Revisionshistorik

Version	Datum	Kommentar
0.1	2019-01-07	Etablering av dokumentet
0.2	2019-01-18	Efter första genomgång av Cygate och SITHS PA
0.3	2019-01-28	Efter andra genomgång av SITHS PA. Tog bort underskriftscertifikat efter diskussion med SecMaker.
0.4	2019-02-21	Tog bort UPN efter diskussion med SITHS PA. orgName och localityName får vara kvar
1.0	2019-02-21	Fastställande av SITHS Policy Authority
1.1	2019-10-16	Beslutad av SITHS PA. Förtydliganden kring åtkomst via Sjunet
1.2	2020-04-02	Tillägg av certifikatprofil med elliptic curve (ECC), med kurvan prime256v1/secp256r1, som privat nyckel

Inledning

Inom SITHS e-id finns det certifikat för olika syften som grupperas enligt:

- Slutanvändarcertifikat för informationsutbyte mellan servrar, tjänster och applikationer
  - SITHS e-id Function CA v1
- Slutanvändarcertifikat för identifiering av personer
  - SITHS e-id Person ID 2 CA v1
  - SITHS e-id Person ID 3 CA v1
  - SITHS e-id Person ID Mobile CA v1 **(beskrivs i detta dokument)**
  - SITHS e-id Person HSA-id 2 CA v1
  - SITHS e-id Person HSA-id 3 CA v1

Certifikaten som beskrivs i denna specifikation utfärdas till personer:

- Som finns i HSA med personnummer.
- Som ett enda certifikat, vilket används både för legitimering och underskrift
- På enheter med mjukvaruskydd av de privata nycklarna. Det vill säga i en, av Inera, kvalitetssäkrad applikation på en mobiltelefon eller surfplatta.

Kodning av attribut sker i enlighet med de för respektive attribut gällande specifikationer. Observera särskilt att vissa attribut kodas enligt UTF-8.

Testmiljö - PKI

Testmiljön för PKI har till största delen likadana certifikatspecifikationer som produktion vad gäller innehåll och egenskaper. Undantagen är följande:

- Samtliga utfärdares namn kompletteras med ett begynnande *”TEST ”,* t ex. *”**TEST** SITHS e-id Root CA v2”*
- Samtliga URL:er för AIA, CRL och CDP kompletteras med
  - *pp* i url, t ex. *”https://crl1**pp**.siths.se”*eller *”https://ocsp1pp.siths.se”*
  - ett inledande *”test”* i själva filnamnet, t ex. *”https://crl1pp.siths.se/**test**sithseidpersonid3cav1.crl*

Åtkomst via Sjunet

Samtliga URL:er för CRL, AIA och OCSP går att nå både via Internet och Sjunet. Detta baserar sig dock på att respektive DNS-värde slås upp korrekt mot Sjunets DNS-server.

Tekniken för detta kallas Dual-view DNS och i praktiken innebär det att ett DNS-värde kan resultera i olika IP-adresser beroende på vilken IP-adress den som ställer frågan presenterar mot DNS-servern.

T ex kommer crl1.siths.se ge:

- En Internet IP-adress om frågan ställs via Sjunet
- En Sjunet IP-adress om frågan ställs via Sjunet

Se mer information i dokumentet ”Sökvägar och brandväggsöppningar”

Tillitsnivå

Certifikat för personer kan ha olika tillitsnivå (LoA=Level of Assurance). För SITHS e-id anges detta i attributet ”Certifikatprinciper” genom att olika O.I.D:er skrivs beroende på egenskaper som:

- vilken utfärdandeprocess som användes
- hur de privata nycklarna skyddats under tillverkning och leverans till användaren
- hur ”aktiveringsdata”, dvs. pin-koder, säkerhetskoder och puk-koder som krävs för att använda e-legitimationen har skyddats under tillverkning och leverans till användaren

Vilken tillitsnivå en viss O.I.D motsvarar representeras av den matris som återfinns på https://www.inera.se/siths/repository.

