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
1.0	2019-02-21	Fastställande av SITHS Policy Authority
1.1	2019-10-16	Beslutad av SITHS PA. Borttag av e-postadress från subject för underskriftscertifikat och övriga förtydliganden kopplat till detta. Förtydliganden kring åtkomst via Sjunet
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
    - SITHS e-id Person HSA-id ID 2 CA v1 **(beskrivs i detta dokument)**
    - SITHS e-id Person HSA-id ID 3 CA v1 **(beskrivs i detta dokument)**
- SITHS e-id Card Identifier CA v1
  - Certifikat för identifiering av smarta kort

För certifikaten som beskrivs i denna specifikation gäller:

- Utfärdas till personer som finns i HSA med HSA-id
- Utfärdas endast som legitimeringscertifikat vid ny utfärdande
- Underskriftscertifikat kan hämtas som tillägg via Mina sidor
- Vid uppdatering av ett SITHS eID som redan har underskriftscertifikat förnyas även underskriftscertifikatet.
- För personer som återfinns i svensk folkbokföring utfärdas till samma kort även legitimeringscertifikat som innehåller personnummer eller samordningsnummer som identifierare.

- För personer som saknas i svensk folkbokföring, så kallade ”CrossBorder”, hämtas endast certifikat med HSA-id
- Utfärdas på bärare med hårdvaruskydd av de privata nycklarna. T ex. smarta kort.

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 personer kan ha olika tillitsnivå (LoA=Level of Assurance). För SITHS eID 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. säkerhetskoder och upplåsningskoder som krävs för att använda e-legitimationen har skyddats under tillverkning och eventuell leverans till användaren.

Vilken tillitsnivå en viss O.I.D motsvarar presenteras i den matris som återfinns på Matris för tolkning av tillitsnivåer

Tillitsnivåer för SITHS eID baserar sig på tillitsramverket för Svensk e-legitimation.

Personcertifikat 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>*	016e179df72614af0dd4508e11f117	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 HSA-id 2 CA v1 ***ELLER*** SITHS e-id Person HSA-id 3 CA v1		CA	M	
validity		*<minst 1 dagar max 5 år>*	Ytterligare begränsningar kan komma av den portal som används			
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		rane.l.ramberg@test.rvn.se	Portal	MIP[1]	
serialNumber (2.5.4.5)	64		SE5565594230-ADDGS	Portal	M	
givenName (2.5.4.42)	64		Rane	Portal	MIP[1]	
surName (2.5.4.4)	64		Larsson Ramberg	Portal	M	
commonName (2.5.4.3)	64		Rane Larsson Ramberg	Portal	M	
organizationName (2.5.4.10)	64		Region Västernorrland	Portal	M	
localityName (2.5.4.7)	128		Västernorrlands län	Portal	MIP[1]	
countryName (2.5.4.6)	2		SE	CA	M	
cardNumber (1.2.752.34.2.1)		*CardNumber enligt svensk standard SS614331*	9752269875705018685	Portal	M	
subjectPublicKeyInfo						
Algorithm		rsaEncryption {1.2.840.113549.1.1.1}		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/sithseidpersonhsaid2cav1.crl ***ELLER***		CA	M	

[1] MIP – Mandatory if present

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
		URL=http://crl1.siths.se/sithseidpersonhsaid3cav1.crl				
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/sithseidpersonhsaid2cav1.cer ***ELLER*** URL=http://aia.siths.se/sithseidpersonhsaid3cav1.cer		CA	M	
subjectAltName (2.5.29.17)						
userPrincipalName (1.3.6.1.4.1.311.20.2.3)	255		rlrg@test.lvn.se	Portal	MIP[1]	
rfc822Name	255		rane.l.ramberg@test.lvn.se	Portal	MIP[1]	
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	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 beskriver detta återfinns på https://www.inera.se/siths/repository	CA	M	

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
		Qualifier: https://www.inera.se/siths/repository				
enhancedKeyUsage					O	
clientAuthentication (1.3.6.1.5.5.7.3.2)				CA		
smartCardLogon (1.3.6.1.4.1.311.20.2.2)				CA		
emailProtection (1.3.6.1.5.5.7.3.4)				CA		
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 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>*	016e179df72614af0dd4508e11f117	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 HSA-id 2 CA v1 ***ELLER*** SITHS e-id Person HSA-id 3 CA v1		CA	M	
validity		*<minst 1 dagar max 5 år>*	Ytterligare begränsningar kan komma av den portal som används			
notBefore	13		190601084459Z	CA	M	
notAfter	13		240601084459Z	Portal	M	
subject						
serialNumber (2.5.4.5)	64		SE5565594230-ADDGS	Portal	M	
givenName (2.5.4.42)	64		Rane	Portal	MIP[1]	
surName (2.5.4.4)	64		Larsson Ramberg	Portal	M	
commonName (2.5.4.3)	64		Rane Larsson Ramberg	Portal	M	
organizationName (2.5.4.10)	64		Region Västernorrland	Portal	M	

