Updates to the Swedish eID Framework

2017-12-18

Table of Contents

1. Introduction
   1.1. Normative References
2. Updates
   E.1 Scoping in Authentication Requests sent by Signature Services
   E.2 Requirements for processing received authentication URI:s
   E.3. Signature Activation Protocol for Federated Signing
   E.4. Support for different person identifiers in certificate profile
   E.5. Updated version numbers and references for the DSS Extension Specification

1. Introduction

This document contains updates to the current version of the Swedish eID Framework. The current version of the Swedish eID Framework is published on http://elegnamnden.github.io/technical-framework, and comprises of specifications that are listed as “normative references” in chapter 1.1.

The updates presented in this document will be suggested to be part of the next official version of the Swedish eID Framework, and parties are not required to implement, or support, a suggested update until it is part of a Swedish eID Framework specification. However, Identity Providers are strongly advised to implement the updates in this document that concerns interoperability issues and/or covers a specific functionality that is handled by the Identity Provides.

For each update the following is covered:

- The reason for the update.
- The parties that will be affected by the change.

The update document represents changes that are not “substantive”. The changes focus on clarifications to ambiguous or conflicting specification text, and are intended to reduce interoperability problems within the Swedish eID federation.

In this document, update change instructions are presented with surrounding context as necessary to make the intent clear. Original specification text is often presented as follows, with problem text highlighted in bold:

- "This is an original specification. **This is text that needs to be changed.**"

New specification text is typically presented as follows, with new or changed text highlighted in bold:

- "This is an original specification. **This is the new text that was added in the errata.**"

1.1. Normative References

[EidProfile]

> Deployment Profile for the Swedish eID Framework, version 1.4

[EidRegistry]

> Registry for identifiers assigned by the Swedish e-identification board, version 1.4

[EidAttribute]

> Attribute Specification for the Swedish eID Framework, version 1.4

[EidEntCat]

> Entity Categories for the Swedish eID Framework, version 1.5

[EidDssProfile]

> Implementation Profile for using OASIS DSS in Central Signing Services, version 1.2

[EidDssExt]

> DSS Extension for Federated Central Signing Services, version 1.1

[EidCertProf]

> Certificate profile for certificates issued by Central Signing services, version 1.0

2. Updates

E.1. Scoping in Authentication Requests sent by Signature Services

Updates: Version 1.4 of the “Deployment Profile for the Swedish eID Framework”

An Identity Provider may adapt user interfaces or authentication procedures to different Service Providers either based on static configuration or based on information found in the Service Provider's metadata. It can therefore be useful for an Identity Provider to know which Service Provider that requested the signature that caused the Signature Service to request authentication in order for the Identity Provider to maintain the same user experience and procedures regardless of whether authentication is requested directly by the Service Provider, or by a Signature Service as a result of a signature request from the same Service Provider. Therefore, section 7.2, "Authentication Requests", of [EidProfile] has been extended with the following:

New:

It is RECOMMENDED that the `<saml2p:Scoping>` **element containing a** `<saml2p:RequesterID>` **element holding the entityID of the Service Requestor is included in** `<saml2p:AuthnRequest>` **messages generated by a Signature Service.**

```
<saml2p:Scoping>
  <saml2p:RequesterID>http://www.origsp.com/sp</saml2:RequesterID>
</saml2p:Scoping>
```

Example when the `<saml2p:RequesterID>` ***element is used to inform the Identity Provider about which Service Provider that requested the signature associated with this request for authentication.***

E.2. Requirements for processing received authentication URI:s

Updates: Version 1.4 of the “Deployment Profile for the Swedish eID Framework”

Section 6.3.4, "The Authentication Statement", contained a requirement about how to process a received authentication context URI that was incorrect. This has been corrected as follows:

Original:

The Service Provider MUST assert that the `<saml2:AuthnStatement>` contains a `<saml2:AuthnContext>` element that holds a `<saml2:AuthnContextClassRef>` element having as its value the authentication context URI indicating under which Level of Assurance the authentication was performed. **The Level of Assurance declared in the assertion MUST be equal to, or stronger[3] than, the Level of Assurance requested by the Service Provider.**

