SAML 2.0 Protocol Extension for Requested Authentication Context

Committee Specification 01

23 May 2007

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cs-01.html

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cs-01.odt

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cs-01.pdf

Previous Version:

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cd-03.html

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cd-03.odt

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac-cd-03.pdf

Latest Version:

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac.html

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac.odt

http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-protocol-ext-rac.pdf

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc

Prateek Mishra, Oracle

Editors:

Paul Madsen (paul.madsen@ntt-at.com), NTT

Ashish Patel (ashish.patel@rd.francetelecom.com), France Telecom

Abstract:

This specification defines a protocol extension to SAML 2.0 specification Error: Reference source not found that facilitates a more flexible model for expressing Authentication Context than that currently supported. The extension allows service providers to express combinations of Authentication Context classes in their requests for authentication assertions. The expectation is that the extension, when its additional functionality was necessary, would be used in replacement

of the existing Authentication Context mechanisms in the authentication request message. Readers should be familiar with Error: Reference source not found before reading this document.

Status

This document was last revised or approved by the OASIS Security Services Technical Committee 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.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security.

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 web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

1 Introduction

SAML protocol extensions consist of elements defined for inclusion in the `<samlp:Extensions>` element that modify the behavior of SAML requesters and responders when processing such extended messages.

This specification defines an extension to the SAML 2.0 protocol specification that can be optionally used to replace the existing mechanisms for Authentication Context #saml_ac in authentication requests. The extension provides a more flexible structure for expressing combinations of Authentication Context classes than do existing mechanisms.

1.1 Notation

This specification uses normative text.

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 Error: Reference source not found:

> …they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)…

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace SAMLCore.
`samlp:`	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace SAMLCore
`md:`	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace Error: Reference source not found. SAMLMeta
`rac:`	urn:oasis:names:tc:SAML:protocol:ext:rac	This is the SAML V2.0 protocol extension namespace, defined by this document and its accompanying schema RAC-XSD
`xsd:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification Schema1 . In schema listings, this is the default namespace and no prefix is shown.

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

2 SAML Protocol Extension for Requested Authentication Context

This specification defines an extension to the SAML 2.0 protocol specification that can be optionally used to replace the existing mechanisms within requests for Authentication Context SAMLAC with a more flexible structure for expressing combinations of Authentication Context classes.

Existing structures for indicating authentication context in authentication request messages are limited in their ability to express combinations of authentication contexts – the assumption is that the full context can be expressed through a single declaration, declaration reference, or a class reference. Consequently, were an SP or IDP to wish to express such a logical combination (or the SSTC to define classes to enable this), it would necessarily imply the creation of a new class URI to represent such a combination.

As a concrete example, certain telco use cases demand the ability for IDPs and SPs to distinguish between whether a principal is authenticated with a credential that is known to be shared amongst a group (e.g. a home phone or an internet kiosk) or unique to that principal. Because no existing SAML AC classes support this distinction (nor the schema as it stands), to allow an SP to make this distinction in its <AuthnRequest> implies that new AC classes would need to be defined to add the shared/unique distinction to each (relevant) existing AC class. For just this single initially onforseen aspect of authentication context, we face the possibility of a combinatorial explosion of AC class URIs. Should other such aspects emerge in the future, the problem would be exacerbated.

More scaleable would be to allow the SP to compose its Authentication Context requirements through the listing of multiple AC classes, and to allow the SP to control how those multiple classes are to be logically combined. Unfortunately, the existing <saml:RequestedAuthnContext> mechanism does not provide this flexibility.

This extension is intended to override existing mechanisms for requesting authentication contexts with a more flexible model – thereby meeting the immediate requirements of the above telco use cases, as well as providing a scaleable solution for dealing with similar currently unforeseen AC aspects should they arise.

Unless specifically noted, nothing in this document should be taken to conflict with the SAML 2.0 protocol specification SAMLCore. Readers are advised to familiarize themselves with that specification first.

2.1 Element <rac:RequestedACCombination>

The <rac:RequestedACCombination> element is used to carry the individual requested Authentication Contexts and to specify the logical operator defining how they should be combined.

The following schema fragment defines the <rac:RequestedACCombination> element:

```
<element name="RequestedACCombination" type="RequestedACCombinationType"/>

<complexType name="RequestedAuthnContextType">
   <choice>
        <element ref="RequestedACCombination" maxOccurs="unbounded"/>
        <element ref="saml:AuthnContextClassRef" maxOccurs="unbounded"/>
   </choice>
   <attribute name="RACComparison" type="anyURI" use="optional"/>
</complexType>
```

The <rac:RequestedACCombination> element can be nested to allow the SP to define combinations of Authentication Contexts. There SHOULD NOT be more than one level of such nesting.

2.1.1 RACComparison attribute

An SP uses the RACComparison attribute of the <rac:RequestedACCombination> element to specify the logical comparison or combination to be performed on the listed Authentication Context classes by the IDP in order to determine the appropriate combined context for any issued statement.

This specification defines the following value(s) for the RACComparison attribute. Other additional values MAY be defined.

