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
1.3	2021-03-16	Justering till korrekt nyckellängd, 2048-bitar RSA för Android
2.0	2024-04-10	Fastställd av SITHS PA

Inledning

Inom SITHS e-id finns det certifikat för olika syften som grupperas under certifikatutfärdare enligt följande struktur:

- SITHS e-id Root CA v2
  - 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 ID 2 CA v1
    - SITHS e-id Person HSA-id ID 3 CA v1
- SITHS e-id Card Identifier CA v1
  - Certifikat för identifiering av smarta kort

Certifikaten som beskrivs i denna specifikation utfärdas:

- Till personer med svenskt personnummer som inte är avregistrerad i svensk folkbokföring med undantag för avregistreringskoden UV *(Utvandrad)*.

- Endast som legitimeringscertifikat.
- På bärare med hårdvaruskydd för privata nycklarna. Det vill säga i en secure enclave/TPM på den mobila enheten med hjälp av en kvalitetssäkrad applikation.

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

Testmiljö – PKI

OBS! PKI i TEST-miljön är avsedd för internt bruk inom Inera och distribueras därför inte till kund med undantag för Mobilt SITHS utfärdaren

Testmiljön har till största delen likadana certifikatspecifikationer som produktion vad gäller innehåll och egenskaper.

Undantagen gäller sökvägar och namnsättning av CA och spärrlistefiler. Undantagen är följande:

- Samtliga utfärdares namn kompletteras med ett inledande *”SYSTEMTEST”,* t ex. *” **SYSTEMTEST** SITHS e-id Root CA v1”*
- Samtliga sökvägar för AIA, CRL och CDP följer denna syntax
  - *crl.<miljö>.siths.se* i url, t ex. *”http://crl.test.siths.se”*eller *”https://ocsp.test.siths.se”*
  - ett inledande *”systemtest”* i själva filnamnet för CRL-filerna, t ex. *”http://crl.test.siths.se/**systemtest**sithseidpersonid3cav1.crl*

QA-miljö - PKI

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

Undantagen gäller sökvägar och namnsättning av CA och spärrlistefiler. Undantagen är följande:

- Samtliga utfärdares namn kompletteras med ett inledande *”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. *”http://crl1**pp**.siths.se, ”http://ocsp1**pp**.siths.se” eller ”http://aia**pp**.siths.se*
  - ett inledande *”test”* i själva filnamnet, t ex. *”https://crl1pp.siths.se/**test**sithseidpersonid3cav1.crl*

Åtkomst via Sjunet

Samtliga sökvägar för CRL, AIA och OCSP går att nå både via Internet och Sjunet. Detta fungerar så att den IP-adress som levereras som svar på DNS-frågan fungerar över både Internet och Sjunet.

Det gäller därför att systemen som ska kontrollera certifikat:

- styr trafiken över rätt nätverk

- sätter en source-ip som tillhör det nätverket
- öppnar brandväggen för rätt nätverk

För mer information, se Nätverksinställningar för SITHS

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 presenteras i den matris som återfinns på Matris för tolkning av tillitsnivåer.

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
version	1	3		CA	M	
serialNumber	64	*<Randomiserad med hemlig algoritm i CA-systemet>*	00d9b4778ba5ed51e811f2a664a793ae3a191	CA	M	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		CA	M	
issuer						
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			
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	CA	M	
subject						
serialNumber (2.5.4.5)	64		191212121212	Ärvs	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 alt. Portal	M	
localityName (2.5.4.7)	128		Västernorrlands län	Ärvs	MIP[1]	
countryName (2.5.4.6)	2		SE	Ärvs	M	
subjectPublicKeyInfo						
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, 2048-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	

[1] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
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) 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		CA	M	
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 certifikatet enligt tillitsramverket för Svensk e-legitimation Matris som presenterar detta återfinns på https://www.inera.se/siths/repository	CA	M	
enhancedKeyUsage					O	
clientAuthentication (1.3.6.1.5.5.7.3.2)				RA		
subjectKeyIdentifier (2.5.29.14)						
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)						
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	

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
version	1	3		CA	M	
serialNumber	64	*<Randomiserad med hemlig algoritm i CA-systemet>*	00d9b4778ba5ed51e811f2a664a793ae3a191	CA	M	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		CA	M	
issuer						
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			
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	CA	M	
subject						
serialNumber (2.5.4.5)	64		191212121212	Ärvs	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 alt. Portal	M	
localityName (2.5.4.7)	128		Västernorrlands län	Ärvs	MIP[1]	
countryName (2.5.4.6)	2		SE	Ärvs	M	
subjectPublicKeyInfo						
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	
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	

[2] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	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 certifikatet enligt tillitsramverket för Svensk e-legitimation Matris som presenterar detta återfinns på https://www.inera.se/siths/repository	CA	M	
enhancedKeyUsage					O	
clientAuthentication (1.3.6.1.5.5.7.3.2)				RA		
subjectKeyIdentifier (2.5.29.14)						
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)						
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	