> **[3]: A stronger Level of Assurance identifier is simply a LoA having a higher value than what it is compared with, i.e.,** `http://id.elegnamnden.se/loa/1.0/loa4` **is stronger than** `http://id.elegnamnden.se/loa/1.0/loa3`**.**

New:

The Service Provider MUST assert that the `<saml2:AuthnStatement>` contains a `<saml2:AuthnContext>` element that holds a `<saml2:AuthnContextClassRef>` element having as its value the authentication context URI indicating under which Level of Assurance the authentication was performed. **If the Service Provider declared one, or more,** `<saml2:AuthnContextClassRef>` **elements under the** `<saml2p:RequestedAuthnContext>` **element of the authentication request (see section 5.4), the received authentication context URI MUST match one of the declared authentication context URI:s from the request. If not, the Service Provider MUST reject the assertion[3].**

> **[3]: If the Service Provider does not declare an authentication context URI in the authentication request it should be prepared to receive any of the authentication context URI:s declared by the Identity Provider in its metadata record (see section 2.1.3).**

E.3. Signature Activation Protocol for Federated Signing

A new specification, Signature Activation Protocol for Federated Signing, was introduced in order to specify a **Signature Activation Protocol** (SAP) and its data elements for implementation of **Sole Control Assurance Level 2** (SCAL2) according the European standards prEN 419241 - Trustworthy Systems Supporting Server Signing - Part 1 and 2 (prEN 419 241-1 and prEN 419 241-2).

The Signature Activation Protocol (SAP) defined in this document is used to exchange data between a signature service and a delegated authenticating authority such as a SAML Identity Provider. The function of the SAP is to authenticate the intent of a signer to sign a particular document, or collection of documents, through exchange of the following data elements.

Furthermore, the following specifications are updated to support SAP and SAD.

[EidProfile] - Deployment Profile for the Swedish eID Framework

In section 2.1.3 of [EidProfile], the following were added:

Identity Providers SHALL advertise support for the SAP protocol according to [SigSAP], by including the service property entity category URI `http://id.elegnamnden.se/sprop/1.0/scal2` in its metadata. An Identity Provider that does not advertise support for SAP MAY ignore requests for SAD.

```
<md:Extensions>
  <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    <saml:Attribute Name="http://macedir.org/entity-category"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <saml:AttributeValue xsi:type="xs:string">http://id.elegnamnden.se/sprop/1.0/scal2</saml:AttributeValue>
    </saml:Attribute>
    ...
  </mdattr:EntityAttributes>
</md:Extensions>
```

Example of how an Identity Provider advertises its support for SCAL2 authentication.

The new section 7.2.2 specifies how signature activation data is requested.

[EidRegistry] - Registry for identifiers assigned by the Swedish e-identification board

- Section 3.1.3.2 of [EidRegistry] declares the `http://id.elegnamnden.se/sprop/1.0/scal2` service property entity category.
- Section 3.1.5 of [EidRegistry] declares the XML schema name space for the Signature Activation Protocol - `http://id.elegnamnden.se/csig/1.1/sap/ns`.

[EidAttribute] - Attribute Specification for the Swedish eID Framework

- Section 3.2.3 of [EidAttribute] clarifies the contents of the `sad` attribute value.

[EidEntCat] - Entity Categories for the Swedish eID Framework

- Section 3.2 of [EidEntCat] defines the new service propety entity category **scal2**.

[EidDssProf] - Implementation Profile for using OASIS DSS in Central Signing Services

Section 2.1.3.9 of [EidDssExt] is extended with the following text:

When the `CertType` attribute is present with a value of `QC/SSCD` the signature service MUST request authentication in accordance with the “Deployment Profile for the Swedish eID Framework” [Eid-Profile] section 7.2.2, or reject the request.

E.4. Support for different person identifiers in certificate profile

Updates: Version 1.0 of the "Certificate profile for certificates issued by Central Signing services".

Section 2.3.1.1, "Person identifier attributes" was added where data sources and data formats are described to make it possible to use Swedish "personnummer"/"samordningsnummer", Provisional ID:s or eIDAS person identifiers in the `serialNumber` attribute.

E.5. Updated version numbers and references for the DSS Extension Specification

Updates: Version 1.1 of the "DSS Extension for Federated Central Signing Services" specification.

The version 1.1 contained some outdated references and version numbers that have been corrected. See the diff for details.