SIP	H. Tschofenig	
Internet-Draft	Nokia Siemens Networks	
Intended status: Experimental	J. Hodges	
Expires: April 28, 2011		
	J. Peterson	
	NeuStar, Inc.	
	J. Polk	
	Cisco	
	D. Sicker	
	CU Boulder	
	October 25, 2010	

TOC

SIP SAML Profile and Binding
draft-ietf-sip-saml-08.txt

Abstract

This document specifies a Session Initiation Protocol (SIP) profile of Security Assertion Markup Language (SAML) as well as a SAML SIP binding. The defined SIP SAML Profile composes with the mechanisms defined in the SIP Identity specification and satisfy requirements presented in "Trait-based Authorization Requirements for the Session Initiation Protocol (SIP)".

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on April 28, 2011.

Copyright Notice

Table of Contents

---

1. Introduction

TOC

This document specifies composition of the Security Assertion Markup Language (SAML) V2.0 with SIP [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.) in order to accommodate richer authorization mechanisms and enable "trait-based authorization". Trait-based authorization is where one is authorized to make use of some resource based on roles or traits rather than ones identity. Motivations for trait-based authorization, along with use-case scenarios, are presented in [RFC4484] (Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, “Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP),” August 2006.). Security Assertion Markup Language (SAML) v2.0, "SAMLv2", is an XML-based framework for creating and exchanging security information. [OASIS.sstc-saml-exec-overview-2.0-cd-01] (Madsen, P. and E. Maler, “SAML V2.0 Executive Overview,” April 2005.) and [OASIS.sstc-saml-tech-overview-2.0-draft-16] (Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview,” May 2008.) provide non-normative overviews of SAMLv2. The SAMLv2 specification set is normatively defined by [OASIS.saml-conformance-2.0-os] (Mishra, P., Philpott, R., and E. Maler, “Conformance Requirements for the Security Assertion Markup Language (SAML) V2.0,” March 2005.).
Various means for encoding authorization information exists, such as authorization certificates [RFC3281] (Farrell, S. and R. Housley, “An Internet Attribute Certificate Profile for Authorization,” April 2002.), SPKI [RFC2693] (Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and T. Ylonen, “SPKI Certificate Theory,” September 1999.), or extensions to the authenticated identity body [RFC3893] (Peterson, J., “Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format,” September 2004.). This document focuses on an encoding of the authorization information using SAML assertions but does not exclude other formats to be used utilized in the future.

2. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

The SIP network element "Authentication Service" is introduced in [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.). We reuse this term to refer to a network element that authenticates and authorizes a user and creates a "SIP identity assertion". This system entity is the logical equivalent of a "SAML Authority" in the SAML terminology.

For overall SIP terminology, see [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.).

In this specification, the term, or term component, "SAML" refers to SAML V2.0 in all cases. For example, the term "SAML assertion" implicitly means "SAMLv2 assertion". For overall SAML terminology, see [OASIS.saml-glossary-2.0-os] (Hodges, J., Philpott, R., and E. Maler, "Glossary for the Security Assertion Markup Language (SAML) V2.0," March 2005.).

The below list maps other various SIP terms to their SAML (rough-)equivalents:

Element, Network Element:
System Entity, Entity

Authentication Service:
SAML Authority

Invitee, Invited User, Called Party, Callee:
Relying Party

Server, User Agent Server (UAS):
SAML Responder

User Agent Client (UAC), client:
SAML Requester

Additional terms defined in the context of this specification:

> **profile attribute(s):** one or more attributes of a "user profile".
>
> **user profile, subject profile:** the set of various attributes accompanying (i.e., mapped to) a user account in many environments.

---

3. SAML Introduction

TOC

SAML [OASIS.sstc-saml-exec-overview-2.0-cd-01] (Madsen, P. and E. Maler, “SAML V2.0 Executive Overview,” April 2005.) [OASIS.sstc-saml-tech-overview-2.0-draft-16] (Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview,” May 2008.) defines an XML-based framework for exchanging "security assertions" between entities. In the course of making, or relying upon such assertions, SAML system entities may use SAML protocols, or other protocols, to communicate an assertion itself, or the subject of an assertion.
Thus one can employ SAML to make and encode statements such as "Alice has these profile attributes and her domain's certificate is available over there, and I'm making this statement, and here's who I am." Then one can cause such an assertion to be conveyed to some party who can then rely on it in some fashion for some purpose, for example input it into some local policy evaluation for access to some resource. This is done in a particular "context of use". Such a context of use could be, for example, deciding whether to accept and act upon a SIP-based invitation to initiate a communication session.
The specification of how SAML is employed in a particular context of use is known as a "SAML profile". The specification of how SAML assertions and/or protocol messages are conveyed in, or over, another protocol is known as a "SAML Binding". Typically, a SAML profile specifies the SAML bindings that may be used in its context. Both SAML profiles and SAML bindings reference other SAML specifications, especially the SAML Assertions and Protocols, aka "SAML Core", specification [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).
There is an additional subtle aspect of SAML profiles that is worth highlighting -- the notion of a "SAML assertion profile". A SAML assertion profile is the specification of the assertion contents in the

context of a particular SAML profile. It is possibly further qualified by a particular implementation and/or deployment context. Condensed examples of SAML assertion profiles are:

- The SAML assertion must contain at least one authentication statement and no other statements. The relying party must be represented in the <AudienceRestriction> element. The SubjectConfirmation Method must be Foo. etc.

- The SAML assertion must contain at least one attribute statement and may contain more than one. The values for the subject's profile attributes named "Foo" and "Bar" must be present. An authentication statement may be present. etc.

The primary facets of SAML itself are:

- Assertions

- Abstract Request/Response protocol

We describe each in turn below:

3.1. SAML Assertions

TOC

A SAML assertion is a package of information including issuer and subject, conditions and advice, and/or attribute statements, and/or authentication statements and/or other statements. Statements may or may not be present. The SAML assertion "container" itself contains the following information:

Issuing information:
Who issued the assertion, when was it issued and the assertion identifier.

Subject information:
The name of the subject, the security domain and optional subject information, like public key.

Conditions under which the assertion is valid:
Special kind of conditions like assertion validity period, audience restriction and target restriction.

> **Additional advice:** Explaining how the assertion was made, for example.

In terms of SAML assertions containing SAML attribute statements or SAML authentication statements, here are explanatory examples:

> With a SAML assertion containing a SAML attribute statement, an issuing authority is asserting that the subject is associated with certain attributes with certain subject profile attribute values. For example, user jon@cs.example.com is associated with the attribute "Department", which has the value "Computer Science".
>
> With a SAML assertion containing a SAML authentication statement, an issuing authority is asserting that the subject was authenticated by certain means at a certain time.
>
> With a SAML assertion containing both a SAML attribute statement and a SAML authentication statement, an issuing authority is asserting the union of the above.

