SAML v2.0 Protocol Extension for Requesting Attributes per Request Version 1.0

Working Draft 03

9 December 2016

Technical Committee:
OASIS Security Services (SAML) TC

Chairs:
Thomas Hardjono (hardjono@mit.edu), MIT
Nate Klingenstein (ndk@internet2.edu), Internet2

Editors:
Madalina Sultan (madalina.sultan@connectis.nl), Connectis
Mert Aybat (mert.aybat@connectis.nl), Connectis
Robert van Herk (robert.van.herk@connectis.nl), Connectis
Martijn Kaag (martijn.kaag@connectis.nl), Connectis

Additional artifacts:
This prose specification is one component of a Work Product that also includes:
- XSD schema: sstc-req-attr-ext.xsd

Related work:
This specification is related to:
- Security Assertion Markup Language (SAML) v2.0. OASIS Standard.

Abstract:
This specification defines an extension to SAML 2.0 protocol specification SAMLCore. The extension allows Service Providers to specify ad-hoc sets of attributes per request. This brings more flexibility than existing mechanisms, which are based on signaling pre-defined sets of requested attributes.

Status:
This Working Draft (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or approved as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document Approval Process begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

Any machine-readable content (aka Computer Language Definitions) declared Normative for this Work Product must also be provided in separate plain text files. In the event of a discrepancy between such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

URI patterns:
Initial publication URI:
http://docs.oasis-open.org/security/saml-protoc-req-atrr-req/v1.0/csd01/saml-protoc-req-atrr-req-v1.0-csd01.odt

Permanent "Latest version" URI:
http://docs.oasis-open.org/security/saml-protoc-req-atrr-req/v1.0/saml-protoc-req-atrr-req-v1.0.odt
(Managed by OASIS TC Administration; please don’t modify.)
1 Introduction

1.1 Terminology
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 [RFC2119].

1.2 Normative References

1.3 Non-Normative References
2 SAML V2.0 Protocol Extension For Requesting Attributes Per Request

This specification defines an extension to the SAML 2.0 protocol specification [SAML2Core], specifically to the Authentication Request protocol. The extension allows Service Providers to specify ad-hoc sets of attributes per-request.

The existing mechanism for specifying requested attributes is based on signaling predefined sets of attributes via SAML metadata in conjunction with the AttributeConsumingServiceIndex attribute. This approach has two limitations. First, all possible combinations of attributes must be known and exchanged beforehand. Second, the number of possible combination of attributes is limited because AttributeConsumingServiceIndex is of type short. In federations with many different attributes and where data minimization is required, the number of possible combinations easily exceeds the maximum number of 32767. Enumerating that number of combinations is impractical in any event.

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 <req-attr:RequestedAttributes>

The element <req-attr:RequestedAttributes>, of complex type req-attr:RequestedAttributesType, contains a list of one or more <md:RequestedAttribute> elements. In this way, the Service Provider specifies its desire that the resultant assertion contains a list of AttributeStatements expressing the values of the queried attribute.

The following schema fragment defines the <req-attr:RequestedAttribute> element:

```xml
<element name="RequestedAttributes" type="req-attr:RequestedAttributesType"/>
<complexType name="RequestedAttributeType">
  <sequence>
    <element ref="md:RequestedAttribute" minOccurs="1" maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

2.2 Example

The following is an example of a <samlp:Extensions> element (in an <samlp:AuthnRequest>, not shown) where the SP is expressing that it desires the resultant assertions to contain a <saml:AttributeStatement> that contains the LDAP-derived sn and givenName attributes, optionally includes mail, and includes a custom role attribute where its values match 'User' or 'Administrator'.

