Revisionshistorik

Version	Datum	Kommentar
0.1	2019-01-07	Etablering av dokumentet
0.2	2019-01-28	Efter första genomgång av Cygate och SITHS PA
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	2020-01-16	Beslutad av SITHS PA. Rättning av URL för OCSP, samt korrigering av att e-post ej finns i certifikat för underskrift.
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 **(beskrivs i detta dokument)**
  - 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
    - 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 funktionsobjekt *(servrar, klienter och e-postkonton)*:

- Som finns i HSA med HSA-id *(ej obligatoriskt)*
- För servrar och e-postadresser krävs att namnet är formaterat som ett FQDN *(ex. www.inera.se el. no-reply@inera.se)*
- Vars namn och HSA-id prefix/internt funktions-id prefix är godkänt för organisationen genom domänvalidering

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 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 *”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 sökvägar 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 funktioner har inte ett tydligt regelverk när det kommer till tillitsnivåer. SITHS kommer ändå att tilldela funktionscertifikat olika O.I.D:er baserat på vilken rutin och process som användes vid utfärdandet av certifikatet.

O.I.D:er för funktionscertifikat återfinns på Matris för tolkning av tillitsnivåer

Funktionscertifikat för legitimering med HSA-id

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-512WithRSAEncryption (1.2.840.113549.1.1.13)		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 Function CA v1		CA	M	
validity		*<minst 1 dagar max 2 år>*	Exakt tid väljs i portalen av id-administratör			
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	Portal	M	
Subject						

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
emailAddress (1.2.840.113549.1.9.1)	255		test@siths.se	Portal	MIP[1]	
serialNumber (2.5.4.5)	64		SE5565594230-AAAA	Portal	M	
commonName (2.5.4.3)	64		test.siths.se	Portal	M	
organizationName (2.5.4.10)	64		Inera AB	Portal	M	
localityName (2.5.4.7)	128		Stockholm	Portal	M	
countryName (2.5.4.6)	2		SE	Portal	M	
subjectPublicKeyInfo						
Algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M	
subjectPublicKey		*Certifikatets publika nyckel, beräknad enligt angiven algoritm, 2048-4096 bitar lång baserat på nyckellängd i CSR.*		CA	M	
cRLDistributionPoints (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithseidfunctioncav1.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) Alternative Name: URL=http://ocsp1.siths.se		CA	M	

[1] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
		[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/sithseidfunctioncav1.cer				
subjectAltName (2.5.29.17)						
rfc822Name	255		test@siths.se	Portal	MIP[1]	
dNSName	255		test.siths.se	Portal	MIP[1]	
certificatePolicies (2.5.29.32)		[1] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository [2] Certificate Policy: Policy Identifier=SEE RIGHT --> [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. Kan också på sikt användas indikera olika typer av användningsområden för funktionscertifikat Ej i bruk ännu, men när behovet uppstår kommer det beskrivas i en matris på https://www.inera.se/siths/repository	CA	M	
enhancedKeyUsage					M	
serverAuthentication (1.3.6.1.5.5.7.3.1)				RA	M	
clientAuthentication (1.3.6.1.5.5.7.3.2)				RA	M	
emailProtection (1.3.6.1.5.5.7.3.4)				RA	MIP	
subjectKeyIdentifier (2.5.29.14)						

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
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 SHA512*		CA	M	

Funktionscertifikat för underskrift med HSA-id

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-512WithRSAEncryption (1.2.840.113549.1.1.13)		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 Function CA v1		CA	M	

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
validity		*<minst 1 dagar max 2 år>*	Exakt tid väljs i portalen av id-administratör			
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	Portal	M	
subject						
serialNumber (2.5.4.5)	64		SE5565594230-AAAA	Portal	M	
commonName (2.5.4.3)	64		test.siths.se	Portal	M	
organizationName (2.5.4.10)	64		Inera AB	Portal	M	
localityName (2.5.4.7)	128		Stockholm	Portal	M	
countryName (2.5.4.6)	2		SE	Portal	M	
subjectPublicKeyInfo						
algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M	
subjectPublicKey		*Certifikatets publika nyckel, beräknad enligt angiven algoritm, 2048-4096 bitar lång baserat på nyckellängd i CSR.*		CA	M	
cRLDistributionPoints (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithseidfunctioncav1.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) Alternative Name: URL=http://ocsp1.siths.se [2] Authority Info Access		CA	M	

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithseidfunctioncav1.cer				
certificatePolicies (2.5.29.32)		[1] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.inera.se/siths/repository [2] Certificate Policy: Policy Identifier=SEE RIGHT --> [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. Kan också på sikt användas indikera olika typer av användningsområden för funktionscertifikat Ej i bruk ännu, men när behovet uppstår kommer det beskrivas i en matris på https://www.inera.se/siths/repository	CA	M	
subjectKeyIdentifier (2.5.29.14)						
keyIdentifier		*<octet sträng> Byggs upp av en del 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)		nonRepudiation		CA	M	C
signature		*RSA-signatur över SHA512*		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 Function 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**	**notBefore** Certifikatutfärdaren **notAfter** SITHS eID Portal

