inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Certifikatspecifikation för Sveriges kommuner och landsting med samarbetspartners

HCC

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

Innehållsförteckning

Revisionshistorik

Revisionshistorik finns sedan SITHS start, 2001-01-30. Mindre ändringar fram till denna version (3.04) redovisas i arkiverad ”HCC specifikation” (http://www.inera.se/siths/dokument/certifikat).

Version	Datum	Kommentar
1	2001-01-30	Första fastställda version. Beskriver minimiformatet för HCC.
2	2006-01-23	Andra fastställda version. Tabell över OID för ingående attribut tillagd. Attribut för epostadress i Subject ändrat till EmailAddress.
2.2	2007-03-05	Separering av certifikattyperna HCC Person/HCC Organisation och HCC Funktion. Ändring av DN i HCC Funktion för att följa specifikation för funktioner som återfinns i Service-trädet från HSA. Tillägg av EnhancedKeyUsage i HCC Funktion för att följa de facto-standard för servercertifikat.
2.3	2007-09-14	Tillägg av attribut för MS AD-inloggning i HCC Person för autentisering. Tillägg av attribut för säker e-post i samband med användning av *enhancedKeyUsage* (gäller särskilt MS Outlook).
2.31	2007-11-07	Separering av HCC Person och HCC Person för MS Windows.
2.34	2007-12-14	Tillägg av Enhanced Key Usage := emailProtection i HCC Funktion för att säkerställa att HCC Funktion går att använda för att ta emot krypterad e-post.
2.35	2010-02-17	Tillägg av att ”middelName” kompletteras till attributet surName.
3.02	2012-11-23	Tredje fastställda version. Modifiering av samtliga profiler för att passa ny CA-hierarki, borttagning av HCC Organisation, samt tillägg av HCC Funktion SHA512.
3.03	2014-06-18	Tillägg av obligatoriskt attribut, dNSName, i alla funktionscertifikat samt byte av dokumentmall
3.04	2014-10-01	Justering av stycket ”Kommentarer attribut för attribut” och borttag av användningen av organizationalUnit från samtliga certifikatspecifikationer. Rättning av att localityName inte ska finnas under mappningsöversikten.

Inledning

Detta dokument specificerar certifikat för Sveriges kommuner och landsting med samarbetspartners inom ramen för SITHS-modellen:

- HCC Person
- HCC Funktion

Observera att skilda katalogstrukturer i HSA-katalogen används för HCC Person och HCC Funktion, se dokumentation av HSA-katalogen.

HCC Funktion i denna specifikation skiljer sig från tidigare versioner genom att de helt inriktar sig på att lösa behovet för servers och applikationer. Behovet av HCC Funktion som certifikat för personer som innehar en viss funktion/roll inom en organisation täcks ej av denna specifikation.

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

HCC Person

HCC Person består av ett certifikat för legitimering (identifiering/autentisering) och ett certifikat för underskrift (signering/oavvislighet).

Översikt HCC Person för legitimering och kryptering

HCC Person för legitimering (identifiering/autentisering) och kryptering kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen:

		OID
Version		
SerialNumber		
SignatureAlgorithm		
Issuer		
	countryName	**2.5.4.6**
	organizationName	**2.5.4.10**
	commonName	**2.5.4.3**
Validity		
	notBefore	
	notAfter	
Subject		
	serialNumber	**2.5.4.5**
	emailAddress	**1.2.840.113549.1.9.1**
	title	**2.5.4.12**
	givenName	**2.5.4.42**
	surname	**2.5.4.4**
	commonName	**2.5.4.3**
	organizationName	**2.5.4.10**
	localityName	**2.5.4.7**
	countryName	**2.5.4.6**
subjectPublicKeyInfo		
	Algorithm	
	subjectPublicKey	
cardNumber		**1.2.752.34.2.1**
subjectDirectoryAttributes		**2.5.29.9**
	title	
cRLDistributionPoints		**2.5.29.31**
authorityInformationAccess		
	OCSP	**1.3.6.1.5.5.7.48.1**
	Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName		**2.5.29.17**
	userPrincipalName	**1.3.6.1.4.1.311.20.2.3**
	rfc822Name	
certificatePolicies		**2.5.29.32**
	policyIdentifer	
enhancedKeyUsage		
	clientAuthentication	**1.3.6.1.5.5.7.3.2**
	smartCardLogon	**1.3.6.1.4.1.311.20.2.2**
	emailProtection	**1.3.6.1.5.5.7.3.4**
subjectKeyIdentifier		**2.5.29.14**
	keyIdentifier	
authorityKeyIdentifier		**2.5.29.35**
	keyIdentifier	
keyUsage		**2.5.29.15**
	digital Signature, keyEncipherment	
Signature		

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

HCC Person för legitimering och kryptering - attribut för attribut

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

Tabell 1. HCC Person för legitimering och kryptering.

