SAML V2.0 EAP GSS SSO Profile Version 1.0

Committee Draft 00

March 18, 2010

Specification URIs:

This Version:

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].html

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].odt

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].pdf

Previous Version:

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].html

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].odt

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].pdf

Latest Version:

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].html

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].odt

http://docs.oasis-open.org/[tc-short-name]/[additional path/filename].pdf

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.

Thomas Hardjono, MIT

Editor(s):

Josh Howlett, Individual

Declared XML Namespace(s):

[list namespaces here]

Abstract:

This specification defines an SSO profile using the Generic Security Services Extensible Authentication Protocol mechanism.

Status:

This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committeees/sstc/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/sstc/ipr.php.

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/sstc/.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication 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 OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names, abbreviations, etc. here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

TODO

1.1 Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 [RFC 2119].

1.2 Normative References

[EAPGSS] S. Hartman, J. Howlett. *A GSS-API Mechanism for the Extensible Authentication Protocol*. IETF ID draft-howlett-eap-gss-00, March 2010. *http://tools.ietf.org/search/draft-howlett-eap-gss-00*.

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[RFC2246] T. Dierks. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See http://www.ietf.org/rfc/rfc2246.txt.

[SAMLCore] OASIS Standard**,** *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAMLProf] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SSL3] A. Frier et al. *The SSL 3.0 Protocol*. Netscape Communications Corp, November 1996.

[RFC 2743] J. Linn. *Generic Security Service Application Program Interface Version 2, Update 1*. IETF RFC 2743, Janurary 2000. http://www.ietf.org/rfc/rfc2743.txt.

[RFC 3748] B. Adoba et al. *Extensible Authentication Protocol (EAP)*. IETF RFC 3748. http://www.ietf.org/rfc/rfc3748.txt.

1.3 Non-normative References

[Reference] [reference citation]

2 SAML EAP GSS SSO Profile

In the scenario supported by the SAML EAP GSS SSO profile, a user agent requests access to a resource at a service provider. The user agent and the service provider use the Generic Security Service Application Program Interface (GSS-API) to exchange Extensible Authentication Protocol (EAP) messages.

Previous SSO profiles of SAML have only considered HTTP user agents. This SSO profile is intended to address a wider range of user agents, and specifically those that support the GSS-API.

The service provider passes these messages back and forth between the user agent and the identity provider which, if it successfully authenticates the principal, produces an authentication assertion. The service provider consumes the assertion to establish a security context for the user agent. During this process, a name identifier might also be established between the providers for the principal, subject to the parameters of the interaction and the consent of the parties.

To implement this scenario, a profile of the SAML Authentication Request protocol is used, in conjunction with the SAML AAA binding and the EAP GSS mechanism.

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:profiles:EAPGSS

Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

2.2 Profile Overview

Figure 1 below illustrates the basic template for achieving SSO. The following steps are described by the profile. Within an individual step, there may be one or more actual message exchanges depending on the binding used for that step and other deployment-specific behavior.

