Principal Selection in SAML Authentication Requests

Version 1.0 - 2019-11-01 - *Draft version*

ELN-0614-v1.0

Table of Contents

1. Introduction

When a Service Provider requests authentication of a user (principal), the Service Provider may have prior knowledge about the user to be authenticated, for example, when re-authenticating an already authenticated user, or when a user authenticates to a signature service where the user signs a document in a context where he or she already has been authenticated.

This specification defines the `<psc:PrincipalSelection>` element that may be included in the `<saml2p:Extensions>` element of a SAML `<saml2p:AuthnRequest>` where the requesting Service Provider can specify matching criteria that may be used by the Identity Provider to select the particular user that should be authenticated.

The specification also defines the `<psc:RequestedPrincipalSelection>` element that should be used by Identity Providers that may need information about a known user in order to avoid prompting for the user ID[1]. The element should be included as an extension in the Identity Provider metadata under the `<md:IDPSSODescriptor>` element.

Even though the main purpose of the `<psc:PrincipalSelection>` extension is to aid the Identity Provider in selecting a particular subject for the authentication, an Identity Provider MAY also compare the match values present in the extension with the resulting attributes from the user authentication, and in case of a mismatch, respond with an error. In these cases the second-level SAML status code MUST be set to `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal` [SAML2Core].

> [1]: The typical use case is when a user once has authenticated for a service and provided his or hers user ID to the Identity Provider, and is about to perform a signature. If the Identity Provider prompts the user for the user ID once again the user experience is poor and the Service Provider will receive customer complaints.

1.1. Requirements Notation

The key words **MUST**, **MUST NOT**, **REQUIRED**, **SHALL**, **SHALL NOT**, **SHOULD**, **SHOULD NOT**, **RECOMMENDED**, **MAY**, and **OPTIONAL** are to be interpreted as described in [RFC2119].

These keywords are capitalized when used to unambiguously specify requirements over protocol features and behaviour that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.2. XML Namespace References

The prefix **psc:** stands for the Principal Selection Criteria XML schema namespace `http://id.swedenconnect.se/authn/1.0/principal-selection/ns`.

The prefix **saml2:** stands for the OASIS SAML 2 Assertion schema namespace `urn:oasis:names:tc:SAML:2.0:assertion`.

The prefix **saml2p:** stands for the OASIS SAML 2 Protocol schema namespace `urn:oasis:names:tc:SAML:2.0:protocol`.

The prefix **md:** stands for the OASIS SAML 2 Metadata schema namespace `urn:oasis:names:tc:SAML:2.0:metadata`.

1.3. Structure

This specification uses the following typographical conventions in text: `<LocalElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

2. Data elements

This specification defines the element `<PrincipalSelection>` to be included in the `<Extensions>` element of an `AuthnRequest`.

This element MAY be used by an Identity Provider to select the subject to authenticate.

2.1. PrincipalSelection

The Principal Selection Criteria is provided in a `<PrincipalSelection>` element. The element has the following elements and attributes:

`<MatchValue>` [One or more]

> This element holds values that MAY be used by the Identity Provider to match against a principal to be authenticated.

The following schema fragment defines the `<PrincipalSelection>` element:

```
<xs:element name="PrincipalSelection" type="psc:PrincipalSelectionType"/>
<xs:complexType name="PrincipalSelectionType">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" name="MatchValue" type="psc:MatchValueType" minOccurs="1"/>
  </xs:sequence>
</xs:complexType>
```

2.1.1 MatchValue

The `<MatchValue>` element contains a string value to be matched against the selected principal. This element has the following attributes which determines the meaning of the match value:

`Name` [Required]

> The identifying name of the type of identifier value expressed in the `MatchValue` element. This is analogous to the `Name` attribute of a SAML `<saml2:Attribute>` element.

`NameFormat` [Default `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`]

> Attribute specifying the format of the `Name` attribute value. This attribute is analogous to the `NameFormat` attribute of a SAML `<saml2:Attribute>` element.

`##any` [Optional]

> Extension point for any attribute in accordance with local conventions and future specifications.