```xml
<samlp:Extensions>
  <req-attr:RequestedAttributes>
    <md:RequestedAttribute isRequired="true" Name="urn:oid:2.5.4.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
    <md:RequestedAttribute isRequired="true" Name="urn:oid:2.5.4.42" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
    <md:RequestedAttribute Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  </req-attr:RequestedAttributes>
</samlp:Extensions>
```
2.3 Processing Rules

A <req-attr:RequestedAttributes> element is included in a <samlp:AuthnRequest> message by placing it in the optional <samlp:Extensions> element. 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. The metadata extension defined in section 2.4 MAY be used for this purpose.

Each <md:RequestedAttribute> describes a SAML attribute the requester desires or requires to be supplied by the identity provider in the response. The identity provider MAY use this information to populate one or more <saml:AttributeStatement> elements in the assertion(s) it returns.

The isRequired attribute, expressing that an attribute is mandatory, remains advisory. The Identity Provider MAY choose to ignore this flag and omit these attributes in the response, if it cannot or will not provide them.

If a Service Provider includes the <req-attr:RequestedAttributes> extension, then it MUST NOT include an AttributeConsumingServiceIndex attribute in the same message. In the event that both are present, an Identity Provider SHOULD ignore the extension and process the request based on the AttributeConsumingServiceIndex attribute.

2.4 Metadata Considerations

SAML V2.0 metadata [SAML2Meta] MAY be used to indicate support for this protocol extension at particular protocol endpoints, using the extensions capabilities of the metadata schema.

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

The following schema fragment defines the req-attr:supportsRequestedAttributes attribute:

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

2.4.1 Metadata Example

The example below shows a fragment of an <md:SingleSignOnService> element that advertises support for this extension. The namespace declaration must be in scope, but the prefix is arbitrary.
2.4.2 Metadata Processing Rules

If the Identity Provider's metadata contains the `req-attr:supportsRequestedAttributes` attribute set to "true", then the Service Provider MAY send the `<req-attr:RequestedAttributes>` element in its messages to the corresponding endpoint(s).

If the Identity Provider metadata contains both the `req-attr:supportsRequestedAttributes` attribute (set to "true") and also contains one or more `<md:AttributeConsumingService>` elements with sets of associated attributes, then the Service Provider SHOULD use the `AttributeConsumingServiceIndex` attribute if it can find a predefined set of attributes matching its needs.

2.5 Security Considerations

The Identity Provider is always free to ignore this extension and populate its response with more or fewer attributes than requested, as well as ignore the `isRequired` attribute. A Service Provider must therefore always inspect the response and cannot assume the contents will match its requirements.
3 Conformance

3.1 Conformance as a Service Provider

A Service Provider implementation conforms to this specification if it supports the extension defined in section 2.1 and the processing rules defined in section 2.3.

3.2 Conformance as an Identity Provider

An Identity Provider implementation conforms to this specification if it supports the extension defined in section 2.1 and the processing rules defined in section 2.3.
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]

Appendix B  Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Editor</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01-09-2015</td>
<td>Mert Aybat</td>
<td>First Draft</td>
</tr>
<tr>
<td>2</td>
<td>19-01-2016</td>
<td>Mert Aybat</td>
<td>Adding in xsd and wrapping RequestedAttribute elements with RequestedAttributes element.</td>
</tr>
<tr>
<td>3</td>
<td>13-10-216</td>
<td>Madalina Sultan</td>
<td>Defined a new namespace for RequestedAttribute Added supportsRequestedAttributes metadata flag</td>
</tr>
<tr>
<td>4</td>
<td>21-10-2016</td>
<td>Madalina Sultan</td>
<td>Added the req:RequestedAttributes element, as a wrapper for a list of md:RequestedAttribute elementss</td>
</tr>
<tr>
<td>5</td>
<td>21-11-2016</td>
<td>Madalina Sultan</td>
<td>Cosmetic changes</td>
</tr>
<tr>
<td>6</td>
<td>02-12-2016</td>
<td>Madalina Sultan</td>
<td>Added Conformance section and other changes based on feedback received during SSTC meeting</td>
</tr>
<tr>
<td>7</td>
<td>09-12-2016</td>
<td>Scott Cantor</td>
<td>Editorial pass for formatting, references, and some language cleanup.</td>
</tr>
</tbody>
</table>
Appendix C  sstc-req-attr-ext.xsd

<?xml version="1.0" encoding="UTF-8"?>

    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified" attributeFormDefault="unqualified" blockDefault="substitution"
    version="1.0">
    <import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
        schemaLocation="saml-schema-metadata-2.0.xsd"/>

    <annotation>
        <documentation>
            Document title: SAML V2.0 Protocol Extension For Requesting Attributes Per Request
            Document identifier: sstc-req-attr-ext
            Location: http://docs.oasis-open.org/security/saml/Post2.0/
            Revision history: V4.0 (October 2016): Document with integrated feedback
        </documentation>
    </annotation>

    <element name="RequestedAttributes" type="req-attr:RequestedAttributesType"/>

    <complexType name="RequestedAttributesType">
        <sequence>
            <element ref="md:RequestedAttribute" minOccurs="1" maxOccurs="unbounded"/>
        </sequence>
    </complexType>

    <attribute name="supportsRequestedAttributes" type="boolean"/>
</schema>