3.2. Abstract Request/Response Protocol

TOC

SAML defines an abstract request/response protocol for obtaining assertions. See Section 3 "SAML Protocols" of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.). A request asks for an assertion. A response returns the requested assertion or an error. This abstract protocol may then be cast into particular contexts of use by binding it to specific underlying protocols, e.g., HTTP or SIP, and "profiling" it for the specific use case at hand. The SAML HTTP-based web single sign-on profile is one such example (see Section 4.1 Web Browser SSO Profile of [OASIS.saml-profiles-2.0-os] (Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., and E. Maler, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.)). Trait-based SIP communication session establishment, the topic of this specification, is another.

TOC

4. Specification Scope

The scope of this specification is:

* Specify a SIP profile of SAML -- also known as a "SIP SAML profile" -- such that a subject's profile attributes, and their domain's certificate, can be conveyed to a relying party using SAML. In doing so, satisfy the requirements outlined in [RFC4484] (Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)," August 2006.), and compose with [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.).

The following are outside the scope of this specification:

* Defining a means for configuring the runtime behavior, or deployment characteristics, of the Authentication Service.

  Discussion:

  For example, a SIP Authentication Service could be implemented such that its SAML-based features are employed, or not, on a subject-by-subject basis, and/or on a domain-by-domain basis.

* The definition of specific conveyed subject profile attributes (aka traits).

  Discussion:

  This specification defines a facility enabling "trait-based authorization" as discussed in [RFC4484] (Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)," August 2006.).

  The attributes of interest in trait-based authorization will be ones akin to, for example: roles, organizational membership, access rights, or authentication event context. Definition of such attributes is application- and/or deployment-context-dependent and are not defined in this specification. However, The SAMLv2 specification defines several "SAML Attribute Profiles" for encoding attributes from various application domains, e.g., LDAP, UUID/GUID, DCE PAC, and XACML, in SAML assertions [OASIS.saml-profiles-2.0-os] (Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., and E. Maler, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005.).

In order for any trait-based system to be practical, participating entities must agree on attributes and traits that will be conveyed and subsequently relied upon. Without such agreements, a trait-based system cannot be usefully deployed. This specification does not discuss the manner in which participating entites might discover one another or agree on the syntax and semantics of attributes and traits.

Note that SAMLv2 specifies a "metadata" facility that may be useful in addressing this need.

---

5. Employing SAML in SIP

TOC

Employing SAML in SIP necessitates devising a new SAML profile(s) and binding(s) because those already specified in the SAMLv2 specification set are specific to other use contexts, e.g., HTTP-based web browsing. Although SIP bears some similarity to HTTP, it is a seperately distinct protocol, thus requiring specification of SIP-specific SAML profile(s) and binding(s). This is technically straightforward as both SAML and SIP are explicitly extensible.

The SIP SAML Profiles defined in this document make use of concepts defined by [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)" -- also known as "SIP Identity". SIP Identity allows the SIP UA client and an entity on behalf of the UA client to attach a SAML assertion (or a reference to it). Since intermediaries, like an outbound SIP proxy, are not allowed to modify the body of a SIP message such an intermediary would attach a pointer to the assertion instead.

The specific details on how the SAML assertion is requested are outside the scope of this document. Possible mechanisms are to use a software library that can be accessed via an API, a separate authorization server that can be queried via HTTP (as envisioned by OAuth [I-D.ietf-oauth-v2] (Hammer-Lahav, E., Recordon, D., and D. Hardt, “The OAuth 2.0 Protocol,” July 2010.)), or any other mechanism. As such, this document does not further describe the functional split between the party that attaches the SAML assertion to the SIP message and the party that creates the SAML assertion.

The SIP Identity specification calls the party that makes identity assertions about the caller "Authentication Service (AS)". Such an Authentication Service, which likely has access to various pieces of information concerning the calling party, could also act as a SAML Authority, and make such information available to the callee via SAML. This document uses the term SAML Authority and Authentication Service

interchangable particularly because of the fact that the entity that attaches the SAML assertion to the SIP message also uses the SIP Identity mechanism to bind it to the message.
Note that technically there is a difference between attaching a reference to a SAML assertion and attaching a SAML assertion to the body of a message. We define two different profiles to cover these two cases:

AS-driven SIP SAML URI-based Attribute Assertion Fetch Profile: In case of this profile the AS attaches a reference to a SAML assertion to the SIP message and makes it available to the verifier. More details about this profile can be found in Section 7.1 (AS-driven SIP SAML URI-based Attribute Assertion Fetch Profile).

Assertion-by-Value Profile: In case of this profile the SAML assertion is made available to the verifying party directly without the additional step of utilizing a reference. This approach is described in Section 7.2 (Caller-driven SIP SAML Conveyed Assertion Profile).

---

6. URI Parameter Definition

TOC

This document represents the URL pointing to the authorization information using a URI parameter. The grammar for this parameter is (following the ABNF [RFC4234] (Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," October 2005.) in Section 25 of RFC 3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.)):

```
token-info         =
          "token-info" HCOLON ident-info *( SEMI ident-info-params )

ident-info         = LAQUOT absoluteURI RAQUOT

ident-info-params = generic-param
```

Figure 1: 'token-info' ABNF Grammar

The "absoluteURI" MUST contain a URI which dereferences to a resource containing a SAML assertion. All implementations of this specification MUST support the use of HTTP and HTTPS URIs. Such HTTP and HTTPS URIs MUST follow the conventions of RFC 2585 [RFC2585] (Housley, R. and P. Hoffman, “Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP,” May 1999.), and for those URIs the indicated resource MUST be of the form 'application/samlassertion+xml' described in that specification.
An example of the syntax of the "token-info" parameter is given below:

```
From: <tel:+17005554141;
      token-info=https://example.com/assns/?ID=abcde>;
      tag=1928301774
```

7. SIP SAML Profiles

TOC

This section defines two "SIP SAML profiles":

* The "AS-driven SIP SAML URI-based Attribute Assertion Fetch Profile"

* The "Assertion-by-Value" Profile

7.1. AS-driven SIP SAML URI-based Attribute Assertion Fetch Profile

TOC

7.1.1. Required Information

TOC

The information given in this section is similar to the info provided when registering something, a MIME Media Type, say, with IANA. In this case, it is for registering this profile with the OASIS SSTC. See Section 2 "Specification of Additional Profiles" in [OASIS.saml-profiles-2.0-os] (Hughes, J., Cantor, S., Hodges, J.,

Hirsch, F., Mishra, P., Philpott, R., and E. Maler, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).

Identification:
urn:ietf:params:sip:sip-saml-profile:as:uri:attr:1.0

Contact Information:
Hannes Tschofenig (Hannes.Tschofenig@nsn.com)

SAML Confirmation Method Identifiers:
The SAML V2.0 confirmation method identifier is used in this profile.