Attribut	*Antal förek.*	*Max-längd*	*Värde*	*Exempel*	*Källa*	*HSA*	*Optional/ Mandatory*	*Critical/ Non-critical*
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a1916838126543008963190214768545544 65740	CA		M	N/A
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 1 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		101108084459Z	CA		M	
subject								N/A
title*	1	64		Sjukskötare	RA	X	O	
emailAddress	1	255		rane.l.ramberg@test.lvn.se	RA	X	O	
serialNumber	1	64		SE5565968202-3PCH	RA	X	M	
givenName*	1	64		Rane	RA	X	M	
surName*	1	64		Larsson Ramberg	RA	X	M	
commonName	1	64		Rane Larsson Ramberg	RA	X	M	
organizationName*	1	64		Landstinget Västernorrland	RA	X	M	
localityName*	1	128		Västernorrlands län	RA	X	O	
countryName	1	2		SE	RA	X	M	
cardNumber	1		< CardNumber enligt svensk standard SS614331>	9752269875705018685	CA		M	NC
subjectDirectoryAttributes								NC
title	1			Sjukskötare	RA	X	M	
subjectPublicKeyInfo	1							N/A
algorithm	1		rsaEncryption {1.2.840.113549.1.1.1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cardNumber	1		< CardNumber enligt svensk standard SS614331>	9752269875705018685	CA		M	NC
subjectDirectoryAttributes								NC
title	1			Sjukskötare	RA	X	M	
cRLDistributionPoints	1		[[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithstype1cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet.org/sithstype1cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype1cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype1cav1.cer		CA		M	NC
subjectAltName			{OID= 2.5.29.17}					NC
userPrincipalName	1	255	{OID= 1.3.6.1.4.1.311.20.2.3}	rlrg@test.lvn.se	RA	X	O	
rfc822Name	1	255		rane.l.ramberg@test.lvn.se	RA	X	O	
certificatePolicies								NC
policyIdentifer	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	
enhancedKeyUsage								NC
clientAuthentication	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
smartCardLogon	1		{OID= 1.3.6.1.4.1.311.20.2.2}		CA		O	
emailProtection	1		{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
subjectKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
authorityKeyIdentifier **keyIdentifier**	1		<subjectKeyIdentifier för utfärdande CA>		CA		M	NC
keyUsage	1		digitalSignature, keyEncipherment		CA		M	C
Signature	1		<RSA-signatur över SHA1>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Översikt HCC Person för underskrift

HCC Person för underskrift (signering/oavvislighet) kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen:

	OID
Version	
SerialNumber	
SignatureAlgorithm	
Issuer	
countryName	**2.5.4.6**
organizationName	**2.5.4.10**
commonName	**2.5.4.3**
Validity	
notBefore	
notAfter	
Subject	
serialNumber	**2.5.4.5**
emailAddress	**1.2.840.113549.1.9.1**
title	**2.5.4.12**
givenName	**2.5.4.42**
surname	**2.5.4.4**
commonName	**2.5.4.3**
organizationName	**2.5.4.10**
localityName	**2.5.4.7**
countryName	**2.5.4.6**
subjectPublicKeyInfo	
Algorithm	
subjectPublicKey	
cardNumber	**1.2.752.34.2.1**
subjectDirectoryAttributes	**2.5.29.9**
title	
cRLDistributionPoints	**2.5.29.31**
authorityInformationAccess	
OCSP	**1.3.6.1.5.5.7.48.1**
Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName	**2.5.29.17**
rfc822Name	
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
keyUsage	**2.5.29.15**
nonRepudiation	
Signature	

inera
LANDSTING OCH REGIONER I SAMVERKAN FÖR E-HÄLSA

HCC Person för underskrift - attribut för attribut

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

Tabell 2. HCC Person för underskrift.

