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

Committee Specification Draft 01 / Public Review Draft 01

09 May 2017

Specification URIs

This version:

http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/csprd01/saml-protoc-req-attr-req-v1.0-csprd01.odt (Authoritative)
http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/csprd01/saml-protoc-req-attr-req-v1.0-csprd01.html
http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/csprd01/saml-protoc-req-attr-req-v1.0-csprd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/saml-protoc-req-attr-req-v1.0.odt (Authoritative)
http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/saml-protoc-req-attr-req-v1.0.html
http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/saml-protoc-req-attr-req-v1.0.pdf

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:

- XML schema: http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/csprd01/schema/sstc-req-attr-ext.xsd

Related work:

This specification is related to:

- *Security Assertion Markup Language (SAML) v2.0*, comprised of the following documents:
  - *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

- *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
- *Conformance Requirements for the OASIS Security Assertion Mark Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
- *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
- *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
- *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- *Security Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*: http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
- *SAML Version 2.0 Errata 05*. 01 May 2012. OASIS Approved Errata. http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html.

Abstract:

This specification defines an extension to the SAML 2.0 protocol specification [SAML2Core]. 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 document was last revised or approved by the OASIS Security Services (SAML) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the Technical Committee’s web page at https://www.oasis-open.org/committees/security/.

This Committee Specification Public Review Draft is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this Work Product, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/security/ipr.php).

Note that any machine-readable content (aka Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any 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.

Citation format:

When referencing this Work Product the following citation format should be used:

[SAML-ReqAttrExt-v1.0]

SAML v2.0 Protocol Extension for Requesting Attributes per Request Version 1.0. Edited by Madalina Sultan, Mert Aybat, Robert van Herk, and Martijn Kaag. 09 May 2017. OASIS Committee Specification Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/csprd01/saml-protoc-req-attr-req-v1.0-csprd01.html. Latest version: http://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/saml-protoc-req-attr-req-v1.0.html.

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 name "OASIS" is a trademark 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 https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction 6
1.1 IPR Policy 6
1.2 Terminology 6
1.3 Normative References 6
1.4 Non-Normative References 6
2 SAML V2.0 Protocol Extension For Requesting Attributes Per Request 7
2.1 Element <req-attr:RequestedAttributes> 7
2.2 Example 7
2.3 Processing Rules 8
2.4 Metadata Considerations 8
2.4.1 Metadata Example 8
2.4.2 Metadata Processing Rules 8
2.5 Security Considerations 8
3 Conformance 10
3.1 Conformance as a Service Provider 10
3.2 Conformance as an Identity Provider 10
Appendix A Acknowledgments 11
Appendix B Revision History 12
Appendix C sstc-req-attr-ext.xsd 13

1 Introduction

1.1 IPR Policy

This Committee Specification Draft is being developed under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established.

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 TC's web page (https://www.oasis-open.org/committees/security/ipr.php).

1.2 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].

1.3 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[SAML2Core] 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.

[SAML2Meta] S. Cantor et al. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. Document ID saml-metadata-2.0-os. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

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

1.4 Non-Normative References

[ReqAttrExt-xsd] See schema file linked from Additional artifacts.

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:

```
<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'.

```
<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" />
    <md:RequestedAttribute Name="https://example.org/attributes/role"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue>User</saml:AttributeValue>
      <saml:AttributeValue>Administrator</saml:AttributeValue>
    </md:RequestedAttribute>
</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:suppportsRequestedAttributes attribute:

```
<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.

```
<md:SingleSignOnService xmlns:req-attr="urn:oasis:names:tc:SAML:protcol:ext:req-attr"
       req-attr:supportsRequestedAttributes="true"  .../>
```

2.4.2 Metadata Processing Rules

If the Identity Provider's metadata contains the req-attr:suppportsRequestedAttributes 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:suppportsRequestedAttributes 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:

Mert Aybat – Connectis
Scott Cantor -- Internet2
Thomas Hardjono – MIT
Robert van Herk – Connectis
Mohammad Jafari -- Veterans Health Administration
Martijn Kaag – Connectis
Hal Lockhart -- Oracle
Madalina Sultan -- Connectis

Appendix B Revision History

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

Appendix C sstc-req-attr-ext.xsd

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

<schema xmlns:req-attr="urn:oasis:names:tc:SAML:protocol:ext:req-attr"
        targetNamespace="urn:oasis:names:tc:SAML:protocol:ext:req-attr"
        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>
```

