Certificate profile for certificates issued by Central Signing services

Version 1.0 - 2013-10-30

ELN-0608-v1.0

Table of Contents

1. Introduction

This document specifies a certificate profile for certificates issued by a signature service within the infrastructure for “Svensk E-legitimation”.

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 behavior 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 **saci:** stands for the SAML Authentication Context Information XML Schema namespace (`http://id.elegnamnden.se/auth-cont/1.0/saci`).

1.3. Structure

This specification uses the following typographical conventions in text: `<Eid2Element>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

2. Certificate Profile

2.1. Standards

The following standards provides normative requirements for this certificate profile:

Standard	Function	Referens
RFC 5280	Main certificate standard	[RFC5280]
RFC 3739	Main certificate profile for Qualified Certificates	[RFC3739]
EN 319 412-5	EU profile of RFC 3739 providing defined data structures for issuing Qualified Certificate in accordance with the EU electronic signature directive [EUSig].	[EU-QC]
TS 102 280	EU interoperability profile for certificates issued to Natural Persons.	[EU-INTEROP]

2.2. Qualified and PKC Certificates

This profile supports both Qualified Certificates as well as certificates that are not Qualified Certificates, here named PKC certificates (Public Key Certificates).

The same profile requirements apply for both Qualified Certificates and for PKC certificates unless a requirement is explicitly related to only Qualified Certificates.

2.3. Certificate content

All certificates SHALL be fully compliant with [RFC5280], [RFC3739] and [EU-INTEROP]. All Qualified Certificates SHALL also be fully compliant with [EU-QC].

Qualified Certificates SHALL implement the “Statement regarding location of Policy Disclosure Statements” (PDS) as specified in section 5.2.4 of [EU-QC].

2.3.1. Subject attributes and name forms

Subject name attributes and other name forms in the certificate SHALL comply with [RFC3739].

The following specific certificate subject name conventions SHALL be met:

Subject data	Requirement
Swedish “personnummer”	Swedish “personnummer” obtained from a SAML assertion using the attribute with OID 1.2.752.29.4.13, SHALL be stored in a serialNumber attribute (OID 2.5.4.5) in the subject field. The data SHALL be composed according to [SKV704]

Subject data	Requirement
Swedish “samordningsnummer”	Swedish “samordningsnummer” obtained from a SAML assertion using the attribute with OID 1.2.752.29.4.13, SHALL be stored in a serialNumber attribute (OID 2.5.4.5) in the subject field. The data SHALL be composed according to [SKV707].
E-mail address	E-mail address, when present, SHALL be stored in a Subject Alternative Name extension as an rfc822Name.

2.3.2. Authentication Context and Attribute mapping

Certificates MUST include an `AuthContextExtension` according to [AuthCont]. This extension SHALL include one SAML Authentication Context Information element identified by the XML schema name space identifier:

```
http://id.elegnamnden.se/auth-cont/1.0/saci
```

The `<saci:SAMLAuthContext>` element SHALL contain both an `<saci:AuthContextInfo>` element as well as an `<saci:IdAttributes>` element.

The `<saci:IdAttributes>` element SHALL contain one `<saci:AttributeMapping>` element for each subject attribute or other name form that was obtained from a SAML attribute in the SAML assertion used to authenticate the signer as part of the signature creation process. Each `<saci:AttributeMapping>` element SHALL provide the `<saml:AttributeValue>` that were obtained from the SAML assertion.

3. Normative References

[RFC2119]

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

[RFC3739]

> Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[RFC5280]

> Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[EU-QC]

> “Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile”, ETSI TS 319 412-5 V1.1.1, Jan 2013.

[EU-INTEROP]

> “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons”, ETSI TS 102 280 V1.1.1, March 2004.

[AuthCont]

> RFC-7773: Authentication Context Certificate Extension

[SKV704]

> Skatteverket, SKV 704 utgåva 8, Personnummer, September 2007.

[SKV707]

> Skatteverket, SKV 707, Utgåva 2, Samordningsnummer.