Attribut	*Antal förek.*	*Max-Längd*	*Värde*	*Exempel*	*Källa*	*HSA*	*Optional/ Mandatory*	*Critical/ Non-critical*
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA		M	N/A
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 1 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		101108084459Z	CA		M	
subject								N/A
title*	1	64		Sjukskötare	RA	X	O	
emailAddress	1	255		rane.l.ramberg@test.lvn.se	RA	X	O	
serialNumber	1	64		SE5565968202-3PCH	RA	X	M	
givenName*	1	64		Rane	RA	X	M	
surname*	1	64		Larsson Ramberg	RA	X	M	
commonName	1	64		Rane Larsson Ramberg	RA	X	M	
organizationName*	1	64		Landstinget Västernorrland	RA	X	M	
localityName*	1	128		Västernorrlands län	RA	X	O	
countryName	1	2		SE	RA	X	M	
subjectPublicKeyInfo	1							N/A
algorithm	1		rsaEncryption {1.2.840.113549.1.1.1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cardNumber	1		< CardNumber enligt svensk standard SS614331>	9752269875705018685	CA		M	NC
subjectDirectoryAttributes								NC
title	1			Sjukskötare	RA	X	M	
cRLDistributionPoints	1		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithstype1cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet.org/sithstype1cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype1cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype1cav1.cer		CA		M	NC
subjectAltName			{OID= 2.5.29.17}					NC
rfc822Name	1	255		rane.l.ramberg@test.lvn.se	RA	X	O	
certificatePolicies **policyIdentifer**	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	NC
subjectKeyIdentifier **keyIdentifier**	1		<octet string>		CA		M	NC
authorityKeyIdentifier **keyIdentifier**	1		<subjectKeyIdentifier för utfärdande CA>		CA		M	NC
keyUsage	1		Nonrepudiation		CA		M	C
Signature	1		<RSA-signatur över SHA1>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

HCC Funktion SHA1

Översikt HCC Funktion SHA1 för legitimering och kryptering

HCC Funktion SHA1 för legitimering (identifiering/autentisering) och kryptering kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen.

	OID
Version	
serialNumber	
signatureAlgorithm	
Issuer	
countryName	**2.5.4.6**
organizationName	**2.5.4.10**
commonName	**2.5.4.3**
Validity	
notBefore	
notAfter	
Subject	
serialNumber	**2.5.4.5**
emailAddress	**1.2.840.113549.1.9.1**
commonName	**2.5.4.3**
orgNo	**1.2.752.29.4.3**
organizationName	**2.5.4.10**
DC	**0.9.2342.19200300.100.1.25**
countryName	**2.5.4.6**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
cRLDistributionPoints	**2.5.29.31**
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
OCSP	**1.3.6.1.5.5.7.48.1**
Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName	**2.5.29.17**
Rfc822Name	
dNSName	
certificatePolicies	**2.5.29.32**
policyIdentifer	
enhancedKeyUsage	**2.5.29.37**
serverAuthentication	**1.3.6.1.5.5.7.3.1**
clientAuthentication	**1.3.6.1.5.5.7.3.2**
emailProtection	**1.3.6.1.5.5.7.3.4**
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
keyUsage	**2.5.29.15**
digital Signature, keyEncipherment	
Signature	

HCC Funktion SHA1 för legitimering och kryptering - attribut för attribut

Tabell 3. HCC Funktion (sha1) för legitimering och kryptering.

Attribut	Antal förek.	Max-Längd	Värde	Exempel	Källa	HSA	Optional/ Mandatory	Critical/ Non-critical
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA		M	N/A
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 2 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		071108084459Z	CA		M	
subject								N/A
serialNumber	1	64		SE5565594230-1000	RA	X	M	
emailAddress	1	255		testsiths@inera.se	RA	X	O	
commonName	1	64		test.siths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationName	1	64		Inera AB	RA	X	O	
DC	2	64		DC=Services, DC=Nod1	RA	X	O	
countryName	1	2		SE	RA	X	M	
subjectPublicKeyInfo	1							NC
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cRLDistributionPoints	1		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/siths type2cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet. org/sithstype2cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype2cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype2cav1.cer		CA		M	NC
subjectAltName								NC
rfc822Name	1	255		testsiths@inera.se	RA	X	O	
dNSName	1	255		test.siths.se	RA	X	M	
certificatePolicies								NC
policyIdentifer	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	
enhancedKeyUsage					CA		M	NC
clientAuthentication	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
serverAuthentication	1		{OID= 1.3.6.1.5.5.7.3.1}		CA		M	
emailProtection			{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
subjectKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
authorityKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
keyUsage			digitalSignature, keyEncipherment		CA		M	C
Signature	1		<RSA-signatur över SHA1>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

Översikt HCC Funktion SHA1 för underskrift

HCC Funktion för underskrift (signering/oavvislighet) kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen.