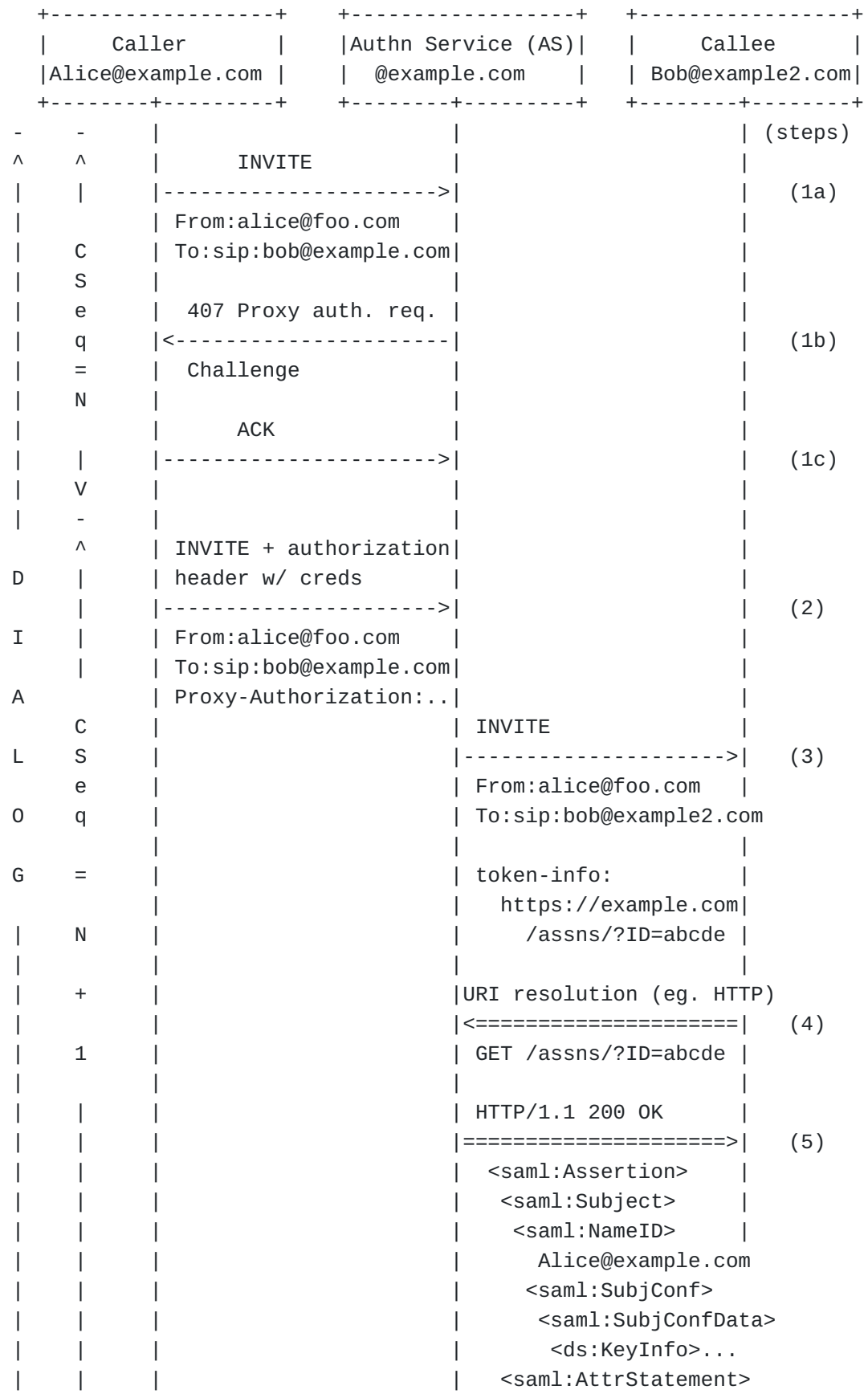
Description:
Given below.

Updates:
None.

7.1.2. Profile Overview

TOC

Figure 2 (AS-driven SIP SAML Attribute Fetch Profile: Example INVITE Transaction) illustrates this profile's overall protocol flow. The following steps correspond to the labeled interactions in the figure. Within an individual step, there may be one or more actual message exchanges depending upon the protocol binding employed for that particular step and other implementation-dependent behavior. Although this profile is overview is cast in terms of a SIP INVITE transaction, the reader should note that the mechanism specified herein, may be applied to any SIP request message.
Figure 2 (AS-driven SIP SAML Attribute Fetch Profile: Example INVITE Transaction) begins on the next page.


Caller
Alice@example.com
Authn Service (AS)
@example.com
Callee
Bob@example2.com
(steps)
INVITE
From:alice@foo.com
To:sip:bob@example.com
(1a)
407 Proxy auth. req.
Challenge
(1b)
ACK
(1c)
INVITE + authorization
header w/ creds
From:alice@foo.com
To:sip:bob@example.com
Proxy-Authorization:..
(2)
INVITE
From:alice@foo.com
To:sip:bob@example2.com
(3)
token-info:
https://example.com
/assns/?ID=abcde
URI resolution (eg. HTTP)
(4)
GET /assns/?ID=abcde
HTTP/1.1 200 OK
(5)
<saml:Assertion>
<saml:Subject>
<saml:NameID>
Alice@example.com
<saml:SubjConf>
<saml:SubjConfData>
<ds:KeyInfo>...
<saml:AttrStatement>
CSeq=N+1
DIALOG

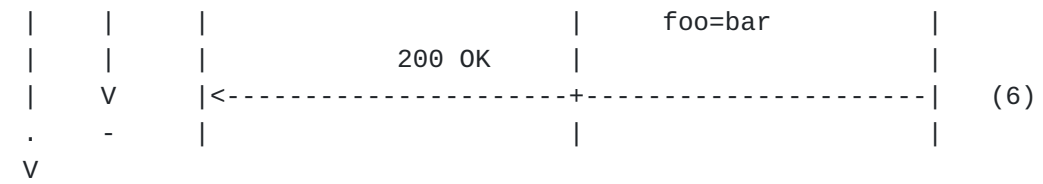


Figure 2: AS-driven SIP SAML Attribute Fetch Profile: Example INVITE Transaction

Step 1. Initial SIP Transaction between Caller and AS
This optional initial step is comprised of substeps 1a, 1b, and 1c in Figure 2 (AS-driven SIP SAML Attribute Fetch Profile: Example INVITE Transaction). In this step, the caller, Alice, sends a SIP request message, illustrated as an INVITE, indicating Bob as the callee (1a), is subsequently challenged by the AS (1b), and sends an ACK in response to the challenge (1c). The latter message signals the completion of this SIP transaction (which is an optional substep of this profile).

Step 2. Caller sends SIP Request Message with Authorization Credentials to the AS
Alice then sends an INVITE message in response to the challenge, or uses cached credentials for the domain if step 1 was skipped, as specified in [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.) and [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.). Depending on the chosen SIP security mechanism for client authentication either digest authentication, client side authentication of Transport Layer Security, or a combination of both is used to provide the AS with a strong assurance about the identity of Alice.

