Principal Selection in SAML Authentication Requests

Version 1.0 - 2019-01-24 - *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.

> Note: An Identity Provider acting as a proxy for BankID (see [ELN-0612]), in some cases require the user to provide his or hers personal identity number in order to initiate a BankID operation. Using the extension defined in this specification a BankID Identity Provider does not have to prompt the user for the personal identity number. This is especially useful when it is processing a request from a signature service.

This specification defines an element that may be included in the `<Extensions>` element of a SAML `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.

1.1. Requirement key words

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 name space 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`.

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>` [Zero 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>
```

2.2 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>
```

3. Examples

```
<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>
```

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

```
<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>
```

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.

Attributes in the examples above are specified in [ELN-0604].

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 maxOccurs="unbounded" name="MatchValue" type="psc:MatchValueType" minOccurs="1" />
    </xs:sequence>
  </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.

[ELN-0604]

> Attribute Specification for the Swedish eID Framework.

[ELN-0612]

> Implementation Profile for BankID Identity Providers within the Swedish eID Framework.

6. Changes between versions

This is the first version of this draft.