated. Note that this is true even if the request contained a From header field of the form sip:anonymous@example.com. As long as the signature verifies that the request legitimately came from this identity, it is considered authenticated.

3.1.2.2. Computing a URI for the Sender

For requests that are authenticated using SIP Digest, the identity of the sender is set equal to the SIP Address of Record (AOR) for the user that has authenticated themselves. For example, consider the following "user record" in a database:

```
SIP AOR: sip:alice@example.com
digest username: ali
digest password: f779ajvvh8a6s6
digest realm: example.com
```

If the relay receives a request, challenges it with the realm set to "example.com", and the subsequent request contains an Authorization header field with a username of "ali" and a digest response generated with the password "f779ajvvh8a6s6", the identity used in matching operations is "sip:alice@example.com".

For requests that are authenticated using RFC 3325 [5], the identity of the sender is equal to the SIP URI in the P-Asserted-ID header field. If there are multiple values for the P-Asserted-ID header field (there can be one sip URI and one tel URI [10]), then each of them is used for the comparisons outlined in [8], and if either of them match a <one> or <except> element, it is considered a match.

For requests that are authenticated using the SIP Identity mechanism [7], identity of the sender is equal to the SIP URI in the From header field of the request, assuming that the signature in the Identity header field has been validated.

SIP also allows for anonymous requests. If a request is anonymous because the digest challenge/response used the "anonymous" username, the request is considered unauthenticated and will not match the <sender> condition. If a request is anonymous because it contains a Privacy header field [4], but still contains a P-Asserted-ID header field, the identity in the P-Asserted-ID header field is still used in the authorization computations; the fact that the request was anonymous has no impact on the identity processing. However, if the request had traversed a trust boundary and the P-Asserted-ID header field and the Privacy header field had been removed, the request will be considered unauthenticated when it arrives at the presence server, and thus not match the <sender> condition. Finally, if a request contained an Identity header field that was validated, and the From header field contained a URI of the form sip:anonymous@example.com, then the watcher is considered authenticated, and it will have an identity equal to sip:anonymous@example.com. Had such an identity been placed into a <one> or <except> element, there will be a match.

3.1.2.3. Computing a SIP URI from the id Attribute

If the <one> or <except> condition does not contain a scheme, conversion of the value in the 'id' attribute to a SIP URI is done trivially. If the characters in the 'id' attribute are valid characters for the user and hostpart components of the SIP URI, a 'sip:' is appended to the contents of the 'id' attribute, and the result is the SIP URI. If the characters in the 'id' attribute are not valid for the user and hostpart components of the SIP URI, conversion is not possible. This happens, for example, when the user portion of the 'id' attribute contain UTF-8 characters.

3.1.3. Target Condition

The target condition is matched against the target URI of a translation. Target conditions can contain the same elements and attributes as identity conditions.

When performing a translation, a relay matches the target condition against the destination of the incoming request, which is typically contained in the Request-URI.

3.2. Actions

The actions in a permission document provide URIs to grant or deny permission to perform the translation described in the document.

3.2.1. Translation Handling

The <trans-handling> provides URIs for a recipient to grant or deny the relay permission to perform a translation. The defined values are:

deny: this action tells the relay not to perform the translation.

grant: this action tells the server to perform the translation.

The 'perm-uri' attribute in the <trans-handling> element provides a URI to grant or deny permission to perform a translation.

4. Example Document

The following permission document is generated by the relay handling 'sip:alices-friends@example.com' in order to ask for permission to relay requests sent to that URI to 'sip:bob@example.org'.

```
<?xml version="1.0" encoding="UTF-8"?>
   <cr:ruleset
    xmlns="urn:ietf:params:xml:ns:consent-rules"
    xmlns:cp="urn:ietf:params:xml:ns:common-policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:ietf:params:xml:ns:consent-rules
                        consent-rules.xsd">
    <cp:rule id="1">
     <cp:conditions>
      <cp:identity>
       <cp:one id="sip:bob@example.org"/>
      </cp:identity>
      <target>
       <cp:one id="sip:alices-friends@example.com""/>
      </target>
      <sender>
       <cp:any/>
      </sender>
     </cp:conditions>
     <cp:actions>
      <trans-handling
             perm-uri="sip:foo@example.com">grant</trans-handling>
      <trans-handling
             perm-uri="sip:bar@example.com">deny</trans-handling>
     </cp:actions>
     <cp:transformations/>
    </cp:rule>
   </cp:ruleset>
```

5. XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
   <xs:schema
     targetNamespace="urn:ietf:params:xml:ns:consent-rules"
     xmlns:cr="urn:ietf:params:xml:ns:consent-rules"
     xmlns:cp="urn:ietf:params:xml:ns:common-policy"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     elementFormDefault="qualified"
     attributeFormDefault="unqualified">

     <!-- Conditions -->
     <xs:element name="sender" type="cp:identityType"/>
     <xs:element name="target" type="cp:identityType"/>

    <!-- Actions -->
    <xs:simpleType name="trans-values">
       <xs:restriction base="xs:string">
         <xs:enumeration value="deny"/>
         <xs:enumeration value="grant"/>
       </xs:restriction>
     </xs:simpleType>

     <xs:element name="trans-handling">
       <xs:complexType>
         <xs:simpleContent>
           <xs:extension base="trans-values">
             <xs:attribute name="perm-uri" type="xs:anyURI"
                           use="required"/>
           </xs:extension>
         </xs:simpleContent>
       </xs:complexType>
     </xs:element>

   </xs:schema>
```

6. IANA Considerations

This section registers a new XML namespace and a new XML schema per the procedures in [6].

6.1. XML Namespace Registration

URI: urn:ietf:params:xml:ns:common-policy

Registrant Contact: IETF SIPPING working group, <sipping@ietf.org>, Gonzalo Camarillo <Gonzalo.Camarillo@ericsson.com>

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
        content="text/html;charset=iso-8859-1"/>
  <title>Consent Rules Namespace</title>
</head>
<body>
  <h1>Namespace for Permission Documents</h1>
  <h2>urn:ietf:params:xml:ns:consent-rules</h2>
<p>See <a href="[URL of published RFC]">RFCXXXX
    [NOTE TO IANA/RFC-EDITOR:
     Please replace XXXX with the RFC number of this
    specification.]</a>.</p>
</body>
</html>
END
```

6.2. XML Schema Registration

URI: urn:ietf:params:xml:schema:common-policy

Registrant Contact: IETF SIPPING working group,
<sipping@ietf.org>, Gonzalo Camarillo
<Gonzalo.Camarillo@ericsson.com>

XML: The XML schema to be registered is contained in Section 5.

7. Security Considerations

Permission documents can reveal sensitive information. Additionally, attackers may attempt to modify them in order to have clients grant or deny permissions different to the ones they think are granting or denying. For this reason, it is RECOMMENDED that relays use strong means for information integrity protection and confidentiality when sending permission documents to clients.

The mechanism used for conveying information to clients SHOULD ensure the integrity and confidentially of the information. In order to achieve these, an end-to-end SIP encryption mechanism, such as S/MIME, as described in RFC 3261 [3], SHOULD be used.

If strong end-to-end security means (such as above) is not available, it is RECOMMENDED that hop-by-hop security based on TLS and SIPS URIs, as described in [3], is used.

8. Acknowledgements

Jonathan Rosenberg provided useful ideas on this document. Ben Campbell and Mary Barnes performed a thorough review of this document.

9. References

9.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[3] 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.

[4] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[5] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[6] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[7] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[8] Schulzrinne, H., "Common Policy: A Document Format for Expressing Privacy Preferences", draft-ietf-geopriv-common-policy-11 (work in progress), August 2006.

[9] Rosenberg, J., Camarillo, G., and D. Willis, "A Framework for Consent-Based Communications in the Session Initiation Protocol

(SIP)", draft-ietf-sip-consent-framework-00 (work in progress), September 2006.

9.2. Informative References

[10] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

Author's Address

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: Gonzalo.Camarillo@ericsson.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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