SITHS tillitsnivåer baserar sig på tillitsramverket för Svensk e-legitimation

Personcertifikat (RSA) för legitimering med personnummer

Med maxlängd i tabellen nedan avses antal tecken i datadelen av attributet.

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
version	1	3		CA	M	N/A
serialNumber	64	*<Randomiserad med hemlig algoritm i CA-systemet>*	00d9b4778ba5ed51e811f2a664a793ae3a191	CA	M	N/A
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		CA	M	N/A
issuer						N/A
countryName (2.5.4.6)	2	SE		CA	M	
organizationName (2.5.4.10)	64	Inera AB		CA	M	
commonName (2.5.4.3)	64	SITHS e-id Person ID Mobile CA v1		CA	M	
validity		*<minst 1h max 2 år>*	Exakt tid bestäms av portalen			N/A
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	CA	M	
subject						N/A
serialNumber (2.5.4.5)	64		191212121212	RA (HSA)	M	
givenName (2.5.4.42)	64		Rane	Ärvs	MIP[1]	
surName (2.5.4.4)	64		Larsson Ramberg	Ärvs	M	
commonName (2.5.4.3)	64		Rane Larsson Ramberg	Ärvs	M	
organizationName (2.5.4.10)	64		Region Västernorrland	Ärvs	M	
localityName (2.5.4.7)	128		Västernorrlands län	Ärvs	MIP[1]	
countryName (2.5.4.6)	2		SE	Ärvs	M	
subjectPublicKeyInfo						N/A
algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M	
Algorithm Parameters		*05 00* NULL		CA	M	
subjectPublicKey		*Certifikatets publika nyckel, beräknad enligt angiven algoritm, 3072-bitar lång*		CA	M	
cRLDistributionPoints (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithseidpersonidmobilecav1.crl		CA	M	NC
authorityInformationAccess (1.3.6.1.5.5.7.1.1)		[1] Authority Info Access		CA	M	NC

[1] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
		Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.siths.se [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithseidpersonidmobilecav1.cer				
certificatePolicies (2.5.29.32)		[1]Certificate Policy: Policy Identifier=2.23.140.1.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository [2]Certificate Policy: Policy Identifier=SE EXEMPEL --> [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository	Värdet ”Qualifier” i det andra [2] av dessa objekt kommer att kunna anta olika värden beroende på vilken rutin som användes vid utfärdande av certifikatet. Detta indikerar också tillitsnivån för den identitet som certifikatet pekar enligt tillitsramverket för Svensk e-legitimation Matris som indikerar detta återfinns på https://www.inera.se/siths/repository	CA	M	NC
enhancedKeyUsage					O	NC
clientAuthentication (1.3.6.1.5.5.7.3.2)				RA		
subjectKeyIdentifier (2.5.29.14)						NC
keyIdentifier		*<octet sträng> Byggs upp av en del av certifikatets publika nyckel kombinerat med HASH över SHA-1*		CA	M	
authorityKeyIdentifier (2.5.29.35)						NC
keyIdentifier		*<octet sträng> bestående av subjectKeyIdentifier för utfärdande CA*		CA	M	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment		CA	M	C
Signature		*RSA-signatur över SHA256*		CA	M	N/A

Personcertifikat (ECC) för legitimering med personnummer

Med maxlängd i tabellen nedan avses antal tecken i datadelen av attributet.