Step 3. AS Authorizes the SIP Request and Forwards it to Callee
First, the AS authorizes the received INVITE message as specified in [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.) and [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.). If the authorization is successful, the AS constructs and caches a SAML assertion asserting Alice's profile attributes required by Bob's domain (example2.com), and also containing a the domain's (example.com) public key certificate, or a reference to it. The AS constructs a

HTTP-based SAML URI Reference incorporating the assertion's Assertion ID (see Section 2.3.3 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005.)). The AS uses this URI and puts the value into the token-info parameter.

The AS determines which profile attributes (if any) to assert in the <AttributeStatement> via local configuration and/or obtaining example2.com's metadata [OASIS.saml-metadata-2.0-os] (Cantor, S., Moreh, J., Philpott, R., and E. Maler, "Metadata for the Security Assertion Markup Language (SAML) V2.0," March 2005.). The AS then sends the updated INVITE message to Bob.

Step 4. Callee Dereferences HTTP-based SAML URI Reference

Bob's UAC or SIP Proxy receives the message and begins verifying it per the "Verifier Behavior" specified in [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.). In order to accomplish this task, it needs to obtain Alice's domain certificate. It obtains the HTTP-based SAML URI reference from the message's token-info parameter and dereferences it per Section 9.1 (SAML HTTP-URI-based SIP Binding). Note that this is not a SIP message, but an HTTP message [RFC2616] (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.).

Step 5. AS Returns SAML Assertion

Upon receipt of the above HTTP request, which contains an embedded reference to Alice's SAML Assertion, Alice's AS returns her assertion in an HTTP response message.

Upon receipt of Alice's SAML Assertion, the AS continues its verification of the INVITE message. If successful, it returns a 200 OK message directly to Alice. Otherwise it returns an appropriate SIP error response.

Step 6. Callee Returns SIP 200 OK to Caller

If Bob determines, based upon Alice's identity as asserted by the AS, and as further substantiated by the information in the SAML assertion, to accept the INVITE, he returns a SIP 200 OK message directly to Alice.

TOC

7.1.3. Profile Description

The following sections provide detailed definitions of the individual profile steps. The relevant illustration is Figure 3 (AS-driven SIP SAML Attribute Fetch Profile: Message Flow), below. Note that this profile is agnostic to the specific SIP request, and also that the Sender and Authentication Service (AS) may be seperate or co-located in actuality.

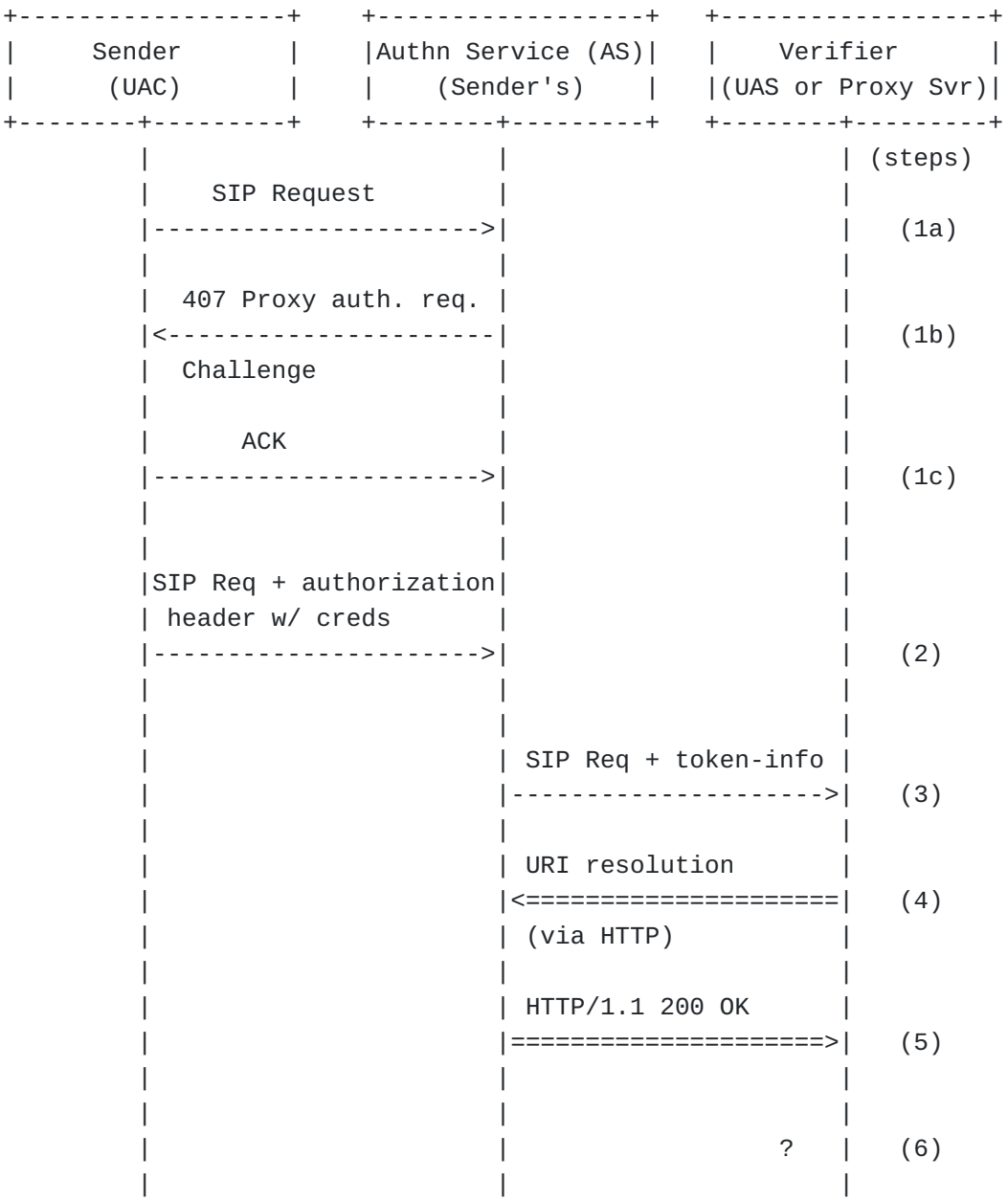


Figure 3: AS-driven SIP SAML Attribute Fetch Profile: Message Flow

7.1.3.1. Initial SIP Transaction between Sender and AS

TOC

This optional step maps to Steps 1 and 2 of Section 5 "Authentication Service Behavior" of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.). If the SIP request sent by the caller in substep 1a is deemed insufficiently authenticated by the AS per the rules stipulated by [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) Steps 1 and 2, then the AS MUST authenticate the sender of the message. The particulars of how this is accomplished depend upon implementation and/or deployment instantiation as discussed in [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.). Substeps 1b and 1c as shown in Figure 3 (AS-driven SIP SAML Attribute Fetch Profile: Message Flow) are non-normative and illustrative only.