	OID
Version	
serialNumber	
signatureAlgorithm	
Issuer	
countryName	**2.5.4.6**
organizationName	**2.5.4.10**
commonName	**2.5.4.3**
Validity	
notBefore	
notAfter	
Subject	
serialNumber	**2.5.4.5**
emailAddress	**1.2.840.113549.1.9.1**
commonName	**2.5.4.3**
orgNo	**1.2.752.29.4.3**
organizationName	**2.5.4.10**
DC	**0.9.2342.19200300.100.1.25**
countryName	**2.5.4.6**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
cRLDistributionPoints	**2.5.29.31**
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
OCSP	**1.3.6.1.5.5.7.48.1**
Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName	**2.5.29.17**
Rfc822Name	
dNSName	
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
keyUsage	**2.5.29.15**
nonRepudiation	
Signature	

HCC Funktion SHA1 för underskrift - attribut för attribut

Tabell 4. HCC Funktion (sha1) för underskrift.

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optional/ Mandatory	Critical/ Non-critical
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA		M	N/A
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 2 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		071108084459Z	CA		M	
subject								N/A
serialNumber	1	64		SE5565594230-1000	RA	X	M	
emailAddress	1	255		testsiths@inera.se	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationName	1	64		Inera AB	RA	X	O	
DC	2	64		DC=Services, DC=Nod1	RA	X	O	
countryName	1	2		SE	RA	X	M	
subjectPublicKeyInfo	1							N/A
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cRLDistributionPoints	1		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithstype2cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet.org/sithstype2cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype2cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype2cav1.cer		CA		M	NC
subjectAltName								NC
rfc822Name	1	255		testsiths@inera.se	RA	X	O	
dNSName	1	255		test.siths.se	RA	X	M	
certificatePolicies								NC
policyIdentifer	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	
subjectKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
authorityKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
keyUsage	1		Nonrepudiation		CA		M	C
Signature	1		<RSA-signatur över SHA1>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

HCC Funktion SHA512

Översikt HCC Funktion SHA512 för legitimering och kryptering

HCC Funktion SHA512 för legitimering (identifiering/autentisering) och kryptering kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen.

	OID
Version	
serialNumber	
signatureAlgorithm	
Issuer	
countryName	**2.5.4.6**
organizationName	**2.5.4.10**
commonName	**2.5.4.3**
Validity	
notBefore	
notAfter	
Subject	
serialNumber	**2.5.4.5**
emailAddress	**1.2.840.113549.1.9.1**
commonName	**2.5.4.3**
orgNo	**1.2.752.29.4.3**
organizationName	**2.5.4.10**
DC	**0.9.2342.19200300.100.1.25**
countryName	**2.5.4.6**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
cRLDistributionPoints	**2.5.29.31**
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
OCSP	**1.3.6.1.5.5.7.48.1**
Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName	**2.5.29.17**
Rfc822Name **dNSName**	
certificatePolicies	**2.5.29.32**
policyIdentifer	
enhancedKeyUsage	**2.5.29.37**
serverAuthentication	**1.3.6.1.5.5.7.3.1**
clientAuthentication	**1.3.6.1.5.5.7.3.2**
emailProtection	**1.3.6.1.5.5.7.3.4**
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
keyUsage	**2.5.29.15**
digital Signature, keyEncipherment	
Signature	

HCC Funktion SHA512 för legitimering och kryptering - attribut för attribut

Tabell 5. HCC Funktion (sha2) för legitimering och kryptering.

Attribut	Antal förek.	Max-Längd	Värde	Exempel	Källa	HSA	Optional/ Mandatory	Critical/ Non-critical
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA		M	N/A
signatureAlgorithm	1		sha-512WithRSAEncryption {1.2.840.113549.1.1.13}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 3 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		071108084459Z	CA		M	
subject								N/A
serialNumber	1	64		SE5565594230-1000	RA	X	M	
emailAddress	1	255		testsiths@inera.se	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationName	1	64		Inera AB	RA	X	O	
DC	2	64		DC=Services, DC=Nod1	RA	X	O	
countryName	1	2		SE	RA	X	M	
subjectPublicKeyInfo	1							N/A
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cRLDistributionPoints	1		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithstype3cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet.org/sithstype3cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype3cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype3cav1.cer		CA		M	NC
subjectAltName								NC
rfc822Name	1	255		testsiths@inera.se	RA	X	O	
dNSName	1	255		test.siths.se	RA	X	M	
certificatePolicies								NC
policyIdentifer	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	
enhancedKeyUsage					CA		M	NC
clientAuthentication	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
serverAuthentication	1		{OID= 1.3.6.1.5.5.7.3.1}		CA		M	
emailProtection	1		{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
subjectKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
authorityKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
keyUsage	1		digitalSignature, keyEncipherment		CA		M	C
Signature	1		<RSA-signatur över SHA512>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