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
version	1	3		CA	M	N/A
serialNumber	64	*<Randomiserad med hemlig algoritm i CA-systemet>*	00d9b4778ba5ed51e811f2a664a793ae3a191	CA	M	N/A
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		CA	M	N/A
issuer						N/A
countryName (2.5.4.6)	2	SE		CA	M	
organizationName (2.5.4.10)	64	Inera AB		CA	M	
commonName (2.5.4.3)	64	SITHS e-id Person ID Mobile CA v1		CA	M	
validity		*<minst 1h max 2 år>*	Exakt tid bestäms av portalen			N/A
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	CA	M	
subject						N/A
serialNumber (2.5.4.5)	64		191212121212	RA (HSA)	M	
givenName (2.5.4.42)	64		Rane	Ärvs	MIP[2]	
surName (2.5.4.4)	64		Larsson Ramberg	Ärvs	M	
commonName (2.5.4.3)	64		Rane Larsson Ramberg	Ärvs	M	
organizationName (2.5.4.10)	64		Region Västernorrland	Ärvs	M	
localityName (2.5.4.7)	128		Västernorrlands län	Ärvs	MIP[1]	
countryName (2.5.4.6)	2		SE	Ärvs	M	
subjectPublicKeyInfo						N/A
Algorithm		ECC {1.2.840.10045.2.1}		CA	M	
Algorithm Parameters		*06 08 2a 86 48 ce 3d 03 01 07* prime256v1/secp256r1 (1.2.840.10045.3.1.7)		CA	M	
subjectPublicKey		*Certifikatets publika nyckel, beräknad enligt angiven algoritm*		CA	M	
cRLDistributionPoints (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithseidpersonidmobilecav1.crl		CA	M	NC
authorityInformationAccess (1.3.6.1.5.5.7.1.1)		[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		CA	M	NC

[2] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
		Alternative Name: URL=http://ocsp1.siths.se [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithseidpersonidmobilecav1.cer				
certificatePolicies (2.5.29.32)		[1]Certificate Policy: Policy Identifier=2.23.140.1.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository [2]Certificate Policy: Policy Identifier=SE EXEMPEL --> [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository	Värdet ”Qualifier” i det andra [2] av dessa objekt kommer att kunna anta olika värden beroende på vilken rutin som användes vid utfärdande av certifikatet. Detta indikerar också tillitsnivån för den identitet som certifikatet pekar enligt tillitsramverket för Svensk e-legitimation Matris som indikerar detta återfinns på https://www.inera.se/siths/repository	CA	M	NC
enhancedKeyUsage					O	NC
clientAuthentication (1.3.6.1.5.5.7.3.2)				RA		
subjectKeyIdentifier (2.5.29.14)						NC
keyIdentifier		*<octet sträng> Byggs upp av en del av certifikatets publika nyckel kombinerat med HASH över SHA-1*		CA	M	
authorityKeyIdentifier (2.5.29.35)						NC
keyIdentifier		*<octet sträng> bestående av subjectKeyIdentifier för utfärdande CA*		CA	M	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment		CA	M	C
Signature		*RSA-signatur över SHA256*		CA	M	N/A

Kommentarer attribut för attribut

Version

Anger version av X.509 certifikatstandard.

serialNumber

Unikt nummer för certifikat utfärdade av denna CA, som också genererar numret. Skall vara ett heltal. Representeras som ett heltal (”Integer”)

signatureAlgorithm

Denna sträng anger signerings- och hash-algoritm som agerar underlag för signatur.

Issuer

I detta objekt anges utfärdarens identitet. Sätts av certifikatsutfärdaren.

countryName

Detta attribut skall alltid vara “SE” och anger att certifikatsutfärdaren är en organisation registrerad i Sverige. Anges som printable_string.

organizationName

Namnet på certifikatsutfärdaren. Anges som UTF8_string.

commonName

Utfärdande CA. Anges som UTF8_string.

Validity

Detta objekt innehåller två attribut:

notBefore

här anges när certifikatet skall börja gälla; detta kan sättas till valfri tid fram till tidpunkten notAfter.

notAfter

här anges när certifikatet skall sluta gälla; detta attribut sätts idag av certifikatsutfärden 2 år.

Tidpunkterna kodas som ”UTCTime”.

