Session Initiation Protocol
SIP Working Group
Internet-Draft
Intended status: Experimental
Expires: January 8, 2009

A. Pashalidis
J. Girao
NEC Europe Ltd.

July 7, 2008

SIP SAML Profile and Binding
draft-pashalidis-sip-saml-00

Status of this Memo

Abstract

This document specifies the SIP/SAML profile and binding, i.e. a protocol for the use of Security Assertion Markup Language (SAML) assertions for the purposes of authentication and the exchange of attributes in a Session Initiation Protocol (SIP) environment.

Table of Contents

1. Introduction

This document specifies the SIP/SAML profile and binding, i.e. a protocol for the authentication of Session Initiation Protocol (SIP) users by means of Security Assertions Markup Language (SAML) assertions, and for the exchange of user attributes over the SIP protocol.

SAML is a set of protocol specifications that provide, among other things, seamless Single Sign-On (SSO) in a distributed environment where a user wishes to log into multiple Service Providers (SPs). In particular, once a user has authenticated himself towards a trusted entity called the "Identity Provider" (IDP), the SAML protocols enable the IDP and the SPs to exchange information about the user's authentication status at the IDP in a secure manner and in a way that takes into account the user's privacy. Moreover, the SAML protocols enable the SPs and the IDP to exchange information about the user in the form of attributes. This feature is useful in the context of identity management systems that perform such attribute exchanges in an automated way, while enabling the user to exercise control over the dissemination of his personal information.

However, the SAML protocols are not self-contained in the sense that they require a transport mechanism. In particular, SAML messages need to be conveyed from one party to the other by some underlying transport protocol. The encoding of SAML messages in such transport protocols is called a SAML binding; multiple such bindings have been specified in the past. Examples are the HTTP REDIRECT binding, the HTTP POST binding, and the SOAP binding [SAMLBINDINGS].

With each newly specified SAML profile and binding, the number and the diversity of applications and services that can interoperate with any given SAML-based IDP increases. This adds value to the overall system, because it enables the user to log into a larger and more diverse set of services in a seamless manner. Moreover, the number of services that can query the user's attributes from the IDP

increases, resulting in a potentially more personalised experience for the user.

This document specifies the SIP/SAML profile. This profile is used in the case where the service provider is a SIP proxy. The main use case for this profile is a user who would like to register at this a SIP proxy by means of the SIP REGISTER method, and who would like to be authenticated at the SIP proxy by means of a SAML Assertion that is issued by his IDP.

The remainder of this document is structured as follows.

- Section 2 provides an overview of the terminology and the abbreviations used in this document.
- Section 3 specifies the `Direct' variant of the SIP/SAML profile.
- Section 4 specifies the `Artifact' variant of the SIP/SAML profile.
- Section 5 specifies how certain errors are handled in the SIP/SAML profile.
- Section 6 specifies the SIP/SAML binding.
- Section 7 discusses important security aspects of the protocols.

2. Terminology

This document makes use of terms defined in [RFC3261] and [SAML]. In addition, the keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

3. SIP/SAML Direct Variant

In this section, the Direct Variant of the SIP/SAML profile is specified. In the following, UA denotes the user agent (client), SP denotes a SIP Proxy, and IDP denotes a SAML-based Identity Provider. This specification relies on a new SIP header, called the `SAML-Endpoint (SAML-EP)' header. This header contains a URI endpoint pointing to the user's SAML-based IDP. The format of the SAML-EP header is specified in section Section 6.3 in detail.

1. UA -> SP : SIP REGISTER + SAML-EP header(s)

2. SP -> UA : SIP 302 REDIRECT [SIDP URI] + SAML request

3. UA -> IDP : SIP REGISTER + SAML request

4. UA <-> IDP: AUTHENTICATION

5. UA <- IDP : SIP 302 REDIRECT [SP URI] + SAML response

6. UA -> SP : SIP REGISTER + SAML response

Figure 1: The Direct Variant of the SIP/SAML Profile

Figure 1 shows the direct variant of the SAML/SIP profile in full i.e. where the user authenticates himself at the IDP for the first time. The figure shows individual steps that occur during the protocol execution. With the exception of step 4, all the steps uniquely correspond to a particular message that is exchanged in the corresponding step. In the following, we say `message X' in order to refer to the message that is exchanged in step X of the protocol.

