ABFAB
Internet-Draft
Intended status: Informational
Expires: May 3, 2012

J. Howlett
JANET(UK)
S. Hartman
Painless Security
October 31, 2011

A RADIUS Attribute, Binding and Profiles for SAML draft-ietf-abfab-aaa-saml-02

Abstract

This document specifies a RADIUS attribute, binding and two profiles for the Security Assertion Mark-up Language (SAML). The attribute provides RADIUS encapsulation of SAML protocol messages, while the binding describes the transport of this attribute, and the SAML protocol messages within, using RADIUS. The profiles describe the application of this binding for Abfab authentication and assertion query/request. The SAML RADIUS attribute and binding are defined generically to permit application in other scenarios, such as network access.

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 May 3, 2012.

Table of Contents

1. Introduction

The SAML RADIUS attribute, binding and profiles are motivated by the requirements of the Abfab architecture [I-D.lear-abfab-arch]. In this architecture, it is often desirable to convey Security Assertion Mark-up Language (SAML) protocol messages between a SAML requester and SAML responder; for example, to allow a Relying Party to obtain a SAML assertion containing attributes that describe a principal.

SAML [OASIS.saml-core-2.0-os] defines a number of SAML protocol messages that are used for a range of different purposes [OASIS.saml-profiles-2.0-os]. These messages are derived from common request and reponse abstract types. These request and response protocol messages can be exchanged using a variety of underlying transport protocols, such as HTTP. In the SAML model, the means by which a SAML protocol message exchange is framed over an underlying transport protocol is known as a SAML 'binding'. SAML already defines [OASIS.saml-bindings-2.0-os] a number of mainly HTTP-based bindings; these principally use HTTP as the underlying transport protocol, generally for use with the SAML Web Browser Single Sign-On Profile [OASIS.saml-profiles-2.0-os].

However, the goal of Abfab is to extend the applicability of federated identity beyond the Web to other application protocols by building on the AAA framework. Consequently here exists a requirement for an AAA-based binding, that is functionally equivalent to the existing bindings, that uses the RADIUS [RFC2865] and Diameter [RFC3588] protocols, rather than HTTP. This document defines a new RADIUS-based SAML binding, building on a SAML RADIUS attribute also defined by this document.

This attribute and binding are likely to be useful for purposes besides Abfab; an example of one potential application is SAML-based authorisation for network access. The attribute and binding are therefore defined generically to facilitate general applicability. Nonetheless it is useful to also define how the SAML RADIUS binding should be used for Abfab-specific purposes to facilitate interoperability. This document therefore also define two profiles of this binding to support authentication and assertion request.

To summarise, this document specifies:

- A SAML RADIUS attribute that defines how to encapsulate a SAML protocol message within a RADIUS attribute.

- A SAML RADIUS binding that defines how SAML requesters and responders can exchange SAML protocol messages.

- The Abfab Authentication Profile that defines how the SAML RADIUS binding is used to effect SAML-based authentication and authorisation within the Abfab architecture.

- The Abfab Assertion Request Profile that defines how the SAML RADIUS binding is used to effect SAML-based assertion request within the Abfab architecture.

The RADIUS SAML binding and profile specifications aspire to adhere to the guidelines stipulated by [OASIS.saml-bindings-2.0-os] and [OASIS.saml-profiles-2.0-os] respectively. To this end, the binding and profiles provide a 'Required Information' section that enumerates:

- A URI that uniquely identifies the protocol binding or profile

- Postal or electronic contact information for the author

- A reference to previously defined bindings or profiles that the new binding updates or obsoletes.

- In the case of a profile, any SAML confirmation method identifiers defined and/or utilized by the profile.

2. Conventions

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 RFC 2119 [RFC2119].

3. RADIUS SAML-Message Attribute

This attribute contains a SAML [OASIS.saml-core-2.0-os] protocol message. Where multiple SAML-Message attributes are included in a RADIUS message, the Message fields of these attributes are to be concatenated to form a single SAML message.

A summary of the SAML-Message format is shown below. The fields are transmitted from left to right.

