SAML Protocol Extension for Requesting Attributes per Request

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:RequestedAttribut*e elements in *samlp:AuthnReque*st, 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.

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:

Prefix	**XML Namespace**	**Comments**
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace SAMLCore.
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace SAMLCore

md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace. SAMLMeta
xsd:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification Schema1 . In schema listings, this is the default namespace and no prefix is shown.

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: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:RequestedAttribute Name="Email" />
</samlp:Extensions>
```

Processing Rules

A list of *RequestedAttribute* 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.

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.

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.