URI: urn:oasis:names:tc:SAML:protocol:ext:rac:all

Indicates that the authentication context of any resultant statement MUST satisfy the requirements of all the listed <samlp:RequestedAuthenticationContext> elements. This is the default value.

URI: urn:oasis:names:tc:SAML:protocol:ext:rac:exact

Indicates that the authentication context of any resultant statement MUST be the exact match of one of the listed AC classes.

URI: urn:oasis:names:tc:SAML:protocol:ext:rac:minimum

Indicates that the authentication context of any resultant statement MUST be at least as strong (as deemed by the responder) as one of the authentication contexts specified

URI: urn:oasis:names:tc:SAML:protocol:ext:rac:maximum

Indicates that the authentication context of any resultant statement MUST be as strong as possible (as deemed by the responder) without exceeding the strength of at least one of the authentication contexts specified.

URI: urn:oasis:names:tc:SAML:protocol:ext:rac:better

Indicates that the authentication context of any resultant statement MUST be stronger (as deemed by the responder) than any one of the authentication contexts specified.

2.2 Example

The following is an example of a <rac:RequestedACCombination> element in which the SP is expressing that it desires the resultant <AuthnStatement> to have an Authentication Context that:

1. represents an authentication event characterized by a mechanism at least as strong as 'password' AND
2. represents an authentication event characterized by an authentication credential that is not shared by multiple users.
3.

```
<rac:RequestedACCombination RACComparison="all">
   <rac:RequestedACCombination RACComparison="minimum">
      <saml:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:classes:password
      </saml:AuthnContextClassRef>
   </rac:RequestedACCombination>
   <rac:RequestedACCombination RACComparison="exact">
      <saml:AuthnContextClassRef>
       urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:unique
      </saml:AuthnContextClassRef>
   </rac:RequestedACCombination>
</RequestedACCombination>
```

2.3 Processing Rules

This extension is included in a protocol request message by placing it in the optional `<samlp:Extensions>` element. Due to existing processing requirements, all extensions are explicitly deemed optional. Therefore, senders SHOULD only include this extension when they can be reasonably confident that the extension will be understood by the recipient.

This extension element MUST NOT be used in conjunction with any protocol message element whose complex type is not derived from the **samlp:RequestAbstractType** complex types.

A sender MUST NOT include more than one `<rac:RequestedACCombination>` element in a given request message unless additional elements occur as nested children of the top-most extension,

The `<rac:RequestedACCombination>` extension element MUST NOT be used in a message in which there exists a <`samlp:RequestedAuthnContext`> element.

A sender MAY specify the logical combination it desires by providing the appropriate URI in the RAC`Comparison` attribute. If not specified, it is logically equivalent to the RACComparision attribute being present with a value of `urn:oasis:names:tc:SAML:protocol:ext:rac:all.`

If a <AuthnRequest> message's <samlp:Extensions> element contains a <rac:RequestedACCombination> element, then a responder that understands the extension MUST fulfill the request (if it does so at all) by issuing a <Response> containing an assertion with at least one <AuthnStatement> element containing an <AuthnContext> element that satisfies the specified Authentication Context in the <rac:RequestedACCombination> extension.

If the responder is unable to satisfy the specified Authentication Context then the responder MUST return a <Response> message with a second-level <StatusCode> of urn:oasis:names:tc:SAML:2.0:protocol:NoAuthnContext.

2.4 Metadata Considerations

SAML metadata MAY be used to indicate support for this protocol extension at particular protocol endpoints, using the extension capabilities of the metadata schema.

Support for this extension is expressed in SAML 2.0 metadata by adding a boolean-typed XML attribute to an element of or derived from the **md:EndpointType** complex type, indicating that SAML request messages sent to that endpoint MAY include this extension.

The following schema fragment defines the rac:`supportsRequestedACComb` attribute:

```
<attribute name="supportsRequestedACComb" type="boolean"/>
```

2.4.1 Metadata Example

The example below shows a fragmentary `<md:SingleSignOnService>` element that advertises support for the <rac:`RequestedACCombination>` extension. The namespace declaration must be in scope, but the prefix is of course arbitrary.

```
<md:SingleSignOnService
  xmlns:rac="urn:oasis:names:tc:SAML:protocol:ext:rac"
  rac:supportsRequestedACComb="1" .../>
```

3 References

The following works are referenced in the body of this specification.

3.1 Normative References

[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.

[SAMLAuthnCxt] J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-context-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

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

[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://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.

[SAMLMeta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[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://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/.

[rac-xsd] P. Madsen & A. Patel. SAML Requested Authentication Context protocol extension schema. OASIS SSTC, September 2006. Document ID sstc-saml-protocol-ext-rac.xsd. See http://www.oasis-open.org/committees/security/.

Appendix A. Acknowledgements

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- Hal Lockhart, BEA Systems, Inc.
- Steve Anderson, BMC Software
- Thomas Wisniewski, Entrust
- Ashish Patel, France Telecom
- Greg Whitehead, Hewlett-Packard
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, Neustar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- John Hughes, PA Consulting
- Brian Campbell, Ping Identity Corporation
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba Corp.
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veterans Health Administration

Appendix B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.