SAML v2.0 Protocol Extension for Requesting Attributes in AuthnRequest Version 1.1

Working Draft 02

19 January 2016

Technical Committee:
OASIS Security Services (SAML) TC

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

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

Additional artifacts:
This prose specification is one component of a Work Product that also includes:
• XML schemas (list file names or directory name)
• Other parts (list titles and/or file names)

Related work:
This specification is related to:
• Security Assertion Markup Language (SAML) v2.0. OASIS Standard.
  http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

Abstract:
This specification defines an extension to SAML 2.0 protocol specification SAMLCore. The extension provides a more flexible structure for expressing which combination of Attributes are requested by service providers in comparison to the existing mechanisms. This is achieved by allowing md:RequestedAttribute elements in samlp:AuthnRequest, which is an alternative to specifying these elements in SAML metadata. The extension thereby allows service providers to specify attributes per request. The expectation is that the extension is used to limit the set of Attributes returned to the service provider, thereby supporting (new) privacy regulations that require data minimization.
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.

URI patterns:
Initial publication URI:
http://docs.oasis-open.org/security/saml-attributequery-authn/v1.0/csd01/saml-attributequery-authn-v1.0-csd01.odt
Permanent “Latest version” URI:
http://docs.oasis-open.org/security/saml-attributequery-authn/v1.0/saml-attributequery-authn-v1.0.odt
(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2015. All Rights Reserved.
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.
Table of Contents

Introduction
   Notation
SAML Protocol Extension For Requesting Attributes Per Request
   Example
   Processing Rules
   Security Considerations
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 used to request specific Attributes to be returned to the service provider for Web Single Sign On. The extension allows service providers to express per request which specific Attributes may be returned in the response, which attributes are required and what values the service provider is interested in.

Notation

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:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:</td>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>This is the SAML V2.0 assertion namespace <a href="#">SAMLCore</a>.</td>
</tr>
<tr>
<td>samlp:</td>
<td>urn:oasis:names:tc:SAML:2.0:protocol</td>
<td>This is the SAML V2.0 protocol namespace <a href="#">SAMLCore</a>.</td>
</tr>
<tr>
<td>md:</td>
<td>urn:oasis:names:tc:SAML:2.0:metadata</td>
<td>This is the SAML V2.0 metadata namespace. <a href="#">SAMLMeta</a>.</td>
</tr>
<tr>
<td>xsd:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This namespace is defined in the W3C XML Schema specification <a href="#">Schema1</a>. In schema listings, this is the default namespace and no prefix is shown.</td>
</tr>
</tbody>
</table>
SAML Protocol Extension For Requesting Attributes Per Request

This specification defines an extension to SAML 2.0 protocol specification SAMLCore that provides a more flexible structure for expressing combinations of Attributes for Web Single Sign On than do existing mechanisms.

Existing mechanisms for indicating the requested attributes depend on md:RequestedAttribute elements in metadata and samlp:AttributeConsumingServiceIndex in the samlp:AuthnRequest. This approach has two limitations. First, all possible combinations of attributes should be known and exchanged beforehand. Second, the number of possible combination of attributes is limited because of 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.

This specification provides service providers a more flexible way of requesting Attributes by allowing them to specify the md:RequestedAttribute elements in the samlp:AuthnRequest instead of specifying them in their metadata. The extension thereby allows service providers to specify attributes per request.

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.

Example
The following is an example of a <samlp:Extensions> element in <samlp:AuthnRequest> where the SP is expressing that it desires the resultant assertions to contain an <AttributeStatement> that contains the LastName and FirstName, optionally includes the Email and includes the Roles of the user that match ‘End User’ or ‘Administrator’.

<samlp:Extensions>
  <md:RequestedAttributes>
    <md:RequestedAttribute isRequired="true" Name="LastName"/>
    <md:RequestedAttribute isRequired="true" Name="FirstName"/>
    <md:RequestedAttribute Name="Email"/>
    <md:RequestedAttribute Name="Role">
      <saml:AttributeValue>End User</saml:AttributeValue>
      <saml:AttributeValue>Administrator</saml:AttributeValue>
    </md:RequestedAttribute>
  </md:RequestedAttributes>
</samlp:Extensions>

Processing Rules
A list of RequestedAttribute is included in an AuthnRequest message by placing it in the optional <samlp:Extensions> element. RequestedAttribute elements are wrapped by a RequestedAttributes 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.
Each *RequestedAttribute* describes a SAML attribute the requester desires or requires to be supplied by the identity provider in the `<Response>` message. The identity provider MAY use this information to populate one or more `<saml:AttributeStatement>` elements in the assertion(s) it returns. The following schema fragment defines the *RequestedAttribute* complex type

```xml
<xs:complexType name="RequestedAttributeType">
  <xs:sequence>
    <xs:element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Name" type="xs:string" use="required"/>
  <xs:attribute name="isRequired" type="xs:boolean" use="optional"/>
</xs:complexType>
```

**Security Considerations**

The identity provider MAY choose to ignore this extension and populate the response with more or less attributes than provided. The identity provider MAY also ignore the isRequired attribute and continue processing if a user does not possess a specific attribute. The service provider should therefore always inspect the returned attributes and should not rely on the identity provider for authorization.
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]
## 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>
</tbody>
</table>