Certificate Profile for Certificates Issued by Central Signing Services

Version 1.2 - 2018-08-29 - *Draft version*

ELN-0608-v1.2

Table of Contents

1. Introduction

This document specifies a certificate profile for certificates issued by a signature service based on the OASIS DSS protocol [DSS], enhanced by the DSS Extensions for Federated Central Signing Services [DSS-Ext].

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	Reference
RFC 5280	Main certificate standard	[RFC5280]
RFC 7773	Authentication context extension	[RFC7773]
EN 319 411-1	Policy requirements for PKC certificates	[EU-POL-NCP]
EN 319 411-2	Policy requirements for Qualified certificates	[EU-POL-QC]
EN 319 412-1	Definitions of semantic identifies and formatting rules for identity data	[EU-CERT-GEN]
EN 319 412-2	Certificate profile for certificates issued to natural persons	[EU-CERT-NP]
EN 319 412-5	Declaration of qualified certificate properties	[EU-CERT-QC]

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).

All profile requirements apply to both Qualified Certificates and to PKC certificates unless it is explicitly stated that a particular requirement applies only to PKC or Qualified Certificates.

2.3. Certificate content

All certificates SHALL be fully compliant with [RFC5280] and [EU-CERT-NP]. All Qualified Certificates SHALL also implement mandatory QC statements as defined in [EU-CERT-QC].

2.3.1. Subject attributes and name forms

2.3.1.1. Person identifier attributes

2.3.1.1.1. Data source

All certificates SHALL contain a unique person identifier, carried in the `serialNumber` attribute (OID 2.5.4.5) in the subject field. The person identifier SHALL be obtained from the Identity Provider in the form of a SAML attribute. For PKC certificates the SAML attribute SHOULD be one of the attributes listed below. For Qualified Certificates the SAML attribute SHALL be one of the attributes listed below.

Attribute	Attribute name	Specification
Swedish personal identity number (personnummer)[1]	urn:oid:1.2.752.29.4.13	[AttrSpec]
Provisional ID	urn:oid:1.2.752.201.3.4	[AttrSpec]

Attribute	Attribute name	Specification
eIDAS person identifier	urn:oid:1.2.752.201.3.7	[AttrSpec]

> [1]: The urn:oid:1.2.752.29.4.13 attribute is also defined to be able to hold a Swedish coordination number (samordningsnummer).

2.3.1.1.1. Data format

The identifier data obtained from the SAML assertion SHALL be stored in the `serialNumber` attribute using one of the following formats:

- using exactly the same format as it was obtained from the SAML attribute, or,
- using conventions specified in [EU-CERT-GEN] as defined below.

When storing person identifier in the `serialNumber` attribute in accordance with [EU-CERT-GEN], the certificate SHALL include a semantics identifier as specified in section 5.1. of [EU-CERT-GEN].

Swedish personal identity number (personnummer)

When the identifier is a Swedish personal identity number (personnummer), or a coordination number (samordningsnummer), the semantics identifier SHALL be a natural person semantics identifier using the identity type reference "PNO".

> Example: PNOSE-194911172296

Provisional ID

When the identifier is a provisional ID the semantics identifier SHALL be a natural person semantics identifier using a local national identity type reference "PI:SE".

> Example: PI:SE-NO:16043700158

This identifier illustrates that the identifier is a Provisional ID (PI) as defined in Sweden (SE) followed by a hyphen (-) and the actual provisional ID for a person from Norway (NO:16043700158).

When the identity type reference is "PI:SE", the `nameRegistrationAuthorities` element of SemanticsInformation shall be present and shall contain a `uniformResourceIdentifier` `generalName` with the following value:

> `http://id.elegnamnden.se/eln/name-registration-authority`

eIDAS person identifier

eIDAS person identifier attributes MAY be stored in the serial number attribute having exactly the same format as received from the SAML attribute listed above, supported by providing a semantics identifier according to [EU-CERT-GEN] identified by the OID `0.4.0.194121.1.3`.

NOTE:

> A new version of the [EU-CERT-GEN] is processed for approval at the time of publication of this document. The new version will specify a semantics identifier for storing eIDAS person identifier attributes using the semantics identifier OID `0.4.0.194121.1.3`. This semantics identifier (`id-etsi-qcs-semanticsId-eIDASNatural`) is not yet present in the latest published version of the standard.

2.3.1.2. Other attribute requirements

An 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 [RFC7773]. 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.

2.3.3. Certificate Policy

Certificates SHALL contain at least one referenced certificate policy. PKC certificates SHALL contain at least one reference to a policy idefined in [EU-POL-NCP]. Qualified Certificates SHALL reference at least one certificate policy identified in [EU-POL-QC].

3. Normative References

[DSS]

> OASIS Standard - Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, April 11, 2007.

[DSS-Ext]

> DSS Extension for Federated Central Signing Services.

[AttrSpec]

> Attribute Specification for the Swedish eID Framework.

[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.

[RFC7773]

> RFC-7773: Authentication Context Certificate Extension

[EU-POL-NCP]

> ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[EU-POL-QC]

> ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[EU-CERT-GEN]

> ETSI EN 319 412-1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[EU-CERT-NP]

> ETSI EN 319 412-2, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

[EU-CERT-QC]

> ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[SKV704]

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

[SKV707]

> Skatteverket, SKV 707, Utgåva 2, Samordningsnummer.

4. Changes between versions

Changes between version 1.1 and version 1.2:

- Update of logotype, fixes of typos and reference list.

Changes between version 1.0 and version 1.1:

- Removed the requirement to store "personnummer" or "samordningsnummer".
- Updated standards references to remove old deprecated standards and replace them with the currently published documents.
- Specified optional support for using semantics identifiers in accordance with ETSI EN 319 412-1 to specify that the serialNumber attribute contains a Swedish "personnummer" or "samordningsnummer", Provisional ID or eIDAS person identifier.
- Added requirement to specify ETSI policy identifiers.
- Fix of invalid links for SKV704 and SKV707.