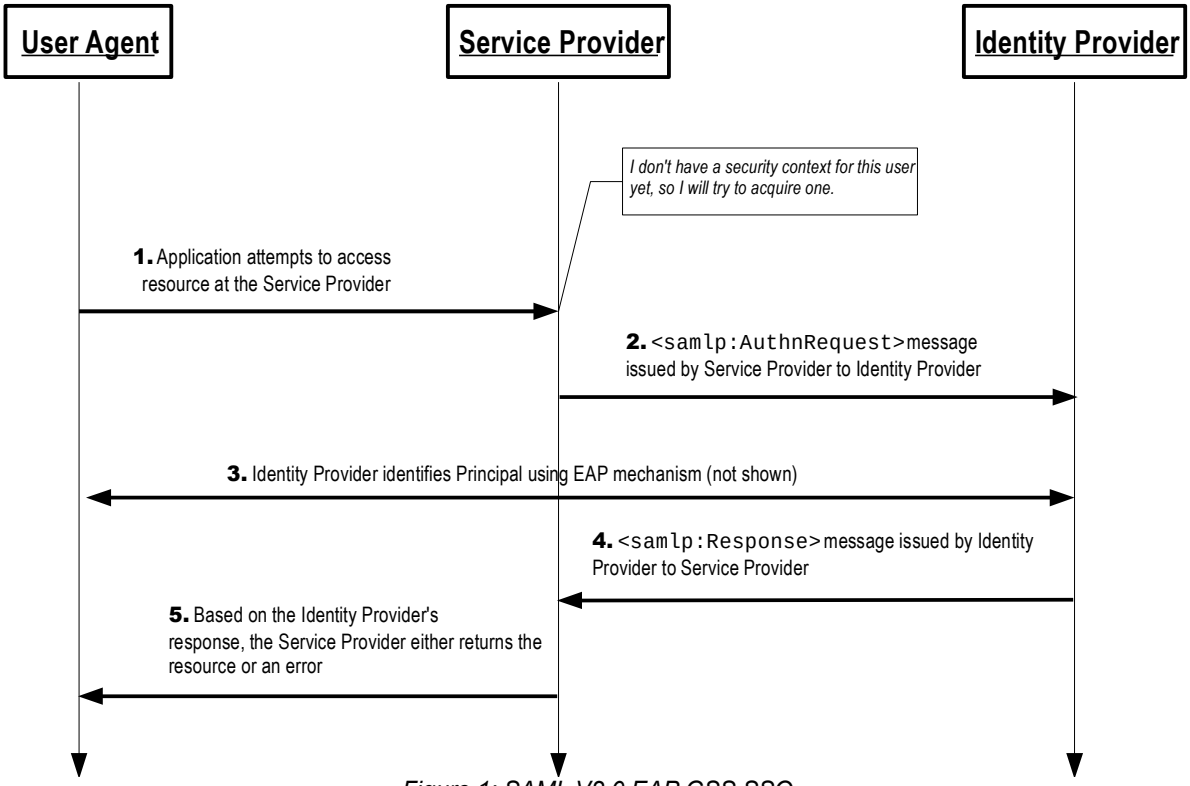

Figure 1: SAML V2.0 EAP GSS SSO

1. **User Agent Request to Service Provider** (section 2.3.1)

   In step 1, the principal, via a user agent, makes a request for a secured resource at the service provider. The service provider determines that no security context for the user agent exists and initiates EAP GSS SSO.

2. **Service Provider Issues <samlp:AuthnRequest> to Identity Provider** (section 2.3.2)

   In step 2, the service provider issues a `<samlp:AuthnRequest>` message to be delivered to the identity provider using the SAML AAA binding.

3. **Identity Provider Identifies Principal** (section 2.3.3)

   In step 3, the principal is identified by the identity provider using EAP, while honoring any requirements imposed by the service provider in the `<samlp:AuthnRequest>` message. This may require a new act of authentication, or it may reuse an existing authenticated session.

4. **Identity Provider Issues <samlp:Response> to Service Provider** (section 2.3.4)

   In step 4, the identity provider issues a `<samlp:Response>` message to the service provider using the SAML AAA binding. The response either indicates an error or includes at least one authentication statement in an assertion.

5. **Service Provider Grants or Denies Access to Principal** (section 2.3.5)

   In step 5, the SAML response is consumed by the service provider who either responds to the user agent by establishing a security context for the principal, or by returning an error.

2.3 Profile Description

The SAML V2.0 EAP GSS SSO Profile is a profile of the SAML V2.0 Authentication Request Protocol [SAMLCore]. Where this specification conflicts with Core, the former takes precedence. Processing rules for all messages are specified in section 2.4 of this profile.

2.3.1 User Agent Request to Service Provider

The profile is initiated by an arbitrary user agent request to the service provider. There are no restrictions on the form of the request. The service provider is free to use any means it wishes to associate the subsequent interactions with the original request. The service provider initiates the establishment of a GSS-API security context by invoking (and if necessary negotiating the use of) the EAP GSS mechanism. The `EAP-Request/Identity` message MUST be the first EAP message sent by the service provider.

2.3.2 Service Provider Issues <samlp:AuthnRequest> to Identity Provider

The service provider, on receiving the `EAP-Response/Identity` message from the user agent, MUST send it towards the identity provider using the SAML AAA binding, including a `<samlp:AuthnRequest>` within this request. The destination MAY be the identity provider, or an intermediate AAA proxy.

Profile-specific rules for the contents of the `<samlp:AuthnRequest>` element are given in section 2.4 .