		Här anges när certifikatet skall sluta gälla. detta kan idag väljas av administratören som beställer certifikatet i portalen i ett intervall från 1 dag till maximalt 2 år från den dag då certifikatet signeras av utfärdaren.	
Subject	**emailAddress** Anges som IA5_string **serialNumber** printable_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). **emailAddress** Finns endast i certifikat för legitimering **OCH** om typen av funktionsobjekt är e-post. Bestäms av namnet på funktionsobjektet i SITHS eID Portal **OBS!** För att emailAddress ska få finnas i Subject **SKALL** samma adress även finnas i attributet rfc822Name under SubjectAltName *(se RFC 5280)*. **serialNumber** Innehåller funktionsobjektets unika system-id i samma format som ett HSA-id. Hämtas från funktionsobjektets id i portalen som i sin tur kan populeras med hjälp av HSA. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation. **commonName** Innehåller funktionens namn, domännamn eller e-postadress. Hämtas från funktionsobjektets namn i portalen. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation. **organizationName** Detta attribut innehåller namnet på den domänägande organisationen *(server/e-post)* eller för den utfärdande organisationen *(klient)* i portalen som äger funktionsobjektet. Hämtas från den utfärdande organisation i portalen som funktionsobjektet har skapats under, men kan justeras för att stämma överens med valideringsreglerna. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation. Skall vara en juridisk organisation. **localityName** Detta attribut innehåller namnet på sätet *(den kommun där styrelsen finns registrerad)* för den domänägande organisationen *(server/e-post)* eller för den utfärdande organisationen *(klient)* i portalen som äger funktionsobjektet. Hämtas från den utfärdande organisation i portalen som funktionsobjektet har skapats under, men kan justeras för att stämma överens med valideringsreglerna.	SITHS eID Portal

		Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation. **countryName** Detta attribut innehåller landskod för den domänägande organisationen *(server/e-post)* eller för den utfärdande organisationen *(klient)* motsvarande det land som organisationen finns registrerad i. Hämtas från den utfärdande organisation i portalen som funktionsobjektet har skapats under, men kan justeras för att stämma överens med valideringsreglerna. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation.	
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 skall alltid vara rsaEncryption {1.2.840.113549.1.1.1}. **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 ”Organization validated” enligt CA Browser Forum Baseline requirements. **samt**	Certifikatutfärdaren

		[2] OID som reflekterar vilken utfärdanderutin som använts och även tillitsnivån för certifikatet. Sätts av certifikatsutfärdaren. **policyQualifier** En per identifier [1,1] & [2,1], innehåller länkar som pekar på https://www.inera.se/siths/repository	
enhancedKeyUsage	object\octet_string	Tilldelas alla certifikat för legitimering, innehåller en eller flera av nedanstående utökade syften. Används endast av certifikat för **legitimering** **clientAuthentication** Tilldelas till certifikat för funktionsobjekt av typen klient och server. Certifikat med detta syfte används för att identifiera en klient som anropar en server. **serverAuthentication** Tilldelas till certifikat för funktionsobjekt av typen server. Certifikat med detta syfte används för att identifiera server som identifierar sig mot en klient. **emailProtection** Tilldelas till certifikat för funktionsobjekt av typen e-post. Certifikat med detta syfte används för att signera och/eller kryptera e-postmeddelanden enl. S/MIME. Används primärt för Microsoft Outlook.	Certifikatutfärdaren
subjectAltName	octet_string	Tilldelas alla certifikat för legitimering, innehåller en av nedanstående utökade syften. Används endast av certifikat för **legitimering** **rfc822Name** Här anges funktionens e-postadress. Bestäms av namnet på funktionsobjektet i portalen. Tilldelas till certifikat för funktionsobjekt av typen e-post. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation. **dNSName** Här anges funktionens e-postadress. Bestäms av namnet på funktionsobjektet i portalen. Tilldelas till certifikat för funktionsobjekt av typen server. Kontrolleras mot regler i valideringsverktyget för respektive utfärdande organisation.	SITHS eID Portal

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** Om administratören väljer Legitimering när certifikatet beställs i portalen. **nonRepudiation** Om administratören väljer Underskrift när certifikatet beställs i portalen.	SITHS eID Portal i kombination av certifikatutfärdaren

Översikt – Hämtning av certifikatsinnehåll

[1] – Finns endast i legitimeringscertifikatet

[2] – Ej obligatorisk

[3] – Endast funktionsobjekt av typen e-post

[4] – Endast funktionsobjekt av typen server