7.1.3.2. Sender sends SIP Request Message with Authorization Credentials to the AS

TOC

This step maps to Steps 1 and 2 of Section 5 "Authentication Service Behavior" of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.). This request is presumed to be made in a context such that the AS will not challenge it -- i.e., the AS will consider the sender of the message to be authenticated. If this is not true, then this procedure reverts back to Step 1, above.

Otherwise, the AS carries out all other processing of the message as stipulated in [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) Steps 1 and 2, and if successful, this procedure procedes to the next step below.

TOC

7.1.3.3. AS Authorizes the SIP Request and Forwards it to Verifier

This first portion of this step maps to Steps 3 and 4 of Section 5 "Authentication Service Behavior" of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), which the AS MUST perform, although with the following additional substeps:

> The AS MUST construct a SAML assertion according to the "Assertion Profile Description (Assertion Profile Description)" specified in Section 8.1 (Assertion Profile Description) of this specification.
>
> The AS SHOULD construct an HTTPS, and MAY construct an HTTP, URI per Section "3.7.5.1 URI Syntax" of [OASIS.saml-bindings-2.0-os] (Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and E. Maler, “Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).
>
> The AS MUST use the URI constructed in the immediately preceding substep as the value of the token-info parameter that is added to the SIP request message.

Upon successful completion of all of the above, the AS forwards the request message.
At this point in this step, after perhaps traversing some number of intermediaries, the SIP request message arrives at a SIP network entity performing the "verifier" role. This role and its behavior are specified in Section 6 "Verifier Behavior" of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.). The verifier MUST perform the steps enumerated in the aforementioned section, with the following modifications:

> Step 1 of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) Section 6 maps to and is updated by, the following two steps in this procedure.
>
> Steps 2, 3, and 4 of [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) Section 6 may be mapped across this latter portion of this step, and/or the following two steps, as appropriate.

TOC

7.1.3.4. Verifier Dereferences HTTP-based SAML URI Reference

The verifier SHOULD ascertain whether it has a current cached copy of the SIP message sender's SAML assertion and domain certificate. If not, or if the verifier chooses to (e.g., due to local policy), it MUST dereference the the HTTP-based SAML URI Reference found in the SIP message's token-info parameter. To do so, the verifier MUST employ the "SAML HTTP-URI-based SIP Binding (SAML HTTP-URI-based SIP Binding)" specified in Section 9.1 (SAML HTTP-URI-based SIP Binding).

7.1.3.5. AS Returns SAML Assertion

TOC

This step also employs Section 9.1 (SAML HTTP-URI-based SIP Binding) "SAML HTTP-URI-based SIP Binding (SAML HTTP-URI-based SIP Binding)".
If the prior step returns an HTTP error (e.g., 4xx series), then this procedure terminates and the verifier returns (upstream) a SIP 436 'Bad token-info' Response code.
Otherwise, the HTTP response message will contain a SAML assertion and be denoted as such via the MIME media type of "application/samlassertion+xml" [IANA.application.samlassertion-xml] (OASIS Security Services Technical Committee (SSTC), "application/samlassertion+xml MIME Media Type Registration," December 2004.). The verifier MUST perform the verification steps specified in Section 8.2 (Assertion Verification) "Assertion Verification (Assertion Verification)", below. If successful, then this procedure continues with the next step.

7.1.3.6. Verifier performs Next Step

TOC

The SIP request was successfully processed. The verifier now performs its next step, which depends at least in part on the type of SIP request it received.

7.2. Caller-driven SIP SAML Conveyed Assertion Profile

TOC

For the "Assertion-by-value" profile we assume that a SAML assertion is obtained out-of-band and attached to the body of the SIP message. Note that any SIP message may be used to convey the SAML assertion even though SIP INVITE may be the most appropriate candiate. The verification step described in Section 8.2 (Assertion Verification) is applicable to this profile as well as the description on the content of

the assertion illustrated in Section 8.1 (Assertion Profile Description).

---

8. Assertion Profile

TOC

This section provides some guidance on what information should be put into a SAML assertion by the SAML Authority and how that information is then used by the Verifier.

8.1. Assertion Profile Description

TOC

The schema for SAML assertions themselves is defined in Section 2.3 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).
An example SAML assertion, formulated according to this profile is given in Section 10 (Example SAML Assertions).
Overall SAML assertion profile requirements:

> If a SAML assertion is signed then it MUST be signed by the same key that is used in the Transport Layer Security mechanism utilized with HTTPS. Signing of SAML assertions is defined in Section 5.4 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).

In the following subsections, the SAML assertion profile is specified element-by-element, in a top-down, depth-first manner, beginning with the outermost element, "<Assertion>". Where applicable, the requirements for an element's XML attributes are also stated, as a part of the element's description. Requirements for any given element or XML attribute are only stated when, in the context of use of this profile, they are not already sufficiently defined by [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).

8.1.1. Element: <Assertion>

TOC

> **Attribute: ID**
>
> The value for the ID XML attribute SHOULD be allocated randomly such that the value meets the randomness

> requirments specified in Section 1.3.4 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.).
>
> **Attribute: IssueInstant**
>
> The value for the IssueInstant XML attribute SHOULD be set at the time the SAML assertion is created (and cached for subsequent retrieval). This time instant value MAY be temporally the same as that encoded in the SIP message's Date header, and MUST be at least temporally later, although it is RECOMMENDED that it not be 10 minutes or more later.

8.1.1.1. Element: <Issuer>

TOC

The value for the Issuer XML element MUST be a value that matches either the Issuer or the Issuer Alternative Name fields [RFC3280] (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) in the certificate conveyed by the SAML assertion in the ds:X509Certificate element located on this path within the SAML assertion:

```
<Assertion
  <ds:Signature
    <ds:KeyInfo
      <ds:X509Data
        <ds:X509Certificate
```

8.1.1.2. Element: <Subject>

TOC

The <Subject> element SHOULD contain both a <NameID> element and a <SubjectConfirmation> element.
The value of the <NameID> element MUST be the Address of Record (AoR).
The <SubjectConfirmation> element attribute Method SHOULD be set to the value:

> urn:oasis:names:tc:SAML:2.0:cm:sender-vouches

Although it MAY be set to some other implementation- and/or deployment-specific value. The <SubjectConfirmation> element itself SHOULD be empty.

8.1.1.3. Element: <Conditions>

TOC

The <Conditions> element SHOULD contain an <AudienceRestriction> element, which itself SHOULD contain an <Audience> element. When included the value of the <Audience> element MUST be the same as the addr-spec of the SIP request's To header field.
The following XML attributes of the <Conditions> element MUST be set as follows:

> **Attribute: NotBefore**
>
> The value of the NotBefore XML attribute MUST be set to a time instant the same as the value for the IssueInstant XML attribute discussed above, or to a later time.
>
> **Attribute: NotOnOrAfter**
>
> The value of the NotOnOrAfter XML attribute MUST be set to a time instant later than the value for NotBefore.