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
localityName (2.5.4.7)	128		Västernorrlands län	Portal	MIP[1]	
countryName (2.5.4.6)	2		SE	CA	M	
cardNumber (1.2.752.34.2.1)		*CardNumber enligt svensk standard SS614331*	9752269875705018685	Portal	M	
subjectPublicKeyInfo						
algorithm		rsaEncryption {1.2.840.113549.1.1.1}		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/sithseidpersonhsaid2cav1.crl ***ELLER*** URL=http://crl1.siths.se/sithseidpersonhsaid3cav1.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 Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithseidpersonhsaid2cav1.cer ***ELLER*** URL=http://aia.siths.se/sithseidpersonhsaid3cav1.cer		CA	M	

Attribut (O.I.D)	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical
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 beskriver detta återfinns på https://www.inera.se/siths/repository	CA	M	
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)		nonRepudiation		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 någon av ”SITHS e-id Person HSA-id 2 CA v1” eller ”SITHS e-id Person HSA-id 3 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 baseras på vilket flöde administratören följer vid beställning av SITHS eID och kan ibland vara valbart och ibland ett fördefinierat värde om max 5 år och **aldrig** längre än bärarens giltighetstid.	
Subject	**emailAddress** Anges som IA5_string **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). **emailAddress** Endast certifikat för **legitimering** Här anges personens e-postadress då en sådan förekommer i HSA-katalogen. För att emailAddress ska få finnas i Subject, **SKA** samma adress även finnas i attributet rfc822Name under SubjectAltName *(se RFC 5280)*. Hämtas ur attributet mail i HSA-katalogen. **serialNumber** Personens HSA-id. Hämtas ur HSA. **Obligatoriskt** **givenName** Personens samtliga förnamn. Hämtas från Personuppgiftstjänsten om förnamn finns i folkbokföringen. Om förnamn inte finns i folkbokföringen ersätts det med ”-”. Hämtas från HSA för personer som saknas i folkbokföringen. **surName** Personens samtliga mellannamn och efternamn. Hämtas från Personuppgiftstjänsten. Hämtas från HSA för personer som saknas i folkbokföringen. **Obligatoriskt**. **commonName** Personens tilltalsnamn, mellannamn och efternamn. Skapas av SITHS eID Portal utifrån information som hämtas från Personuppgiftstjänsten för personer som finns i folkbokföringen eller från HSA för personer som saknas i folkbokföringen. Om förnamn saknas utelämnas detta och ersätts inte av något annat tecken. **Obligatoriskt** **organizationName**	SITHS eID Portal

		Namn på den utfärdande organisationen. Hämtas från konfigurationen för den utfärdande organisation som den valda personposten tillhör. **Obligatoriskt**. **localityName** Namn på den ort som den utfärdande organisationen historiskt har inordnats under i HSAs katalogstruktur. Hämtas från konfigurationen för den utfärdande organisation som den valda personposten tillhör. *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** Detta attribut innehåller landskod för det land som utfärdande organisation finns registrerad i. Hämtas från konfigurationen för den utfärdande organisation som den valda personposten tillhör. **Obligatoriskt och värdet ska alltid vara SE**	
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)*.	Certifikatutfärdaren

		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.	
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	Tilldelas alla certifikat för legitimering. Används endast av certifikat för **legitimering** Följande tilldelas till samtliga certifikat: **clientAuthentication** **emailProtection** **smartCardLogon**	Certifikatutfärdaren
cardNumber	octet_string	**cardNumber** Innehåller kortets serienummer. CardNumber skall alltid finnas om ett kort är bärare av den/de privata nycklarna. Skapas av kortproduktionstjänsten som en del av tillverkningsprocessen.	SITHS eID Portal
subjectAltName	octet_string	Tilldelas certifikat för legitimering, innehåller ingen, en eller flera av nedanstående utökade syften. Används endast av certifikat för **legitimering** **rfc822Name** Här anges användarens e-postadress givet att hen har en sådan ifylld i attributet **mail** i HSA	SITHS eID Portal

		userPrincipalName Här anges användarens inloggningsnamn för Microsoft Active Directory förutsatt att hen har en sådan ifylld i attributet **userPrincipalName** i HSA	
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. **nonRepudiation** För användarens certifikat som används för legacyimplementationer för underskrift. Detta certifikat skapas endast om användare väljer att hämta det via Mina sidor eller vid uppdatering av ett SITHS eID där användaren redan har ett hämtat underskriftscertifikatet.	SITHS eID Portal i kombination av certifikatutfärdaren

Översikt – Hämtning av certifikatsinnehåll

* - Finns endast i legitimeringscertifikatet