First, the UA constructs a SIP REGISTER message and sends it to the SP (message 1). This message MUST contain one or more SAML-EP headers, where the value of each SAML-EP header MUST be one or more URIs. All the indicated URIs MUST belong to some SAML-based IDP that is able to consume SIP REGISTER messages conforming to the format of message 3. The population of the SAML-EP header values is the responsibility of the UA. If multiple SAML-EP header values are present in message 1 (either in the same or in multiple SAML-EP headers), then each URI within a SAML-EP header value MUST refer to a different IDP. Also, each URI within a SAML-EP header value MUST refer to an IDP where the user maintains an active account. However, there is no requirement to include more than IDP URI, even if the user maintains accounts at multiple IDPs. Moreover, the order of the URIs within SAML-EP header values SHOULD reflect the user's preferences, most preferred first. That is, if the user prefers to

be authenticated by IDP A in preference to IDP B, then the URI referring to IDP A SHOULD be included in a SAML-EP header before the URI referring to IDP B.

The following two possibilities exist when message 1 is received by the SP. Case 1: the SP does not support the SIP/SAML profile specified in this document. In this case, the SAML-EP header(s) are ignored, and the SP responds 'normally', i.e. as in standard SIP.

The UA MUST be able to correctly handle a message conforming to standard SIP (instead of message 2 in Figure 1) as a response to message 1. Case 2: the SP supports the SIP/SAML profile. In this case, it MUST examine the SAML-EP headers and check whether or not an agreement exists with at least one of the indicated IDPs. If an agreement exists with at least one of them, then it MUST pick one of those with whom an agreement exists; the one it selects is denoted by SIDP. The SP SHOULD select the IDP that corresponds to the first URI within any SAML-EP header with whom an agreement exists. If no agreement consists with any of the IDPs then the SP MUST act as if it does not support the SIP/SAML profile specified in this document, i.e. respond with a message conforming to 'standard' SIP.

After the SIDP has been selected, the SP MUST decide with which SAML/SIP profile it would like to proceed. This decision MAY be based on a policy or similar criteria. If the 'SIP Artifact' profile profile is selected, then the remainder of the processing and the protocol is as described in section Section 4. Otherwise, i.e. if the 'direct' profile is selected, then processing continues as follows.

Message 2 is constructed as follows. The SP constructs a SIP 302 REDIRECT message where the value of the 'Contact' header is equal to the value of the SAML-EP header (from message 1) that corresponds to the SIDP. This value is denoted by SIDP URI in Figure 1. Moreover, message 2 MUST contain a SAML Request, which MUST be constructed according to [SAML]. This SAML Request MUST be included into message 2 according to the SIP/SAML binding specified in Section 6.1.

Upon reception of message 2, the UA SHOULD check that the SIDP URI indicated in the 'Connect' header is one of those proposed in message 1. If this is not the case, then the UA MAY abort the protocol execution at this point. It also MAY inform the user about the inconsistency, and it MAY ask for the user's permission on whether to proceed with the given SIDP URI. It is RECOMMENDED that the UA does not proceed with the protocol execution if the indicated SIDP URI is not one of the ones proposed in message 1, unless the user explicitly allows the protocol execution to continue.

After reception of message 2, the UA MUST decide how to proceed in trying to obtain a SAML Response that matches the SP's SAML Request

in message 2. Multiple possibilities MAY exist for this, and this

specification does not impose the UA to use any particular method. However, if the UA decides to continue with the `Direct Variant' of the SIP/SAML profile, then it MUST proceed as follows.

It constructs message 3 as a new SIP REGISTER message, which is sent to the SIDP URI. The message contains the SAML Request from message 2, which is included according to the SIP/SAML binding specified in Section 6.1. Note that, since message 3 is sent to an IDP (which is NOT a SIP Proxy), its purpose it not to register at a SIP Proxy; its purpose is to trigger authentication at the IDP.

In step 4 of the protocol, IDP authenticates the user. This may involve multiple messages between the UA and the IDP. This specification does not impose any particular authentication mechanism. However, in order to guarantee minimal interoperability, the standard SIP user authentication mechanism (Digest Authentication, see section 22 of [RFC3261]) MUST be implemented at both the IDP and the UA. However, whether or not the IDP will choose this method or some other method, is dependent on policy.

After the authentication of the user towards the IDP, the IDP constructs message 5. This is a SIP 302 REDIRECT message where the 'Contact' header MUST contain a value that is extracted from the SAML request in 3, according to [SAML]. According to [SAML], the SAML Response contains the description of an authentication context if the user's authentication in step 4 has been successful. If this is the case, the authentication context in the SAML Response MUST describe the user's authentication context that resulted from the authentication in step 4. The SAML Response is included in message 5 according to the SIP/SAML binding, as specified in Section 6.1.