8.1.1.4. Element: <AttributeStatement>

TOC

The SAML assertion MAY contain an <AttributeStatement> element. If so, the <AttributeStatement> element will contain attribute-value pairs, e.g., of a user profile nature, encoded according to either one of the "SAML Attribute Profiles" as specified in [OASIS.saml-profiles-2.0-os] (Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., and E. Maler, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.), or encoded in some implementation- and/or deployment-specific attribute profile.
The attribute-value pairs SHOULD in fact pertain to the entity identified in the SIP From header field, since a SAML assertion formulated per this overall section is stating that they do.

TOC

8.2. Assertion Verification

This section specifies the steps that a verifier has to perform to verify a SAML assertion created according to the profile from Section 8.1.1 (Element: <Assertion>).
The steps are:

1. Before Step 1 in Section 6 of [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.), the verifier MUST extract the AS's domain certificate from the <ds:X509Certificate> XML element at the end of the element path given in Section 8.1.1.1 (Element: <Issuer>).

2. Perform Step 1 in Section 6 of [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.).

3. After Step 1 in Section 6 of [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.), but before Step 2 of that section, the verifier MUST verify the SAML assertion's signature via the procedures specified in Section 5.4 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005.) as well as [W3C.xmldsig-core] (Eastlake, D., Reagle , J., and D. Solo, "XML-Signature Syntax and Processing," October 2000.). The 479 'Invalid SAML Assertion' response code is used when the verifier is unable to process the SAML assertion.

4. Perform Step 2 in Section 6 of [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.).

5. Verify that the signer of the SIP message's Identity header field is the same as the signer of the SAML assertion, if SIP Identity is used to bind the token-info parameter to the SIP signaling message. Note that without such protection certain attacks are feasible as described in Section 11 (Security Considerations).

6. Verify that the content of the SAML assertion matches with the information carried in the SIP message. This may include the following checks:

7. Verify that the SAML assertion's <Issuer> element value matches the Issuer or the Issuer Alternative Name fields [RFC3280] (Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509

Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," April 2002.) in the AS's domain certificate.

8. Verify that the SAML assertion's <NameID> element value is the same as the Address of Record (AoR) value.

9. Verify that the SAML assertion's <SubjectConfirmation> element value is set to whichever value was configured at implementation- or deployment-time. The default value is:

   > urn:oasis:names:tc:SAML:2.0:cm:sender-vouches

10. Verify that the SAML assertion contains an <Audience> element, and that its value matches the value of the addr-spec of the SIP To header field.

11. Verify that the validity period denoted by the NotBefore and NotOnOrAfter attributes of the <Conditions> element meets the requirements given in Section 8.1.1.3 (Element: <Conditions>).

---

9. SAML SIP Binding

TOC

This section specifies one SAML SIP Binding at this time. Additional bindings may be specified in future revisions of this specification. The description in Section 8.1 (Assertion Profile Description) is applicable to this profile.

9.1. SAML HTTP-URI-based SIP Binding

TOC

This section specifies the "SAML HTTP-URI-based SIP Binding", (SHUSB). The SHUSB is a profile of the "SAML URI Binding" specified in Section 3.7 of [OASIS.saml-bindings-2.0-os] (Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and E. Maler, "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005.). The SAML URI Binding specifies a means by which SAML assertions can be referenced by URIs and thus be obtained through resolution of such URIs.
This profile of the SAML URI Binding is congruent with the SAML URI Binding -- including support for HTTP-based URIs being mandatory to implement -- except for the following further restrictions which are specified in the interest of interoperability (section numbers refer to [OASIS.saml-bindings-2.0-os] (Cantor, S., Hirsch, F., Kemp, J.,

Philpott, R., and E. Maler, “Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.):

> **Section 3.7.5.3 Security Considerations:** Support for TLS 1.0 or SSL 3.0 is mandatory to implement.
>
> **Section 3.7.5.4 Error Reporting:** All SHOULDs in this section are to be interpreted as MUSTs.

---

10. Example SAML Assertions

TOC

This section presents two examples of a SAML assertion, one unsigned (for clarity), the other signed (for accuracy).
In the first example, Figure 4 (Unsigned SAML Assertion Illustrating Conveyance of Subject Attribute), the assertion is attesting with respect to the subject (lines 7-15) "Alice@example.com" (line 11). The validity conditions are expressed in lines 16-23, via both a validity period expressed as temporal endpoints, and an "audience restriction" stating that this assertion's semantics are valid for only the relying party named "example2.com". Also, the assertion's issuer is noted in lines 4-5.
The above items correspond to some aspects of this specification's SAML assertion profile, as noted below in Security Considerations dicussions, see: Section 11.1 (Man-in-the-Middle Attacks and Stolen Assertions) and Section 11.3 (Forged Assertion).
In lines 24-36, Alice's telephone number is conveyed, in a "typed" fashion, using LDAP/X.500 schema as the typing means.

```
<Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
   IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
   xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   <Issuer>
      example.com
   </Issuer>
   <Subject>
      <NameID
        Format=
        "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
        Alice@example.com
      </NameID>
      <SubjectConfirmation
        Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
   </Subject>
   <Conditions NotBefore="2003-04-17T00:46:02Z"
               NotOnOrAfter="2003-04-17T00:51:02Z">
      <AudienceRestriction>
         <Audience>
            example2.com
         </Audience>
      </AudienceRestriction>
   </Conditions>
   <AttributeStatement>
      <saml:Attribute
   xmlns:x500=
     "urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
   NameFormat=
     "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
   Name="urn:oid:2.5.4.20"
   FriendlyName="telephoneNumber">
         <saml:AttributeValue xsi:type="xs:string">
               +1-888-555-1212
         </saml:AttributeValue>
      </saml:Attribute>
   </AttributeStatement>
</Assertion>
```

Figure 4: Unsigned SAML Assertion Illustrating Conveyance of Subject Attribute

---

In the second example, Figure 5 (Signed SAML Assertion Illustrating Conveyance of Subject Attribute), the information described above is the same, the addition is that this version of the assertion is signed. All the signature information is conveyed in the <ds:signature>

element, lines 7-47. Thus this assertion's origin and its integrity are assured. Since this assertion is the same as the one in the first example above, other than having a signature added, the second example below addresses the same Security Considerations aspects, plus those requiring a Signature.

```
<Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
   IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
   xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   <Issuer>
      example.com
   </Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference
          URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
           <ds:Transforms>
              <ds:Transform
                  Algorithm=
         "http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform
                 Algorithm=
                    "http://www.w3.org/2001/10/xml-exc-c14n#">
                 <InclusiveNamespaces
                    PrefixList="#default saml ds xs xsi"
                    xmlns=
                     "http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
           </ds:Transforms>
           <ds:DigestMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
           <ds:DigestValue>
              Kclet6XcaOgOWXM4gty6/UNdviI=
           </ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
        hq4zk+ZknjggCQgZm7ea8fI7...Hr7wHxvCCRwubfZ6RqVL+wNmeWI4=
      </ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
             <ds:X509Certificate>
    MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxNVBAYTAlVT
    MRIwEAYDVQQIEwlXaXNjb .....  dnP6Hr7wHxvCCRwubnZAv2FU78pLX
    8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdioG8cCx3w/w==
             </ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
```

```
48    <Subject>
49       <NameID
50         Format=
51       "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
52         Alice@example.com
53       </NameID>
54       <SubjectConfirmation
55        Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
56    </Subject>
57    <Conditions NotBefore="2003-04-17T00:46:02Z"
58                NotOnOrAfter="2003-04-17T00:51:02Z">
59       <AudienceRestriction>
60          <Audience>
61             example2.com
62          </Audience>
63       </AudienceRestriction>
64    </Conditions>
65    <AttributeStatement>
66       <saml:Attribute
67    xmlns:x500=
68      "urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
69    NameFormat=
70      "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
71    Name="urn:oid:2.5.4.20"
72    FriendlyName="telephoneNumber">
73          <saml:AttributeValue xsi:type="xs:string">
74                +1-888-555-1212
75          </saml:AttributeValue>
76       </saml:Attribute>
77    </AttributeStatement>
78 </Assertion>
```