Subject

I detta objekt anges egenskaper hos personen i certifikatstermer även kallad nyckelinnehavaren (subjektet).

countryName

Detta attribut skall alltid vara “SE” och anger att nyckelinnehavaren är en organisation eller person registrerad i Sverige. Sätts av certifikatsutfärdaren. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som printable_string.

localityName

Detta attribut innehåller namn på ort i klartext. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som UTF8string.

organizationName

Detta attribut innehåller namn på huvudman eller motsvarande. Skall vara en juridisk person[2] med organisationsnummer. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som UTF8string.

commonName

Bildas av givenName följt av surName. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som UTF8_string.

surName

I de fall en person har ett mellannamn (middleName i HSA) används även det i surName. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som UTF8_string.

givenName

Obligatoriskt om det finns i folkbokföringen, om det inte finns lämnas attributet tomt. Hämtas från det certifikat som användaren loggar in i Självadministrationen med. Anges som UTF8_string.

serialNumber

Personnummer enligt YYYYMMDDNNNN. Hämtas från HSA genom uppslagning av HSA-id för det certifikat som användaren använder för att hämta Mobilt SITHS e-id i Självadmin. Anges som printable_string.

subjectPublicKeyInfo

Detta objekt innehåller två attribut som definierar den publika nyckeln i certifikatet.

Algorithm

Anger vilken algoritm som skall används vid kryptering/dekryptering med den publika nyckeln. Sätts av certifikatsutfärdaren. Värdet ska vara något av följande:

- **rsaEncryption** {1.2.840.113549.1.1.1}.
- **ecPublicKey** {1.2.840.10045.2.1}

Algorithm Parameters

Varierar med vilken nyckelalgoritm som pekas ut i attributet *Algorithm* ovan:

- ECC:

  06 08 2a 86 48 ce 3d 03 01 07

  prime256v1/secp256r1 {1.2.840.10045.3.1.7}
- RSA:

  05 00

  NULL

subjectPublicKey
Detta attribut innehåller den publika nyckeln. Genereras av certifikatsutfärdaren. Anges som bit string.

cRLDistributionPoints
Identifierar platserna där spärrlistan lagras. Två platser finns, en på Internet och en på Sjunet. Dessa delar dock samma URL som returnerar olika IP-adresser beroende på om frågan till DNS-servern ställs via Internet eller Sjunet

authorityInformationAccess
Innehåller adress till aktuell OCSP-tjänst (online certificate status protocol) samt länkar som leder till utfärdarens CA-certifikat. Två platser finns, en på Internet och en på Sjunet. Dessa delar dock samma URL som returnerar olika IP-adresser beroende på om frågan till DNS-servern ställs via Internet eller Sjunet.

certificatePolicies

policyIdentifer
[1] OID som pekar på ”Individual validated” enligt CA Browser Forum Baseline requirements

samt

[2] OID som reflekterar vilken utfärdanderutin som använts och även tillitsnivån för certifikatet enligt tillitsramverket för Svensk e-legitimation, se separat matris på https://www.inera.se/siths/repository. Sätts av certifikatsutfärdaren.

policyQualifier

En per identifier, innehåller länkar som pekar på https://www.inera.se/siths/repository

enhancedKeyUsage

clientAuthentication

Certifikat med detta syfte kan användas för att identifiera en användare som anropar en server.

subjectKeyIdentifier

keyIdentifier
Obligatoriskt attribut som består av en SHA-1 HASH av en del av certifikatet publika nyckel. Anges som octet_string.

authorityKeyIdentifier

keyIdentifier
Detta attribut innehåller *subjectKeyIdentifier* för den certifikatsutfärdare som utfärdat certifikatet. Detta möjliggör att det kan finnas flera samtidigt gällande publika CA-nycklar. Anges som octet_string.

keyUsage
I detta attribut definieras hur den publika nyckel (och den privata) får användas. Anges som bit_string. Attributet antar alltid följande två värden:
a) *digitalSignature + keyEncipherment*

Översikt mappning av certifikatinnehållet jämför med Identitetsintyg

* - Subject i certifikat bestäms genom ärvd legitimering och blir alltså detsamma som för det certifikat som användes vid hämtning av Mobilt SITHS.

Subject	Attribut i Identitetsintyg*
serialNumber	X509SubjectName\serialNumber
givenName	X509SubjectName\givenName
Surname	X509SubjectName\surname
	X509SubjectName\middleName
commonName	X509SubjectName\commonName
organizationName	X509SubjectName\organizationName
localityName	X509SubjectName\localityName
countryName	X509SubjectName\SE