Översikt HCC Funktion SHA512 för underskrift

HCC Funktion SHA512för underskrift (signering/oavvislighet) kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen.

	OID
Version	
serialNumber	
signatureAlgorithm	
Issuer	
countryName	**2.5.4.6**
organizationName	**2.5.4.10**
commonName	**2.5.4.3**
Validity	
notBefore	
notAfter	
Subject	
serialNumber	**2.5.4.5**
emailAddress	**1.2.840.113549.1.9.1**
commonName	**2.5.4.3**
orgNo	**1.2.752.29.4.3**
organizationName	**2.5.4.10**
DC	**0.9.2342.19200300.100.1.25**
countryName	**2.5.4.6**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
cRLDistributionPoints	**2.5.29.31**
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
OCSP	**1.3.6.1.5.5.7.48.1**
Certification Authority Issuer	**1.3.6.1.5.5.7.48.2**
subjectAltName	**2.5.29.17**
Rfc822Name	
dNSName	
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
keyUsage	**2.5.29.15**
nonRepudiation	
Signature	

HCC Funktion SHA512 för underskrift - attribut för attribut

Tabell 6. HCC Funktion (sha2) för underskrift.

Attribut	Antal förek.	Max-Längd	Värde	Exempel	Källa	HSA	Optional/ Mandatory	Critical/ Non-critical
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA		M	N/A
signatureAlgorithm	1		sha-512WithRSAEncryption {1.2.840.113549.1.1.13}		CA		M	N/A
issuer								N/A
countryName	1	2	SE		CA		M	
organizationName*	1	64	Inera AB		CA		M	
commonName*	1	64	SITHS Type 3 CA v1		CA		M	
validity								N/A
notBefore	1	13		051108084459Z	CA		M	
notAfter	1	13		071108084459Z	CA		M	
subject								N/A
serialNumber	1	64		SE5565594230-1000	RA	X	M	
emailAddress	1	255		testsiths@inera.se	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationName	1	64		Inera AB	RA	X	O	
DC	2	64		DC=Services, DC=Nod1	RA	X	O	
countryName	1	2		SE	RA	X	M	
subjectPublicKeyInfo	1							N/A
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M	
subjectPublicKey	1		<bit string>		CA		M	
cRLDistributionPoints	1		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.siths.se/sithstype3cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.siths.sjunet.org/sithstype3cav1.crl		CA		M	NC

authorityInformationAccess	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=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.siths.sjunet.org [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.se/sithstype3cav1.cer [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.siths.sjunet.org/sithstype3cav1.cer		CA		M	NC
subjectAltName								NC
rfc822Name	1	255		testsiths@inera.se	RA	X	O	
dNSName	1	255		test.siths.se	RA	X	M	
certificatePolicies								NC
policyIdentifer	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html		CA		M	
subjectKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
authorityKeyIdentifier								NC
keyIdentifier	1		<octet string>		CA		M	
keyUsage	1		Nonrepudiation		CA		M	C
Signature	1		<RSA-signatur över SHA512>		CA		M	N/A

* - Attribut som nyttjar UTF8-encoding

Kommentarer attribut för attribut

Version

Anger version av X.509 certifikatstandard.

serialNumber

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

signatureAlgorithm

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

Issuer

I detta attribut anges utfärdarens identitet.

countryName

Detta attribut skall alltid vara “SE” och anger att certifikatsutfärdaren är en organisation registrerad i Sverige. Sätts av certifikatsutfärdaren. Del av Issuer.

organizationName

Detta attribut innehåller namnet på certifikatsutfärdaren. Sätts av certifikatsutfärdaren. Del av Issuer. Anges som UTF8-string.

commonName

Sätts av certifikatsutfärdaren. Del av Issuer. Anges som UTF8-string.

Validity

Detta attribut 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 till notAfter i primärcertifikatet eller till utfärdardagen plus fem år.