Figure 5: Signed SAML Assertion Illustrating Conveyance of Subject Attribute

11. Security Considerations

TOC

This section discusses security considerations when using SAML with SIP.

11.1. Man-in-the-Middle Attacks and Stolen Assertions

TOC

Threat:

By making SAML assertions available via HTTP-based requests by a potentially unbounded set of requesters, it is conceivably possible that anyone would be able to simply request one and obtain it. By SIP intermediaries on the signaling path for example. Or, an HTTP intermediary/proxy could intercept the assertion as it is being returned to a requester.

The attacker could then attempt to utilize the SAML assertion in another exchange in order to impersonate the subject (the putative caller) to some SIP-based target entity.

Countermeasures:

Such an attack is implausible for several reasons. The primary reason is that a message constructed by an imposter using a stolen assertion that conveys the public key certificate of some domain will not verify because the values in the SAML assertion, which are tied to the SIP message, will not verify.

Furthermore, the SIP SAML assertion may contain restrictions regarding the parties it can be used by. Finally, the assertion should be signed and thus causing any alterations to break its integrity and make such alterations detectable.

11.2. Privacy

TOC

Threat:

The ability for other entities to obtain additional information about an individual, such as role in an organization or other authorization relevant information raises privacy concerns.

Since the SAML assertion itself is not confidentiality protected nor the exchange of the reference to the SAML assertion an intermediary or a third party adversary would be allowed to gain additional information about an individual

Countermeasures:

To address the threats three cases need to be differentiated.

First, a third party that did not participate in any of the exchange is prevented from eavesdropping on the content of the SAML assertion by employing confidentiality protection of the SIP signaling exchange as well as the HTTP exchange. This ensures

that an eavesdropper on the wire is unable to obtain information. However, this does not prevent intermediaries, such as SIP proxies from observing a URL to a SAML assertion (in the token-info parameter). To deal with this second type of attacker depending on the environment where such a threat must be addressed it is necessary to authenticate the entity that tries to resolve the reference to a SAML assertion and to only provide a positive response (with the SAML assertion) if the requestor is authorized to obtain the desired information. When a SAML assertion is carried inband then such a protection is more difficult to accomplish as the SAML assertion would have to be confidentiality protected with the key of the intented recipient, for example using S/MIME. Finally, the last type of threat concerns the intented recipient of the SAML assertion itself. Proper permissions for the distribution of information about the caller via the content of the SAML assertion to certain recipients need to be available. This permission must be provided by the caller itself or, in certain circumstances, by someone on behalf of the caller. From a technical point of view, some form of authorization policies will be required.

11.3. Forged Assertion

TOC

Threat:

A malicious user could forge or alter a SAML assertion in order to communicate with the SIP entities.

Countermeasures:

To avoid this kind of attack, the entities must assure that proper mechanisms for protecting the SAML assertion are employed, e.g., signing the SAML assertion itself or protecting the transport of the SAML assertion from the AS to the verifying party using TLS. Section 5.1 of [OASIS.saml-core-2.0-os] (Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” March 2005.) specifies the signing of SAML assertions.

Additionally, the assertion content dictated by the SAML assertion profile herein ensures ample evidence for a relying party to verify the assertion and its relationship with the received SIP request.

11.4. Replay Attack

TOC

Threat:

Theft of SIP message protected by the mechanisms described herein and replay of it at a later time.

Countermeasures:

The SAML assertion may contain several elements to prevent replay attacks. There is, however, a clear tradeoff between the replaying an assertion and re-using it over multiple SIP exchanges/sessions.

Additionally, the SAML assertion can be tied to the SIP exchange with the help of the SIP Identity mechanism. RFC 4474 [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) signs certain header fields and the SIP message body and thereby helps to protect message modifications. If a recipient knows that all messages from a certain originator arrive with SIP Identity protection applies then downgrading attacks are not possible.

---

12. Contributors

TOC

The authors would like to thank Marcus Tegnander and Henning Schulzrinne for his contributions to earlier versions of this document.

---

13. Acknowledgments

TOC

We would like to thank RL 'Bob' Morgan, Stefan Goeman, Shida Schubert, Jason Fischl, Sebastian Felis, Nie Pin, Marcos Dytz, Erkki Koivusalo, Richard Barnes, Marc Willekens, Marc Willekens, Steffen Fries and Vijay Gurbani for their comments to this draft.
Eric Rescorla also provided a detailed review of the document. We would like to thank him for his feedback.
The "AS-driven SIP SAML URI-based Attribute Assertion Fetch Profile" is based on an idea by Jon Peterson.

TOC

14. IANA Considerations

When a SAML assertion is attached to the body of the message then the "application/samlassertion+xml" MIME media type is used. This MIME type is already registered with IANA and no further action is required from IANA.

14.1. URI Parameter

TOC

This document extends the registry of URI parameters, as defined RFC 3969 [RFC3969] (Camarillo, G., “The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP),” December 2004.) with the following value:
Parameter Name: token-info
Predefined Values: No
Reference: This document

14.2. 477 'Binding to SIP Message failed' Response Code

TOC

This document registers a new SIP response code. It is sent when a verifier receives a SAML assertion but the Subject and Condition elements cannot be matched to the content in the SIP message, i.e., the binding between the SIP message and the SAML assertion cannot be accomplished. This response code is defined by the following information, which has been added to the method and response-code sub-registry under http://www.iana.org/assignments/sip-parameters.
Response Code Number: 477
Default Reason Phrase: Binding to SIP Message failed

14.3. 478 'Unknown SAML Assertion Content' Response Code

TOC

This document registers a new SIP response code. It is used when the verifier is unable to parse the content of the SAML assertion, because, for example, the assertion contains only unknown elements in in the SAML assertion, or the SAML assertion XML document is garbled. This response code is defined by the following information, which has been added to the method and response-code sub-registry under http://www.iana.org/assignments/sip-parameters.
Response Code Number: 478
Default Reason Phrase: Unknown SAML Assertion Content

14.4. 479 'Invalid SAML Assertion' Response Code

TOC

This document registers a new SIP response code. It is used when the verifier is unable to process the SAML assertion. A verifier may be unable to process the SAML assertion in case the assertion is self-signed, or signed by a root certificate authority for whom the verifier does not possess a root certificate. This response code is defined by the following information, which has been added to the method and response-code sub-registry under http://www.iana.org/assignments/sip-parameters.
Response Code Number: 479
Default Reason Phrase: Invalid SAML Assertion

15. Change Log

TOC

RFC Editor - Please remove this section before publication.

