LEGITIMATIONS NÄMNDEN

Updates to the Swedish eID Framework

2015-12-14

www.elegnamnden.se

Postadress	Besöksadress	Telefon växel	E-postadress
171 94 SOLNA	Korta gatan 10	010-574 21 00	kansliet@elegnamnden.se

LEGITIMATIONS NÄMNDEN

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 www.elegnamnden.se, and comprises of specifications that are listed as “normative references” in chapter 1.1.1.

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 Provider[1].

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] E-legitimationsnämnden may also enforce that a specific Identity Provider implements a given update before it is included in an official release of the Swedish eID Framework. Typically, that may be the case when important functions within the federation do not function as intended without the proper support of the Identity Provider.

1.1 Normative References

1.1.1 Swedish eID Framework

[EidProfile]
Deployment Profile for the Swedish eID Framework, version 1.3.

1.1.2 Other References

[SAML2Meta]
OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2Int]
SAML2int profile v0.21 – SAML 2.0 Interoperability Profile.

2 Updates

E.1 Requirement for AssertionConsumerServiceURL in Authentication Requests

Updates: Version 1.3 of the "Deployment Profile for the Swedish eID Framework"

Section 5.3 of [EidProfile] states that a `<saml2p:AuthnRequest>` message MUST contain an `AssertionConsumerServiceURL` attribute identifying the desired response location. It has shown that this requirement aggravates interoperability since some of the major providers of Service Provider software do not fully support this attribute. Furthermore, the requirement does increase security since an Identity Provider may only post response messages to locations registered in the `<md:AssertionConsumerService>` elements of the Service Provider metadata entry. Therefore, the following changes are made:

In section 5.3 of [EidProfile]:

Original:

> **[SAML2Int]** specifies that a `<saml2p:AuthnRequest>` message **MUST** contain an `AssertionConsumerServiceURL` attribute identifying the desired response location.

New:

> The `<saml2p:AuthnRequest>` message **SHOULD** contain an `AssertionConsumerServiceURL` attribute identifying the desired response location.

In section 5.4.2 of [EidProfile]:

Original:

> **The value of the `AssertionConsumerServiceURL` attribute of the `<saml2p:AuthnRequest>` message** MUST be verified to be consistent with one of the `<md:AssertionConsumerService>` elements having the HTTP-POST binding found in the Service Provider's metadata entry. If this is not the case, the request must be rejected.

New:

LEGITIMATIONS NÄMNDEN

> **If the `AssertionConsumerServiceURL` attribute is present in the `<saml2p:AuthnRequest>` message, its value** MUST be verified to be consistent with one of the `<md:AssertionConsumerService>` elements having the HTTP-POST binding found in the Service Provider's metadata entry. If this is not the case, the request must be rejected.
>
> **If the attribute is not present in the `<saml2p:AuthnRequest>` message, the Identity Provider MUST obtain the desired response location from the Service Provider's metadata entry. This location is found in an `<md:AssertionConsumerService>` element with HTTP-POST binding that is marked as default (has the `isDefault` attribute set), or if no element has the `isDefault` attribute set, the one with the lowest index value (see section 2.4.4.1 of [SAML2Meta]).**

In section 6.3.2 of [EidProfile]:

New:

> The `Recipient` attribute from the bearer `<saml2:SubjectConfirmationData>` element MUST match the location to which the `<saml2p:Response>` message was delivered and match value the `AssertionConsumerServiceURL` attribute included in the request message**, or if this attribute was not provided in the request message, the default response location specified in the Service Provider's metadata entry, as described in section 5.4.2.**