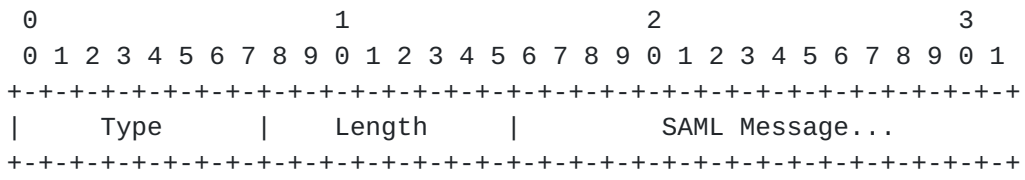


Figure 1

Type: TBD

Length: >=4

Message: The Message field is one or more octets containing a SAML message. If larger than a single attribute, the SAML message data MUST be split on 253-octet boundaries over as many attributes as necessary. The SAML message is reconstructed by concatenating the contents of all SAML-Message attributes.

TODO: request a new RADIUS attribute

4. SAML RADIUS Binding

The SAML RADIUS binding defines how RADIUS [RFC2865] can be used to enable a RADIUS client and server to exchange SAML protocol messages.

4.1. Required Information

Identification: TBD

Contact information: TBD

Updates: None.

4.2. Operation

RADIUS can be used over multiple underlying transports; this binding calls out the use of RADIUS over UDP as REQUIRED. It is RECOMMENDED that the RADIUS exchange is protected using TLS encryption for RADIUS [I-D.ietf-radext-radsec] to provide confidentiality and improve integrity protection.

The system model used for SAML conversations over RADIUS is a simple request-response model, using the RADIUS SAML-Message attribute defined in Section 3 to encapsulate the SAML protocol messages.

1. The RADIUS client, acting as a SAML requester, transmits a SAML request element within a RADIUS Access-Request message. This message MUST include a single instance of the RADIUS User-Name attribute whose value MUST conform to the Network Access Identifier [RFC4282] scheme. The NAI SHOULD be used to route the message towards the SAML responder, which MAY be more than one RADIUS hop distant. The SAML requester MUST NOT include more than one SAML request element.

2. The RADIUS server, acting as a SAML responder, MAY return a SAML protocol message within a RADIUS Access-Accept or Access-Reject

message. The SAML responder MUST NOT include more than one SAML response. A SAML responder that refuses to perform a message exchange with the SAML requester MUST silently discard the SAML request.

A SAML responder MAY also return an unsolicited responser (a SAML response generated and emitted in the absence of a request from a SAML requester).

This binding is intended to be composed with any use of RADIUS, such as network access. Therefore, other arbitrary RADIUS attributes MAY be used in either the request of response.

In the case of a SAML processing error and successful authentication, the RADIUS server SHOULD include a SAML-specified <samlp:Status> element in the SAML response that is transported within the Access-Accept packet sent by the RADIUS server.

In the case of a SAML processing error and failed authentication, the RADIUS server MAY include a SAML-specified <samlp:Status> element in the SAML response that is transported within the Access-Reject packet sent by the RADIUS server.

4.2.1. Metadata Considerations

There are no metadata considerations particular to this binding.

5. Abfab Authentication Profile

In the scenario supported by the Abfab Authentication Profile, a Principal controlling a User Agent requests access to a Relying Party. The User Agent and Relying Party use the GSS EAP mechanism to authenticate the Principal. The Relying Party, acting as an EAP pass-through authenticator, acts as a conduit for the EAP frames emitted by the User Agent and an EAP server which acts as the Principal's Identity Provider. If the Identity Provider successfully authenticates the Principal, it produces an authentication assertion which is consumed by the Relying Party. During this process, a name identifier might also be established between the Relying Party and the Identity Provider.

5.1. Required Information

Identification: TBD

Contact information: TBD

SAML Confirmation Method Identifiers: The SAML V2.0 "sender vouches"

confirmation method identifier, urn:oasis:names:tc:SAML:2.0:cm:sender-vouches, is used by this profile.

Updates: None.

5.2. Profile Overview

To implement this scenario, a profile of the SAML Authentication Request protocol is used in conjuction with the SAML RADIUS binding defined in Section 4 and the GSS EAP mechanism [I-D.ietf-abfab-gss-eap].

This profile is based on the SAML Web Browser Single Sign-On Profile [OASIS.saml-profiles-2.0-os]. There are some important differences between these profiles; specifically:

- Authentication. This profile specifically calls out the use of a particular authentication framework (although not a particular authentication mechanism). This is necessary so that the profile is able to build on the AAA and GSS frameworks.