Finally, the UA constructs a new SIP REGISTER message and sends this to the SP in step 6. This SIP REGISTER message MUST contain the SAML Response from message 5, according to the SIP/SAML binding specified in Section 6.1. Upon reception of that message, the SP MUST examine the SAML Response according to [SAML]. If the SP is satisfied, the user is recorded as 'registered' in the SIP Proxy, and the remaining processing continues according to standard SIP [RFC3261].

4. SIP-Artifact Variant

This section specifies the SIP-Artifact Variant of the SIP/SAML Profile. The main difference between the SIP-Artifact Variant and the Direct Variant is that, in the SIP-Artifact Profile, the UA cannot see the SAML messages that are exchanged between the SP and the IDP. Instead, the SP and the IDP exchange SAML messages directly. Special identifiers that identify individual SAML messages, called `SAML Artifacts' are tunneled through the UA.

1. UA -> SP : SIP REGISTER + a SAML-EP header(s)
2. SP -> UA : SIP 302 REDIRECT [SIDP URI + Artifact] + SAML-EP header
3. UA -> IDP : SIP REGISTER + Artifact + SAML-EP header
4. IDP <-> SP: Artifact Resolution
5. UA <-> IDP: AUTHENTICATION
6. UA <- IDP : SIP 302 REDIRECT [SP URI + Artifact] + SAML-EP header
7. UA -> SP : SIP REGISTER + Artifact + SAML-EP header
8. SP <-> IDP: Artifact Resolution

Figure 2: The SIP-Artifact Variant of the SIP/SAML Profile

Figure 2 shows the SIP-Artifact variant of the SAML/SIP profile in full i.e. where the user authenticates himself at the IDP for the first time. The figure shows individual steps that occur during the protocol execution. With the exception of steps 4, 5, and 8 all the steps uniquely correspond to a particular message that is exchanged in the corresponding step. In the following, we say `message X' in order to refer to the message that is exchanged in step X of the protocol.

First, the UA constructs a SIP REGISTER message and sends it to the SP (message 1). This message is constructed in a manner identical to the construction of the first message in the `direct' variant, as specified in the section above. The behaviour of the SP after having received message 1 is identical to the behaviour specified for the `direct' variant in the section above, up to the point where the SP decides which variant to use. If the SP decides to use the

`Artifact' variant, the processing is as follows.

The SP MUST construct a SAML Artifact pointing to a SAML Request message for consumption by the SIDP, according to [SAML]. Message 2 is then constructed as a SIP 302 REDIRECT message, where the `Contact' header MUST take as value the URI indicated by the SAML-Endpoint header (from message 1) that corresponds to the SIDP, modified as follows. The SAML Artifact MUST be encoded into the URI, according to the binding specified in Section 6.2.

Moreover, message 2 MUST contain exactly one SAML-EP header, where the value is the URI at which the SP will accept a SAML Artifact Resolution request from the SIDP.

Upon reception of message 2, the UA SHOULD check that the SIDP URI indicated in the 'Connect' header is one of those proposed in message 1. If this is not the case, then the UA MAY abort the protocol execution at this point. It also MAY inform the user about the inconsistency, and it MAY ask for the user's permission on whether to proceed with the given SIDP URI. It is RECOMMENDED that the UA does not proceed with the protocol execution if the indicated SIDP URI is does not correspond to any of those that were proposed in message 1, unless the user explicitly allows the protocol execution to continue.

The UA constructs message 3 as a new SIP REGISTER message, which is sent to the SIDP URI. Message 3 MUST contain a single SAML-EP header, with a value identical to the value of the SAML-EP header from message 2. Since message 3 is sent to an IDP (which is NOT a SIP Proxy), its purpose it not to register at a SIP Proxy; its purpose is to trigger authentication at the IDP.

In step 4 of the protocol, the IDP resolves the SAML Artifact found in the query string of the URI from message 3, into a SAML Request message. This is done by means of the Artifact Resolution protocol specified in [SAMLART]. The SAML binding the is used for this exchange MUST be the the SIP/SAML binding specified in section Section 6. Moreover, the SAML Endpoint that the IDP uses for initiating the exchange is the one indicated in the SAML-EP header in message 3.