The following schema fragment defines the `<MatchValueType>` complex type:

```
<xs:complexType name="MatchValueType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="NameFormat" type="xs:anyURI"
          default="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <xs:attribute name="Name" type="xs:string" use="required"/>
```

```
      <xs:anyAttribute namespace="##any"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

2.2. RequestedPrincipalSelection

An Identity Provider uses the `<RequestedPrincipalSelection>` element to declare that it wishes to receive the `<PrincipalSelection>` extension element in authentication requests. The contained `MatchValue` elements should contain no values, only the attribute name of a `MatchValue` element is relevant to declare which attributes of a known user that is interest for the Identity Provider.

The following schema fragment defines the `<RequestedPrincipalSelection>` element:

```
<xs:element name="RequestedPrincipalSelection" type="psc:RequestedPrincipalSelectionType" />
<xs:complexType name="RequestedPrincipalSelectionType">
  <xs:complexContent>
    <xs:extension base="psc:PrincipalSelectionType" />
  </xs:complexContent>
</xs:complexType>
```

3. Examples

Attributes in the examples below are specified in [EidAttributes].

3.1. Authentication Requests

```
...
<saml2p:Extensions>
  <psc:PrincipalSelection xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">
    <psc:MatchValue Name="urn:oid:1.2.752.29.4.13">197309069289</psc:MatchValue>
  </psc:PrincipalSelection>
</saml2p:Extensions>
...
```

Example of a `PrincipalSelection` specifying a Swedish personal identity number (personnummer) as match attribute.

```
...
<saml2p:Extensions>
  <psc:PrincipalSelection xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">
    <psc:MatchValue Name="urn:oid:1.2.752.29.4.13">198906059483</psc:MatchValue>
    <psc:MatchValue Name="urn:oid:1.2.752.201.3.4">NO:05068907693</psc:MatchValue>
  </psc:PrincipalSelection>
<saml2p:Extensions>
...
```

Example of a `PrincipalSelection` specifying two alternative matching policies. The first policy specifies a Swedish personal identity number (personnummer) and the second specifies a ProvisionalID attribute.

3.2. Metadata Extension

```
...
<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
    <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
      ...
    </mdui:UIInfo>
    <psc:RequestedPrincipalSelection
         xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">
      <psc:MatchValue Name="urn:oid:1.2.752.29.4.13" />
    </psc:RequestedPrincipalSelection>
  </md:Extensions>
  <md:KeyDescriptor use="signing">
    ...
```

Example of how an Identity Provider advertises, it its metadata, that it wishes to receive the Swedish personal identity number (personnummer) of the user in a `<PrincipalSelection>` extension element of the authentication request if this information is known to the requestor.

4. Schemas

The following XML schema defines the `http://id.swedenconnect.se/authn/1.0/principal-selection/ns` namespace:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
  targetNamespace="http://id.swedenconnect.se/authn/1.0/principal-selection/ns"
  xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">

  <xs:annotation>
    <xs:documentation>
      Schema location URL: https://docs.swedenconnect.se/schemas/authn/1.0/PrincipalSelection-1.0.xsd
    </xs:documentation>
  </xs:annotation>

  <xs:element name="PrincipalSelection" type="psc:PrincipalSelectionType" />
  <xs:complexType name="PrincipalSelectionType">
    <xs:sequence>
      <xs:element name="MatchValue" type="psc:MatchValueType" minOccurs="1" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>

  <xs:element name="RequestedPrincipalSelection" type="psc:RequestedPrincipalSelectionType" />
  <xs:complexType name="RequestedPrincipalSelectionType">
    <xs:complexContent>
      <xs:extension base="psc:PrincipalSelectionType" />
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="MatchValueType">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="NameFormat" type="xs:anyURI"
            default="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
        <xs:attribute name="Name" type="xs:string" use="required" />
        <xs:anyAttribute namespace="##any" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

</xs:schema>
```

5. Normative References

[RFC2119]

> Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[SAML2Core]

> OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[EidAttributes]

> Attribute Specification for the Swedish eID Framework.

6. Changes between versions

This is the first version of this specification.