2.3.3 Identity Provider Identifies Principal

At any time during the previous step or subsequent to it, the identity provider MUST establish the identity of the principal (or else it will return an error) prior to the issuance of the `<samlp:Response>` message. 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 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 any requirements called out in the `<samlp:AuthnRequest>` message; see section 2.4 for details.

2.3.4 Identity Provider Issues <samlp:Response> to Service Provider

Regardless of the success or failure of the `<samlp:AuthnRequest>`, the identity provider SHOULD produce a `<samlp:Response>` message to be delivered to the service provider using the SAML AAA binding.

Profile-specific rules regarding the contents of the `<samlp:Response>` element are included in section 2.4.3 .

2.3.5 Service Provider Grants or Denies Access to Principal

The service provider MUST process the `<samlp:Response>` message and any enclosed `<saml:Assertion>` elements as described in [SAMLCore] and section 2.4.4 below. Any subsequent use of the `<saml:Assertion>` elements is at the discretion of the service provider and other relying parties, 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 service provider.

To complete the profile, the service provider creates a security context for the user. The service provider MAY establish a security context with the user agent using any session mechanism it chooses.

2.4 Use of Authentication Request Protocol

This profile is based on the Authentication Request Protocol defined in [SAMLCore]. In the nomenclature of actors enumerated in section 3.4 of Core, the service provider is the requester and the relying party, the user agent is the attesting entity, and the principal is the requested subject. There may be additional relying parties at the discretion of the identity provider.

2.4.1 <samlp:AuthnRequest> Usage

A service provider MAY include any message content described in [SAMLCore], Section 3.4.1. All processing rules are as defined in [SAMLCore]. The `<saml:Issuer>` element MUST be present and MUST contain the unique identifier of the requesting service provider; the `Format` attribute MUST be omitted or have a value of `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`.

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 service 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 service provider can be authenticated successfully.

Note that the service provider MAY include a `<saml:Subject>` element in the request that names the actual identity about which it wishes to receive an assertion. This element MUST NOT contain any `<saml:SubjectConfirmation>` elements. If the identity provider does not recognize the principal as that identity, then it MUST respond with a `<samlp:Response>` message containing an error status and no assertions.

The `<samlp:AuthnRequest>` message MAY be signed.

2.4.2 <samlp:AuthnRequest> Message Processing Rules

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:

- The `<saml:Issuer>` element MAY be omitted, but if present it MUST contain the unique identifier of the issuing identity provider; the `Format` attribute MUST be omitted or have a value of `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`.
- It MUST contain at least one `<saml:Assertion>`. Each assertion's `<saml:Issuer>` element MUST contain the unique identifier of the issuing identity provider; the `Format` attribute MUST be omitted or have a value of `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`.
- The set of one or more assertions MUST contain at least one `<saml:AuthnStatement>` that reflects the authentication of the principal to the identity provider.
- At least one assertion containing an `<saml:AuthnStatement>` 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:bearer`.
- The bearer `<saml:SubjectConfirmation>` element described above MUST contain a `<saml:SubjectConfirmationData>` element that contains a `Recipient` attribute containing the service provider's unique entity identifier and a `NotOnOrAfter` attribute that limits the window during which the assertion can be delivered. It MUST NOT contain a `NotBefore`

attribute. 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(s) at the discretion of the identity provider.
- The assertion(s) containing a bearer subject confirmation MUST contain an <saml:AudienceRestriction> including the service provider's unique identifier as an <saml:Audience>.
- Other conditions (and other <saml:Audience> elements) MAY be included as requested by the service provider 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.

2.4.3 <samlp:Response> Usage

If the identity provider wishes to return an error in response to a request, it MUST NOT include any assertions in the <samlp:Response> message. Otherwise, the <samlp:Response> element MUST conform to the following rules:

- The <saml:Issuer> element of the <samlp:Response> element MAY be omitted, but if present it MUST contain the unique identifier of the issuing identity provider. The Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
- The response MUST contain at least one <saml:Assertion> element. Each assertion's <saml:Issuer> element MUST contain the unique identifier of the issuing identity provider, and the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
- The <saml:Subject> element of every assertion returned by the identity provider MUST refer to the authenticated principal.
- Any <saml:Subject> elements in the response MUST strongly match the <saml:Subject> element in the <samlp:AuthnRequest> element (if any) as required by [SAMLCore]. If the <samlp:AuthnRequest> element contains an explicit <saml:SubjectConfirmation> element and the identity provider is unable to produce a strongly matching <saml:Subject> element for any reason, the identity provider MUST return an error.
- Additional <saml:SubjectConfirmation> elements MAY be included in any assertion, though deployers should be aware of the implications of allowing weaker confirmation as the processing as defined in section 2.4.1.1 of [SAMLCore] is effectively satisfy-any. See section 3 for related considerations.
- Any assertion issued for consumption under this profile MUST contain a <saml:AudienceRestriction> element including the service provider's unique identifier in its <saml:Audience> element. Other conditions as defined in section 2.5 of [SAMLCore] (and other <saml:Audience> elements) MAY be included as requested by the service provider or at the discretion of the identity provider. All such conditions MUST be understood by and accepted by the service provider in order for the assertion to be considered valid.
- The set of one or more assertions MUST contain at least one <saml:AuthnStatement> element that reflects the authentication of the principal to the identity provider. Additional statements MAY be included in an assertion at the discretion of the identity provider.

- If the identity provider supports the Single Logout Profile [SAMLProf], a `<saml:AuthnStatement>` element issued for consumption using this profile MUST include a `SessionIndex` attribute to enable per-session logout requests by the service provider.

As indicated above, the identity provider MUST issue at least one `<saml:AuthnStatement>` element. The identity provider typically issues exactly one such element but MAY issue multiple `<saml:AuthnStatement>` elements (in multiple assertions) if the service provider requires multiple assertions for various purposes.

If the identity provider issues multiple `<saml:AuthnStatement>` elements, the values of the `IssueInstant` attributes and the content of the `<saml:SubjectLocality>` elements MUST be identical across the `<saml:AuthnStatement>` elements. The content of the `<saml:AuthnContext>` elements MAY vary across the `<saml:AuthnStatement>` elements, presumably because the consumers of the various assertions have different requirements with respect to authentication context.

2.4.4 <samlp:Response> Message Processing Rules

The service provider MUST do the following:

- Verify any signatures present on the assertion(s) and/or the response.
- Verify that the Recipient attribute in any bearer `<saml:SubjectConfirmationData>` matches the unique entity identifier to which the `<samlp:Response>` was delivered.
- Verify that the `NotOnOrAfter` attribute in any bearer `<saml:SubjectConfirmationData>` has not passed, subject to allowable clock skew between the providers.
- 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 [SAMLCore].

Any assertion that is not valid, or whose subject confirmation requirements cannot be met, SHOULD be discarded and SHOULD NOT be used to establish a security context for the principal.

If the response contains multiple assertions with multiple `<saml:AuthnStatement>` elements, the service provider MAY consume any one of them at its discretion. How the service provider makes this decision is unspecified.

2.5 Unsolicited Responses

An identity provider MAY initiate this profile by delivering an unsolicited `<samlp:Response>` message to a service provider.

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

2.6 SAML AAA Binding Usage

Assertions issued by the identity provider MAY be signed.

The use of TLS 1.0 [RFC2246] or its successors is RECOMMENDED as a means of authentication, integrity protection, and confidentiality.

2.7 EAP GSS Usage

In this profile, principals are authenticated by the identity provider using the Extensible Authentication Protocol (EAP). EAP messages are exchanged between the user agent and the service provider using the GSS-API [RFC 2743] and the EAP GSS-API mechanism [EAPGSS].

The EAP-GSS mechanism permits the encapsulated of any EAP method. This specification does not constrain which EAP methods are used.

In the EAP GSS-API mechanism, the GSS-API base key is obtained from the EAP MSK. Therefore, the EAP method SHOULD support EAP key derivation.

The EAP method SHOULD support EAP channel bindings to allow the EAP server to validate the service provider, in its role as an EAP authenticator.

The service provider, in its role as an EAP authenticator, MUST support EAP pass-through behavior.

2.8 Use of Metadata

TODO

2.9 Security Considerations

TODO

Conformance

The last numbered section in the specification must be the Conformance section. Conformance Statements/Clauses go here.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged

Participants:

- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]

Appendix B. Non-Normative Text

Appendix C. Revision History

Document ID	Date	Committer	Comment
sstc-saml-eapgss-sso-draft-00	15 Mar 2010	J.Howlett	Initial draft