If the SAML Artifact has sucessfully been resolved into a SAML

Request message, in step 5 of the protocol the IDP authenticates the user. This corresponds to step 4 in the 'direct' variant specified in the previous section, and the requirements concerning this steps are identical to the requirements in the 'direct' variant.

After the authentication of the user towards the IDP, the IDP MUST construct a SAML Artifact pointing to a SAML Response message for consumption by the SP, according to [SAML]. Message 6 is then constructed as a SIP 302 REDIRECT message, where the `Contact' header

MUST take the value of an specific URI that is extracted from the SAML request in 3, according to [SAML], modified as follows. The SAML Artifact MUST be encoded into the URI, according to the binding specified in Section 6.2.

The SAML Response to which the SAML Artifact points, MUST contain the description of an authentication context if the user's authentication in step 5 has been successful. If this is the case, the authentication context in the SAML Response MUST describe the user's authentication context that resulted from the authentication in step 5.

Moreover, message 6 MUST contain exactly one SAML-Endpoint header, where the value is the URI at which the IDP will accept a SAML Artifact Resolution request from the SP.

Upon reception of message 6, the UA constructs message 7 as a new SIP REGISTER message. Message 7 MUST contain exactly one SAML-Endpoint header, where the value is identical to the value of the SAML-Endpoint header from message 6. Message 7 is then sent to the URI indicated in the 'Contact' header of message 6.

In step 8 of the protocol, the IDP resolves the SAML Artifact found in the query string of the URI from message 7, into a SAML Response message. This is done by means of the Artifact Resolution protocol specified in [SAMLART]. The SAML binding the is used for this exchange MUST be the the SIP/SAML binding specified in section Section 6. Moreover, the SAML Endpoint that the SP uses for initiating the exchange is the one indicated in the SAML-Endpoint header of message 7.

5. Error handling

This section specifies how certain errors are handled within SIP/SAML Profile.

TBD.

6. The SIP/SAML bindings

This section specifies the SIP transport for SAML messages and SAML Artifacts.

6.1. SIP/SAML message encoding

A SIP message that carries a SAML message MUST include the SAML message as the SIP message body. A 'Content-Type' header MUST be included in the SIP message, with a value of 'text/xml'. The message body MUST consist solely of the SAML message which MUST be constructed according to [SAML]. The SIP message MUST otherwise conform to the format of a standard SIP message. This includes respecting the rules regarding the character encoding and the presence of a 'Content-Length' header - see [RFC3261]

6.2. SIP/SAML artifact encoding

There are three mechanisms to embed the SAML artifact into the message: in the SIP URI, a SIP header or in the body of the SIP message. While the advantage of the first lies in freeing the body of the SIP message to carry other information, the other two conform better to existing SIP specifications. This specification mandates that, should the SIP/SAML artifact binding be supported, then Section 6.2.3 MUST be supported, while Section 6.2.1 and Section 6.2.2 are optional.

6.2.1. SIP/SAML URI artifact encoding

A SAML Artifact is encoded into a URI that occurs in a SIP message. A URI into which a SAML Artifact is encoded is said to 'carry' the SAML Artifact. Multiple URIs in the same SIP message MAY carry a SAML Artifact. However, each URI MUST carry at most one SAML Artifact. Whether or not a SAML Artifact is carried by a URI occurring in a SIP message, is specified in the SIP/SAML profiles.

A SAML Artifact is encoded into a URI as follows. If the URI does not have a query string component, then the URI MUST be appended with a query component containing the parameter 'SAMLart' with the value being the SAML Artifact in question. If the URI already contains a query string component with other parameters, then the other parameters MUST remain intact. If the URI already contains a query string parameter with the name "SAMLart", where the matching algorithm MUST be case-insensitive, then this parameter MUST be replaced.

6.2.2. SIP/SAML Content artifact encoding

A SAML Artifact is encoded into the body of a SIP message as follows. A 'Content-Type' header MUST be included in the SIP message with the value 'text/xml'. The message body MUST contain only the artifact in XML format, which is detailed below. Otherwise, the message should abide to the format of a standard SIP message.

The XML message will belong to the namespace described in [SAML] and MUST contain only one element of type 'urn:oasis:names:tc:SAML:2.0:protocol:Artifact' with the name

'SAMLart'. This element MUST contain the artifact value.