15.1. -06 to -07

TOC

Undo changes made in version 6.
Removed the header fields and switched to a URI parameter
Editorial changes

15.2. -05 to -06

TOC

Defined a new SIP Identity signature mechanism.

15.3. -04 to -05

TOC

Changed the document type to experimental
Removed option tag
Added the Caller-driven SIP SAML Conveyed Assertion Profile
Defined a new header (SAML-Info)
Changed the description for usage with this new header
Updated security considerations

Minor editorial cleanups

15.4. -03 to -04

TOC

Updated IANA consideration section.
Added option tag
Updated acknowledgments section
Minor editorial changes to the security considerations section

---

15.5. -02 to -03

TOC

Denoted that this I-D is intended to update RFC4474 per SIP working group consensus at IETF-69. This is the tact adopted in order to address the impedance mismatch between the nature of the URIs specified as to be placed in the Identity-Info header field, and what is specified in RFC4474 as the allowable value of that header field.
Added placeholder "TBD" section for a to-be-determined "call-by-value" profile, per SIP working group consensus at IETF-69.
Removed use-case appendicies (per recollection of JHodges during IETF-69 discussion as being WG consensus, but such is not noted in the minutes).

15.6. -00 to -02

TOC

Initial specifications to kickstart the work.

---

16. References

TOC

16.1. Normative References

TOC

[OASIS.saml-bindings-2.0-os]	Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and E. Maler, “Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard saml-bindings-2.0-os, March 2005.
[OASIS.saml-core-2.0-os]	Cantor, S., Kemp, J., Philpott, R., and E. Maler, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard saml-core-2.0-os, March 2005.
[OASIS.saml-metadata-2.0-os]	Cantor, S., Moreh, J., Philpott, R., and E. Maler, “Metadata for the Security Assertion Markup Language (SAML) V2.0,” OASIS Standard saml-metadata-2.0-os, March 2005.
[OASIS.saml-profiles-2.0-os]	Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., and E. Maler, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard OASIS.saml-profiles-2.0-os, March 2005.
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2392]	Levinson, E., “Content-ID and Message-ID Uniform Resource Locators,” RFC 2392, August 1998 (TXT, HTML, XML).
[RFC2585]	Housley, R. and P. Hoffman, “Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP,” RFC 2585, May 1999 (TXT).
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1,” RFC 2616, June 1999 (TXT, PS, PDF, HTML, XML).
[RFC3261]	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 (TXT).
[RFC3280]	Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 3280, April 2002 (TXT).
[RFC3515]	Sparks, R., “The Session Initiation Protocol (SIP) Refer Method,” RFC 3515, April 2003 (TXT).
[RFC3553]	Mealling, M., Masinter, L., Hardie, T., and G. Klyne, “An IETF URN Sub-namespace for Registered Protocol Parameters,” BCP 73, RFC 3553, June 2003 (TXT).
[RFC3893]	

	Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," RFC 3893, September 2004 (TXT).
[RFC3969]	Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)," BCP 99, RFC 3969, December 2004 (TXT).
[RFC4234]	Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," RFC 4234, October 2005 (TXT, HTML, XML).
[RFC4474]	Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," RFC 4474, August 2006 (TXT).
[RFC4484]	Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)," RFC 4484, August 2006 (TXT).
[W3C.xmldsig-core]	Eastlake, D., Reagle , J., and D. Solo, "XML-Signature Syntax and Processing," W3C Recommendation xmldsig-core, October 2000.

16.2. Informative References

TOC

[I-D.ietf-oauth-v2]	Hammer-Lahav, E., Recordon, D., and D. Hardt, "The OAuth 2.0 Protocol," draft-ietf-oauth-v2-10 (work in progress), July 2010 (TXT).
[IANA.application.samlassertion-xml]	OASIS Security Services Technical Committee (SSTC), "application/samlassertion+xml MIME Media Type Registration," IANA MIME Media Types Registry application/samlassertion+xml, December 2004.
[OASIS.saml-conformance-2.0-os]	Mishra, P., Philpott, R., and E. Maler, "Conformance Requirements for the Security Assertion Markup Language (SAML) V2.0," OASIS Standard saml-conformance-2.0-os, March 2005.
[OASIS.saml-glossary-2.0-os]	Hodges, J., Philpott, R., and E. Maler, "Glossary for the Security Assertion Markup Language (SAML) V2.0," OASIS Standard saml-glossary-2.0-os, March 2005.

[OASIS.saml-sec-consider-2.0-os]	Hirsch, F., Philpott, R., and E. Maler, "Security and Privacy Considerations for the OASIS Security Markup Language (SAML) V2.0," OASIS Standard saml-sec-consider-2.0-os, March 2005.
[OASIS.sstc-saml-exec-overview-2.0-cd-01]	Madsen, P. and E. Maler, "SAML V2.0 Executive Overview," OASIS SSTC Committee Draft sstc-saml-exec-overview-2.0-cd-01, April 2005.
[OASIS.sstc-saml-protocol-ext-thirdparty-cd-01]	Cantor, S., "SAML Protocol Extension for Third-Party Requests," OASIS SSTC Committee Draft sstc-saml-protocol-ext-thirdparty-cd-01, March 2006.
[OASIS.sstc-saml-tech-overview-2.0-draft-16]	Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., and T. Scavo, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-16, May 2008.
[RFC2543]	Handley, M., Schulzrinne, H., Schooler, E., and J. Rosenberg, "SIP: Session Initiation Protocol," RFC 2543, March 1999 (TXT).
[RFC2693]	Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and T. Ylonen, "SPKI Certificate Theory," RFC 2693, September 1999 (TXT).
[RFC3281]	Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization," RFC 3281, April 2002 (TXT).
[RFC3323]	Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)," RFC 3323, November 2002 (TXT).

Authors' Addresses

TOC

	Hannes Tschofenig
	Nokia Siemens Networks

	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at
	Jeff Hodges
Email:	Jeff.Hodges@KingsMountain.com
	Jon Peterson
	NeuStar, Inc.
	1800 Sutter St Suite 570
	Concord, CA 94520
	US
Email:	jon.peterson@neustar.biz
	James Polk
	Cisco
	2200 East President George Bush Turnpike
	Richardson, Texas 75082
	US
Email:	jmpolk@cisco.com
	Douglas C. Sicker
	University of Colorado at Boulder
	ECOT 430
	Boulder, CO 80309
	US
Email:	douglas.sicker@colorado.edu