Kommentarer attribut för attribut

Attribut	Underliggande attribut & format	Kommentar	Källa
Version	integer	Anger version av X.509 certifikatstandard.	Certifikatutfärdaren
serialNumber	integer	Unikt nummer för certifikat utfärdade av denna CA, som också genererar numret. Skall vara ett heltal. Representeras som ett heltal	Certifikatutfärdaren
signatureAlgorithm	sequence\object_id	Denna sträng anger signerings- och hash-algoritm som agerar underlag för signatur.	SITHS eID Portal i kombination av certifikatutfärdaren
Issuer	**commonName** utf8_string **organizationName** utf8_string **countryName** printable_string	I detta objekt anges utfärdarens identitet. **commonName** Namn på utfärdande CA. I detta fall ”SITHS e-id Person ID Mobile CA v1”. **organizationName** Namnet på den organisation som står bakom certifikatutfärdaren. För SITHS är detta alltid satt till ”Inera AB”. **countryName** Namnet på det Land certifikatutfärdaren finns i. För SITHS är detta alltid satt till ”SE” för Sverige.	Certifikatutfärdaren.
Validity	utc_time	Datum och tid för när certifikatets giltighetstid börjar och tar slut. Tidpunkterna kodas som ”UTCTime”. **notBefore** Här anges när certifikatet skall börja gälla; detta kan sättas till valfri tid fram till tidpunkten notAfter. Anges till den tidpunkt då certifikatet signeras. **notAfter** Här anges när certifikatet skall sluta gälla. I dagsläget alltid 2 år från utfärdandet.	**notBefore** Certifikatutfärdaren **notAfter** SITHS eID Portal
Subject	**serialNumber** printable_string **givenName** utf8_string **surName** utf8_string **commonName** utf8_string **organizationName** utf8_string **localityName** utf8_string **countryName** printable_string	I detta objekt anges egenskaper hos funktionen/personen/objektet, i certifikatstermer även kallad nyckelinnehavaren (subjektet). **serialNumber** Personens personnummer eller samordningsnummer enligt syntaxen YYYYMMDDNNNN. Från certifikatet som användes vid den förnyade autentiseringen. **givenName** Personens samtliga förnamn. Från certifikatet som användes vid den förnyade autentiseringen. **surName** Personens samtliga mellannamn och efternamn från certifikatet som användes vid den förnyade autentiseringen. **commonName** Fullständigt namn från certifikatet som användes vid den förnyade autentiseringen. **organizationName** Om bäraren finns i aktuell miljö för portalen • Namn på den utfärdande organisation i Portalen som bäraren tillhör baserat på SITHS eID som användes vid inloggning till Mina sidor. Hämtas då från konfigurationen för den utfärdande organisation som bäraren tillhör. Om bäraren **inte** finns i aktuell miljö för portalen	SITHS eID Portal

		• Namnet på den organisation som finns angivet i certifikatet som användes vid den förnyade autentiseringen. **localityName** Namnet på det län som finns angivet i certifikatet som användes vid den förnyade autentiseringen. *Rättegångsbalken 10 kap 1§: För bolag, förening eller annat samfund, stiftelse eller annan sådan inrättning gälle som hemvist den ort, där styrelsen har sitt säte eller, om säte för styrelsen ej är bestämt eller styrelse ej finnes, där förvaltningen föres. Lag samma vare i fråga om kommun eller annan sådan menighet.* **countryName** Landskoden som finns angivet i certifikatet som användes vid den förnyade autentiseringen.	

subjectPublicKeyInfo	**Algorithm**
	sequence\object_id
	subjectPublicKey
	sequence\bit_string\integer
		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. Värdet är någon av:
		• 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.
			Certifikatutfärdaren

cRLDistributionPoints	object\octet_string	[1] Adress till aktuell CRL-tjänst *(certificate revocation list)* Det finns en (1) tjänst som är nåbar över både Internet och Sjunet. Dessa delar samma URL och IP-adress. Vilket nät som används beror på lokal routing av nätverkstrafik och brandväggsöppningar.	Certifikatutfärdaren
authorityInformationAccess	object\octet_string	Innehåller: • [1] Adress till aktuell OCSP-tjänst *(online certificate status protocol)* • [2] AIA-länk till utfärdarens CA-certifikat *(authority information access)*. Vardera länk representerar en (1) tjänst som är nåbar över både Internet och Sjunet. Respektive tjänst delar samma URL och IP-adress. Vilket nät som används beror på lokal routing av nätverkstrafik och brandväggsöppningar.	Certifikatutfärdaren
certificatePolicies	object\octet_string	**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 certifikatutfärdaren. **policyQualifier** En per identifier [1,1] & [2,1], innehåller länkar som pekar på https://www.inera.se/siths/repository	Certifikatutfärdaren

enhancedKeyUsage	object\octet_string	**clientAuthentication** Certifikat med detta syfte kan användas för att identifiera en användare som anropar en server.	Certifikatutfärdaren
subjectKeyIdentifier	octet_string	**keyIdentifier** Obligatoriskt attribut som består av en SHA-1 HASH av en del av certifikatet publika nyckel.	Certifikatutfärdaren
authorityKeyIdentifier	octet_string	**keyIdentifier** Detta attribut innehåller subjectKeyIdentifier för den certifikatutfärdare som utfärdat certifikatet. Detta möjliggör att det kan finnas flera samtidigt gällande publika CA-nycklar.	Certifikatutfärdaren
keyUsage	bit_string	I detta attribut definieras hur den publika nyckel (och den privata) får användas. **digitalSignature + keyEncipherment** För användarens certifikat som används för Legitimering eller Legitimering för underskrift enl. referensarkitekturerna för identitet och åtkomst samt digital underskrift. Detta certifikat skapas alltid vid beställning av SITHS eID.	SITHS eID Portal i kombination av certifikatutfärdaren

Översikt – Hämtning av certifikatsinnehåll

* - Subject i certifikat för Mobilt SITHS bestäms genom ärvd legitimering. Innehållet blir alltså detsamma som i det certifikat/SITHS eID som användes vid den förnyade autentiseringen som användaren nyttjade vid hämtning av Mobilt SITHS på Mina sidor. Innehållet hämtas från det identitetsintyg som skapades av IdP:n vid den förnyade autentiseringen.