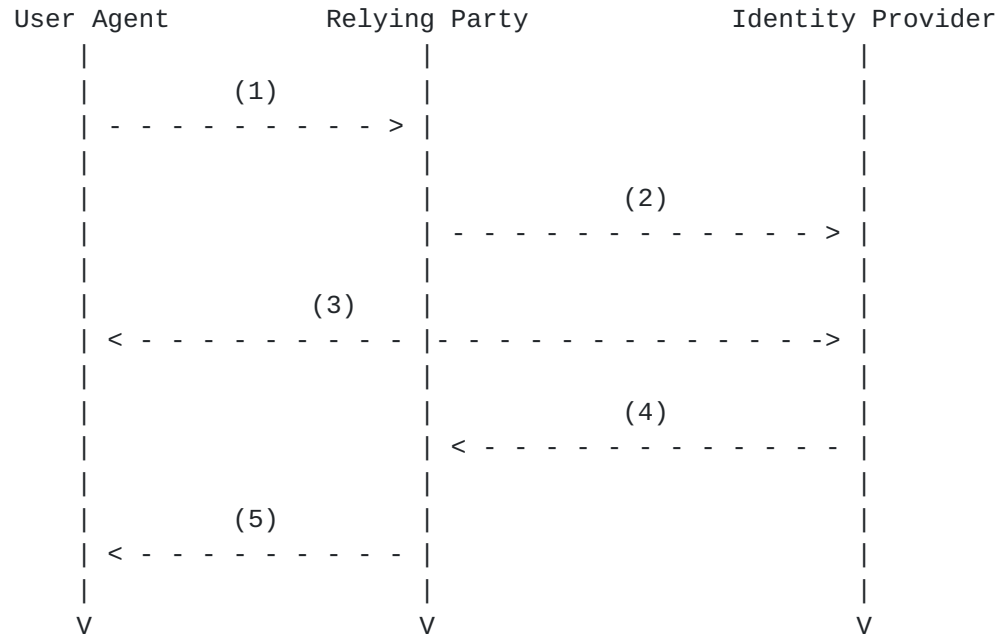
- Bindings. This profile does not use any HTTP-based bindings; instead, all SAML protocol messages are transported using the SAML RADIUS binding defined in Section 4. This is intended to minimize the number of bindings that interoperable implementations must support.

- Signatures. This profile prohibits the use of digital signatures in SAML elements. This includes signatures in the <samlp: AuthnRequest>, <samlp:Response> and <saml:Assertion> elements. Message source authentication and integrity are provided by the binding's transport. This is intended to simplify the trust model and reduce the size of the SAML payloads.

- Requests. The profile does not permit the Relying Party to name the <saml:Subject> of the <samlp:AuthnRequest>. This is intended to simplify the business logic of interoperable implementations.

- Responses. The profile only permits the Identity Provider to return a single assertion that must contain exactly one authentication statement. Other statements may be included within this assertion at the disgression of the Identity Provider. This is intended to simplify the business logic of interoperable implementations.

Figure 1 below illustrates the flow of messages within this profile.



The following steps are described by the profile. Within an individual step, there may be one or more actual message exchanges.

Figure 1

1. User Agent Request to Relying Party (Section 5.3.1): In step 1, the Principal, via a User Agent, makes a request for a secured resource at the Relying Party. The Relying Party determines that no security context for the User Agent exists and initiates GSS EAP authentication of the Principal.

2. Relying Party Issues <samlp:AuthnRequest> to Identity Provider (Section 5.3.2). In step 2, the Relying Party issues a <samlp: AuthnRequest> message to be delivered to the Identity Provider using the SAML RADIUS binding.

3. Identity Provider Identifies Principal (Section 5.3.3). In step 3, the Principal is identified by the Identity Provider using EAP authentication, while honoring any requirements imposed by the Relying Party in the <samlp:AuthnRequest> message.

4. Identity Provider Issues <samlp:Response> to Relying Party (Section 5.3.4). In step 4, the Identity Provider issues a <samlp:Response> message to the Relying Party using the SAML RADIUS binding. The response either indicates an error or includes an authentication statement in exactly one assertion.

