SAML AAA Binding 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 a binding of SAML to AAA transport.

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

This specification defines a binding of SAML to AAA transports.

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

[RADDTLS] A. DeKok. *DTLS as a Transport Layer for RADIUS*. IETF ID draft-dekok-radext-dtls-01, June 2009. http://tools.ietf.org/id/draft-dekok-radext-dtls-01.txt.

[RADSEC] A. DeKok. *TLS encryption for RADIUS*. IETF ID draft-ietf-radext-radsec-06, February 2010. http://tools.ietf.org/id/draft-ietf-radext-radsec-06.txt.

[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.

[RFC 2865] C. Rigney et al. *Remote Authentication Dial In User Service (RADIUS)*. IETF RFC 2865, June 2000. http://www.ietf.org/rfc/rfc2865.txt.

[RFC 2866] C. Rigney et al. *RADIUS Accounting*. IETF RFC 2866, June 2000. http://www.ietf.org/rfc/rfc2866.txt.

[SAMLBind] S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os. See http://www.oasis-open.org/committees/security/.

[SAMLProf] S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See http://www.oasis-open.org/committees/security/.

1.3 Non-normative References

[Reference] [reference citation]

2 SAML AAA Binding

Authentication, Authorization and Accounting (AAA) protocols are widely used to support network access applications by enabling the exchange of AAA information, such as authentication credentials, between system entities.

Some AAA protocols use an extensible attribute framework, which has permitted the definition of an attribute that can be used to encapsulate SAML messages [REF]. The SAML AAA binding defines how to transport SAML messages within this attribute over AAA protocol transports.

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:bindings:AAA

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

Description: Given below.

Updates: None.

2.2 Overview

The SAML AAA Binding uses RADIUS formatted attributes to encapsulate SAML constructs (typically request and response protocol elements) within AAA messages. Like SAML, RADIUS attributes can be used over multiple underlying transports.

2.3 Protocol-Independent Aspects of the SAML AAA Binding

The following sections define aspects of the SAML AAA binding that are independent of the underlying AAA protocol on which the RADIUS attribute encapsulating the SAML constructs are transported.

2.3.1 Basic Operation

The system model used for SAML conversations over AAA is a simple request-response model, using the `SAML-Message` RADIUS attribute [REF] to encapsulate the SAML contructs.

1. The AAA client initiates an arbitrary AAA exchange with an AAA server. In the course of this exchange the AAA client, now acting as a SAML requester, MAY transmit one or more SAML constructs within a single AAA message (the “request message”) using as many instances of the `SAML-Message` RADIUS attribute as necessary. The `Message Type` field of these attributes MUST be set to TBD. The SAML requester MUST NOT attempt to send more than one request message for a given authentication event.

2. The AAA server, acting as a SAML responder, MAY return a SAML construct within a single AAA message (the “response message”) using as many instances of the `SAML-Message` RADIUS attribute as necessary. The `Message Type` field of these attributes MUST be set to TBD. The SAML responder MAY return an unsolicited response. The SAML responder MUST NOT attempt to send more than one response message for a given authentication event.

This binding is intended to be composed with typical AAA applications, such as network authentication and authorization. Therefore, other arbitrary AAA attributes may be used in the AAA messages.

2.4 Use of RADIUS

When using RADIUS, the request message MUST be the first RADIUS `Access-Request` packet issued by a RADIUS client for a given authentication event. The response message MUST be a RADIUS `Access-Accept` or `Access-Reject` packet issued by the RADIUS server that concludes the authentication event.

It is RECOMMENDED that the RADIUS exchange is protected using [RADSEC] or [RADDTLS] to maintain confidentiality and integrity.

2.4.1 Error Reporting

A SAML responder that refuses to perform a message exchange with the SAML requester SHOULD silently discard the SAML request.

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 by the respond RADIUS `Access-Accept` packet.

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 by the RADIUS `Access-Reject` packet using as many instances of the `Reply-Message` attribute as necessary.

2.5 Use of Metadata

TODO

2.6 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-binding-aaa-draft-00	18 Mar 2010	J.Howlett	Initial draft