SAML Protocol Extension for Authentication Context Combinations

Working Draft 02, 18 May 2006

Document identifier:

draft-sstc-saml-protocol-ext-rac-02

Location:


Editors:

Paul Madsen (paul.madsen@ntt-at.com), NTT
Ashish Patel (paul.madsen@ntt-at.com), France Telecom

Contributors:

Abstract:

This specification defines a protocol extension to SAML 2.0 specification [SAML2Core] 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 [SAML2Core] before reading this document.

Status

This is a working draft and the text may change before completion.

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.
## Table of Contents

1 Introduction........................................................................................................................................... 3  
  1.1 Notation........................................................................................................................................... 3  
2 Requested Authentication Context Combinations Protocol Extension.................................................... 4  
  2.1 Element <rac:RequestedAuthnContexts>......................................................................................... 4  
    2.1.1 RACComparison attribute........................................................................................................ 5  
  2.2 Example........................................................................................................................................... 5  
  2.3 Processing Rules............................................................................................................................... 6  
  2.4 Metadata Considerations.................................................................................................................. 6  
    2.4.1 Metadata Example...................................................................................................................... 6  
3 References............................................................................................................................................ 7  
  3.1 Normative References.......................................................................................................................... 7
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 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 [RFC 2119]:

...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:

- The prefix saml: stands for the SAML 2.0 assertion namespace, urn:oasis:names:tc:SAML:2.0:assertion
- The prefix samlp: stands for the SAML 2.0 protocol namespace, urn:oasis:names:tc:SAML:2.0:protocol
- The prefix md: stands for the SAML 2.0 metadata namespace, urn:oasis:names:tc:SAML:2.0:metadata
- The prefix rac: stands for the SAML 2.0 protocol extension namespace developed herein, urn:oasis:names:tc:SAML:protocol:ext:rac
  In schema listings, this is the default namespace and no prefix is shown.
- The prefix xsi: stands for the W3C XML Schema namespace for schema-related markup that appears in XML instances: http://www.w3.org/2001/XMLSchema-instance

This specification uses the following typographical conventions in text: <SAMLElement>, <ns:ForeignElement>, Attribute, Datatype, OtherCode.
2 Requested Authentication Context Combinations
Protocol Extension

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 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 unforeseen 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 exascerbated.

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 [SAML2Core]. Readers are advised to familiarize themselves with that specification first.

2.1 Element <rac:RequestedAuthnContexts>

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

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

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

The <rac:RequestedAuthnContexts> element can be nested to allow the SP to define arbitrarily
complex combinations of Authentication Contexts.
2.1.1 RACComparison attribute

An SP uses the RACComparison attribute of the <rac:RequestedAuthnContexts> 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.


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.


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


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.


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.


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:RequestedAuthnContexts> 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.

```xml
<rac:RequestedAuthnContexts RACComparison="all">
    <rac:RequestedAuthnContexts RACComparison="minimum">
        <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:password
        </saml:AuthnContextClassRef>
    </rac:RequestedAuthnContexts>
    <rac:RequestedAuthnContexts RACComparison="exact">
        <saml:AuthnContextClassRef>
        </saml:AuthnContextClassRef>
    </rac:RequestedAuthnContexts>
</rac:RequestedAuthnContexts>
```
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:RequestedAuthnContexts> extension element in
a given request message.

The <rac:RequestedAuthnContexts> extension element MUST NOT be used in conjunction with a
<samlp:RequestedAuthnContext> element.

A sender MAY specify the logical combination it desires by providing the appropriate URI in the
RACComparison attribute. If not specified, it is logically equivalent to the RACComparison attribute

If a <AuthnRequest> message’s <samlp:Extensions> element contains a
<rac:RequestedAuthnContexts> 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:RequestedAuthnContexts>.

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

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:supportsRequestedAC attribute:

```xml
<attribute name="supportsRequestedAC" type="boolean"/>
```

2.4.1 Metadata Example

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

```xml
<md:SingleSignOnService
rac:supportsRequestedAC="true" .../>
```
3 References

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

3.1 Normative References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>