5. Relying Party Grants or Denies Access to Principal (Section 5.3.5). In step 5, having received the response from the Identity Provider, the Relying Party can respond to the Principal's User Agent with its own error, or can establish its own security context for the Principal and return the requested resource.

Note that an Identity Provider can initiate this profile at step 4 and issue a <samlp:Response> message to a Relying Party without the preceding steps.

5.3. Profile Description

The Abfab Authentication Profile is a profile of the SAML V2.0 Authentication Request Protocol [OASIS.saml-core-2.0-os]. Where this specification conflicts with Core, the former takes precedence.

If the profile is initiated by the Relying Party, start with Section 5.3.1. If initiated by the Identity Provider, start with Section 5.3.4.

5.3.1. User Agent Request to Relying Party

The profile is initiated by an arbitrary User Agent request to the Relying Party. There are no restrictions on the form of the request. The Relying Party is free to use any means it wishes to associate the subsequent interactions with the original request. The Relying Party, acting as a GSS acceptor, MUST invoke the GSS EAP mechanism (either spontaneously or as the result of a mechanism negotiation) and send an EAP-Identity/Request message to the User Agent, acting as a GSS initiator.

5.3.2. Relying Party Issues <samlp:AuthnRequest> to Identity Provider

The Relying Party, on receiving the EAP-Response/Identity message from the User Agent, MUST send it towards the Identity Provider using the SAML RADIUS binding. The Relying Party MAY include a <samlp: AuthnRequest> within this RADIUS Access-Request message. The next hop destination MAY be the Identity Provider or alternatively an intermediate RADIUS proxy.

Profile-specific rules for the contents of the <samlp:AuthnRequest> element are given in Section 5.4.1.

5.3.3. Identity Provider Identifies Principal

The Identity Provider MUST establish the identity of the Principal using EAP authentication, or else it will return an error. If the

ForceAuthn attribute on the <samlp:AuthnRequest> element is present and true, the Identity Provider MUST freshly establish this identity rather than relying on any existing session state it may have with the Principal (for example, TLS state that may be used for session resumption). Otherwise, and in all other respects, the Identity Provider may use any EAP method to authenticate the Principal, subject to the requirements of Section 5.8 of [I-D.ietf-abfab-gss-eap]. and any others called out in the <samlp: AuthnRequest> message.

5.3.4. Identity Provider Issues <samlp:Response> to Relying Party

Regardless of the success or failure of the <samlp:AuthnRequest>, the Identity Provider MUST produce a <samlp:Response> message to be delivered to the Relying Party using the SAML RADIUS binding.

Profile-specific rules regarding the contents of the <samlp:Response> element are given in Section 5.4.2.

5.3.5. Relying Party Grants or Denies Access to Principal

The Relying Party MUST process the <samlp:Response> message and any enclosed <saml:Assertion> elements as described in [OASIS.saml-core-2.0-os]. Any subsequent use of the <saml:Assertion> elements is at the discretion of the Relying Party, subject to any restrictions on use contained within the assertions themselves or previously established out-of-band policy governing interactions between the Identity Provider and the Relying Party.

To complete the profile, the Relying Party creates a GSS security context for the User Agent.

5.4. Use of Authentication Request Protocol

This profile is based on the Authentication Request Protocol defined in [OASIS.saml-core-2.0-os]. In the nomenclature of actors enumerated in section 3.4, the Relying Party is the requester, the User Agent is the attesting entity and the Principal is the Requested Subject.

5.4.1. <samlp:AuthnRequest> Usage

A Relying Party MAY include any message content described in [OASIS.saml-core-2.0-os], Section 3.4.1. All processing rules are as defined in [OASIS.saml-core-2.0-os].

If the Identity Provider cannot or will not satisfy the request, it MUST respond with a <samlp:Response> message containing an

appropriate error status code or codes.

If the Relying Provider wishes to permit the Identity Provider to establish a new identifier for the principal if none exists, it MUST include a <saml:NameIDPolicy> element with the AllowCreate attribute set to "true". Otherwise, only a principal for whom the Identity Provider has previously established an identifier usable by the Relying Party can be authenticated successfully.

