Table of Contents

1. Introduction
   1.1 Notation

2. SAML V2.0 Protocol Extension For Requesting Attributes Per Request
   2.1 Required Information
   2.2 Profile Overview
   2.3 Element <req-attr:RequestedAttributes>
   2.4 Example
   2.5 Processing Rules
   2.6 Metadata Considerations
      2.6.1 Metadata Example
      2.6.2 Metadata Processing Rules
   2.7 Security Considerations

3. Conformance
   3.1 SAML V2.0 Protocol Extension for RequestedAttributes per Request

4. References
   4.1 Normative References

Appendix A. Acknowledgments

Appendix B. Revision History

Appendix C. sstc-req-attr-ext.xsd
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 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.

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.

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:

<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</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</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</td>
</tr>
<tr>
<td>req-attr:</td>
<td>urn:oasis:names:tc:SAML:protocol:ext:req-attr</td>
<td>This is the namespace defined by this document and its accompanying schema [ReqAttrExt-xsd]</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 [Schema1]. In schema listings, this is the default namespace and no prefix is shown.</td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text:
2. SAML V2.0 Protocol Extension For Requesting Attributes Per Request

2.1 Required Information

Contact Information: security-services-comment@lists.oasis-open.org
Description: Given below
Updates: None

2.2 Profile Overview

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. It only takes a set of 15 distinct attributes, and the sum of all their possible combinations is 2^15= 32768.

This specification provides service providers a more flexible way of requesting Attributes by allowing them to specify a req-atr:RequestedAttributes element, wrapping a list of md:RequestedAttribute inside the extensions part of a 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.

2.3 Element <req-atr:RequestedAttributes>

The element <req-atr:RequestedAttributes>, with complex type req-atr:RequestedAttributesType, wraps a list of 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-atr:RequestedAttribute> element:

```xml
<element name="RequestedAttributes" type="req-atr:RequestedAttributesType"/>
<complexType name="RequestedAttributesType">
  <sequence>
    <element ref="md:RequestedAttribute" minOccurs="1" maxOccurs="unbounded"/>
  </sequence>
</complexType>
```
2.4 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 a `<saml: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>
  <req-attr: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>
  </req-attr:RequestedAttributes>
</samlp:Extensions>
```

2.5 Processing Rules

A `RequestedAttributes` element is included in an `AuthnRequest` 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. The SAML V2.0 metadata extension defined in section 2.6 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` message. The identity provider MAY use this information to populate one or more `<saml:AttributeStatement>` elements in the assertion(s) it returns.

The `<md:RequestedAttribute>` elements marked as required are just informational, expressing that they are mandatory for the ServiceProvider. The Identity Provider MAY choose to ignore this flag and do not include these attributes in the response, if it cannot provide them.

If a Service Provider sends out an `AuthenticationRequest` containing both a `<saml:AttributeConsumingServiceIndex>` and a `<req-attr:RequestedAttributes>` section inside extensions, then the Identity Provider receiving this message SHOULD send back the list of attributes associated to the AttributeConsumingService index. In order to keep backwards compatibility, the extension proposed by this document should be processed by Identity Providers only if there is no AttributeConsumingServiceIndex in the message pointing to a different set of attributes.

2.6 Metadata Considerations

SAML Metadata MAY be used to indicate support for this protocol extension at particular protocol endpoints, using the extensions capabilities of metadata schema.
Support for this extension is expressed in SAMLV2.0 metadata [Saml2Meta] 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:

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

### 2.6.1 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.

```
   req-attr:supportsRequestedAttributes="true".../>
```

### 2.6.2 Metadata Processing Rules

If the Identity Provider metadata uses the `req-attr:supportsRequestedAttributes` flag, then the Service Provider MAY send the `<req-attr:RequestedAttributes>` element inside its AuthnRequest extensions.

If the Identity Provider metadata declares both the `req-attr:supportsRequestedAttributes` flag (set on true) and it also defines AttributeConsumingService indices with sets of associated attributes, the Service Provider SHOULD use the AttributeConsumingServiceIndex element if it cannot find a predefined set of attributes matching his needs, and do not use the `<req-attr:RequestedAttributes>` extension.

If there is no predefined set of attributes defined in the metadata of the IdentityProvider matching the ServiceProvider needs, then the Service Provider MAY choose to request the attributes through the `<req-attr:RequestedAttributes>` extension. But in this case, an AttributeConsumingServiceIndex SHOULD NOT be included in the request.

### 2.7 Security Considerations

The identity provider MAY choose to ignore these attributes and populate the response with more or fewer attributes than provided. The identity provider MAY also ignore the `isRequired` attribute and continue processing if a user does not posses a specific attribute.

The service provider should therefore always inspect the returned attributes and should not rely on the identity provider for authorization.
3. Conformance

3.1 SAML V2.0 Protocol Extension for RequestedAttributes per Request

A Service Provider is conformant to this profile if it has the ability to include the
<req-attr:RequestedAttributes> element inside the <samlp:Extensions> of a <samlp:AuthnRequest>.

An Identity Provider is conformant to this profile if it declares the req-attr:supportsRequestedAttributes flag
in its exposed metadata and if it has the ability of processing successfully a request containing requested
attributes. Successful processing MAY consist of no changes to a relying party’s behavior.
4. References
The following works are referenced in the body of this specification.

4.1 Normative References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ReqAttrExt-xsd]</td>
<td>OASIS Committee Draft 01, SAML Protocol Extension For Requesting Attributes Per Request, October 2016.</td>
<td><a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-req-attr-ext.xsd">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-req-attr-ext.xsd</a></td>
</tr>
</tbody>
</table>
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 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 and 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 elements.</td>
</tr>
<tr>
<td>5</td>
<td>21-11-2016</td>
<td>Madalina Sultan</td>
<td>Cosmetic changes</td>
</tr>
</tbody>
</table>
Appendix C. sstc-req-attr-ext.xsd

When submitting the proposal to Oasis SAML TC, the following XSD should be attached and uploaded to http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-req-attr-ext.xsd

```xml
<?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"/>

  <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>

  <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>
```