6.2.3. SIP/SAML artifact header

This section specifies the format of the SAML Artifact Header. The SAML Artifact header follows the header and grammar rules as specified in section 7.1 of [RFC3261].

```
header  =  "SAMLart" HCOLON SAMLart-value
```

Figure 3: The SAML-Endpoint Header Format

The SAMLart-value MUST be a valid base-64 encoded string.

6.3. The SAML-Endpoint Header

This section specifies the format of the SAML-Endpoint Header. The SAML-Endpoint header follows the header and grammar rules as they are specified in section 7.1 of [RFC3261].

```
header  =  "SAML-Endpoint" HCOLON header-value *(COMMA URI-value)
```

Figure 4: The SAML-Endpoint Header Format

The URI-value MUST be a valid URI as specified in [RFC2396].

7. Security Considerations

This specification introduces SAML-based user authentication in the context of the SIP REGISTER method. As such, the privacy and

security considerations described in [SAMLSEC] apply to this specification. The remainder of this section discusses requirements that are specific to this document.

It is important to keep in mind that a SAML Assertion (which is part of the SAML Response from the IDP) is sensitive information that must be kept secret. Similarly, the SAML Artifact, which is part of the IDP's response in the Artifact variant, is also sensitive information. This is because knowledge of the assertion, in particular the IDP's signature which is part of it, or knowledge of the artifact, enables one to login (i.e. register) in the name of the subject for which the assertion or artifact was generated.

The SAML assertion / artifact MUST therefore be conveyed from the IDP to the SP in a way that preserves its confidentiality and its integrity. The only exception to this rule is the case where the authentication mechanism with which the user is authenticated at the IDP involves the user's password being transmitted over the network in the clear. In this case, the confidentiality and the integrity of the SAML assertion / artifact SHOULD be protected along its way from the IDP to the SP. The use of a user authentication mechanism which involves the transmission of the user's password in the clear is NOT RECOMMENDED.

In the "Direct" variant, protecting the SAML Assertion's confidentiality and integrity requires protection both during the transmission of the assertion from the IDP to the UA, and its transmission from the UA of the SP. The protection mechanism that is used MUST provide confidentiality and integrity protection against active attackers. It is RECOMMENDED that a TLS channel with server-side certificates is used both for the transmission of the assertion from the IDP to the UA, and from the UA to the SP.

If a TLS channel is used for the transmission on the path IDP->UA, then the IDP MUST NOT propose or select a TLS ciphersuite with an effective key strength which is lower than the effective key strength of its signature over the SAML Assertion. The IDP MUST use independently generated keys for TLS and for signing SAML Assertions.

If a TLS channel is used for the transmission on the path US->SP, then the UA MUST NOT propose or select a TLS ciphersuite with an effective key strength which is lower than the effective key strength of the signature over the SAML Assertion.

In the "Artifact" variant, too, the use of TLS with server-side certificates is RECOMMENDED. The same considerations and requirements as above apply. Moreover, the communication between the IDP and the SP for the purposes of SAML Artifact Resolution MUST be authenticated, and the integrity and the confidentiality of this communication MUST be protected. The following alternatives for the protection of the direct communication between IDP and the SP are RECOMMENDED. Note that all these alternatives result in a 'secure channel' between the IDP and the SP.

- A long-lived TLS connection that is authenticated based on server-side and client-side certificates.

- A long-lived IPsec connection where both parties are authenticated based on a certificate.

The session key of secure channel MUST be at least as strong as the key used by the IDP to sign SAML Assertions. It is the responsibility of the IDP to reject incomong connection attempts from SPs that do not provide for the minimum required protection level.

[RFC3766] SHOULD be used in order to compare the effective key strengths.

8. IANA Considerations

TBD. (None?)

9. Acknowledgements

TBD.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[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.

[RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", RFC 3766, April 2004.

[SAML] Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[SAMLBINDINGS] Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and E. Maler, "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[SAMLSEC] Hirsch, F., Philpott, R., and E. Maler, "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[utf8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 3629.

Authors' Addresses

Andreas Pashalidis
NEC Europe Ltd.
Kurfuersten Anlage 36
Heidelberg D-69115
Germany

Phone: +49 (0)6221 4342 205
Fax: +49 (0)6221 4342 155
Email: andreas.pashaldis@nw.neclab.eu

Joao Girao
NEC Europe Ltd.
Kurfuersten Anlage 36
Heidelberg D-69115
Germany

Phone: +49 (0)6221 4342 117
Fax: +49 (0)6221 4342 155
Email: joao.girao@nw.neclab.eu

Full Copyright Statement

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.

Intellectual Property

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.