The Relying Party MUST NOT include a <saml:Subject> element in the request. The authenticated EAP Identity implicitly names the Principal of the requested <samlp:AuthnRequest> to the Identity Provider.

The <samlp:AuthnRequest> message MUST NOT be signed. Authentication and integrity are provided by the RADIUS SAML binding.

5.4.2. <samlp:Response message> Usage

If the Identity Provider wishes to return an error, it MUST NOT include any assertions in the <samlp:Response message>. Otherwise, if the request is successful (or if the response is not associated with a request), the <samlp:Response> element MUST conform to the following:

- It MUST NOT be signed.
- It MUST contain exactly one <saml:Assertion>. The <saml:Subject> element of this assertion MUST refer to the authenticated Principal.
- The assertion MUST contain a <saml:AuthnStatement>. This MUST contain a <saml:Subject> element with at least one <saml: SubjectConfirmation> element containing a Method of urn:oasis:names:tc:SAML:2.0:cm:sender-vouches that reflects the authentication of the Principal to the Identity Provider. If the containing message is in response to an <samlp:AuthnRequest>, then the InResponseTo attribute MUST match the request's ID.
- Other statements and confirmation methods MAY be included in the assertion at the discretion of the Identity Provider. In particular, <samlp:AttributeStatement> elements MAY be included. Deployers should be aware of the implications of allowing weaker confirmation as the processing as defined in section 2.4.1.1 of [OASIS.saml-core-2.0-os] is effectively satisfy-any.
- Other conditions MAY be included as requested by the Relying Party or at the discretion of the Identity Provider. The Identity

Provider is NOT obligated to honor the requested set of in the <samlp:AuthnRequest>, if any.

5.4.3. samlp:Response Message Processing Rules

The Relying Party MUST do the following:

- Verify that the InResponseTo attribute in the bearer <saml: SubjectConfirmationData> equals the ID of its original <samlp: AuthnRequest> message, unless the response is unsolicited, in which case the attribute MUST NOT be present.

- If a <saml:AuthnStatement> used to establish a security context for the Principal contains a SessionNotOnOrAfter attribute, the security context SHOULD be discarded once this time is reached, unless the service provider reestablishes the Principal's identity by repeating the use of this profile.

- Verify that any assertions relied upon are valid according to processing rules in [OASIS.saml-core-2.0-os].

- Any assertion which is not valid, or whose subject confirmation requirements cannot be met MUST be discarded and MUST NOT be used to establish a security context for the Principal.

5.4.4. Unsolicited Responses

An Identity Provider MAY initiate this profile by delivering an unsolicited <samlp:Response> message to a Relying Party.

An unsolicited <samlp:Response> MUST NOT contain an InResponseTo attribute, nor should any sender-vouches <saml: SubjectConfirmationData> elements contain one.

5.4.5. Use of the SAML RADIUS Binding

It is RECOMMENDED that the RADIUS exchange is protected using TLS encryption for RADIUS [I-D.ietf-radext-radsec] to provide confidentiality and improve integrity protection.

5.4.6. Metadata Considerations

There are no metadata considerations particular to this binding.

6. Abfab Assertion Query/Request Profile

7. Security Considerations

TODO

8. IANA Considerations

Assignments of additional enumerated values for the RADIUS attributes defined in this document are to be processed as described in [RFC3575], subject to the additional requirements of a published specification.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[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.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[I-D.ietf-radext-radsec] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "TLS encryption for RADIUS", draft-ietf-radext-radsec-09 (work in progress), July 2011.

[I-D.ietf-abfab-gss-eap] Hartman, S. and J. Howlett, "A GSS-API Mechanism for the Extensible Authentication Protocol", draft-ietf-abfab-gss-eap-04 (work in progress), October 2011.

9.2. Informative References

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[I-D.lear-abfab-arch] Howlett, J., Hartman, S., Tschofenig, H., and E. Lear, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture", draft-lear-abfab-arch-02 (work in progress), March 2011.

[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-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.

Authors' Addresses

Josh Howlett
JANET(UK)
Lumen House, Library Avenue, Harwell
Oxford OX11 0SG
UK

Phone: +44 1235 822363
EMail: Josh.Howlett@ja.net

Sam Hartman
Painless Security

Phone:
EMail: hartmans-ietf@mit.edu