Tidpunkterna kodas som ”UTCTime”.

Subject

I detta attribut anges egenskaper hos nyckelinnehavaren.

countryName

Detta attribut skall alltid vara “SE” och anger att nyckelinnehavaren är en organisation eller person registrerad i Sverige. Sätts av certifikatsutfärdaren. Del av Subject. Hämtas ur HSA.

localityName

Detta attribut innehåller namn på län i klartext. Namnet hämtas från objektklassen Locality. Förteckning över namn på län fastställs och tillhandahålls av Inera. Del av Subject. Hämtas ur HSA.

DC, domainComponent,

används endast i HCC Funktion. Används för att ange del av sökväg i Services-trädet där HCC Funktion normalt lagras. Del av Subject. Hämtas ur HSA.

orgNo

används endast i HCC Funktion. Detta attribut innehåller organisationsnummer för organisation som innehar HCC Funktion. Detta attribut skall matcha det registrerade organisationsnumret för respektive organisation. Del av Subject. Hämtas ur HSA.

organizationName

Detta attribut innehåller namn på huvudman eller motsvarande. Skall vara en juridisk person med organisationsnummer. Namnet hämtas av RA-klienten från motsvarande attribut i respektive objektklass: organizationalPerson för Person HCC, organizationalRole för Funktion HCC. Del av Subject. Hämtas ur HSA.

commonName

Namnet hämtas av RA-klienten från motsvarande attribut i objektklassen organizationalPerson i HSA-katalogen, som normalt är givenName följt av surName.

För Funktion HCC används commonName i objektklassen organizationalRole**.**

Del av Subject. Hämtas ur HSA.

surName

Attributet surName förekommer endast i Person HCC. Namnet hämtas av RA-klienten från HSA-katalogen. I de fall en person har ett mellannamn (middleName i HSA) används även det i SurName i HCC. HCC SurName = HSAmiddlename+HSAsurname. Del av Subject. Hämtas ur HSA.

givenName

Attributet givenName förekommer endast i Person HCC. Namnet hämtas av RA-klienten från HSA-katalogen. Del av Subject. Hämtas ur HSA.

title

Detta attribut förekommer endast i Person HCC. Innehållet är ett fritextfält. Namnet hämtas av RA-klienten från HSA-katalogen. Del av Subject. Hämtas ur HSA.

serialNumber

Detta attribut hämtas av RA-klienten från HSA-id och följer gällande riktlinjer för HSA-id. Del av Subject. Hämtas ur HSA.

emailAddress

Här anges objektet eller personens e-postadress då en sådan förekommer i HSA-katalogen. **OBS!** För att *emailAddress* ska få finnas i Subject, SKALL samma adress även finnas i attributet *rfc822Name* under *SubjectAltName* (se även RFC 3280). Hämtas ur attributet *mail i* HSA-katalogen.

subjectPublicKeyInfo

Detta attribut innehåller två attribut som definierar den publika nyckeln i detta certifikat:

Algorithm
En identifierare som 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}. Sätts av certifikatsutfärdaren.

subjectPublicKey
Detta attribut ar en bitsträng som innehåller den publika nyckeln. Genereras av certifikatsutfärdaren.

cardNumber
Innehåller aktuellt korts serienummer. CardNumber skall alltid finnas om ett kort är bärare av den/de privata nycklarna. Hämtas ur kortets tillhörande e-legitimation alternativt ur aktuellt korts transportcertifikat.

subjectDirectoryAttributes

title
I detta attribut skall den legitimerade yrkesrollen kunna anges. Hämtas ur HSA.

cRLDistributionPoints
Identifierar platserna där spärrlistan lagras. Två platser finns, en på Internet och en på Sjunet.

authorityInformationAccess
Innehåller adress till aktuell OCSP-tjänst (online certificate status protocol) samt länkar som leder till utfärdarens CA-certifikat.

subjectAltName,

rfc822Name
Här anges epostadress som SMTP-adress. Observera att detta attribut SKALL finnas i HCC om attributet *emailAddress* är använt i *Subject.* Hämtas ur HSA.

userPrincipalName

Detta attribut används då HCC ska användas för inloggning mot MS Active Directory (Windows Server 2000/2003/2008). Attributet userPrincipalName hämtas ur HSA-katalogen.

dNSName

Används för HCC Funktion och anger DNS-namnet till aktuell funktion. Hämtas från HSA av RA-klienten och består av attributet *commonName* för objekt av objektklassen *organizationalRole.* Observera att detta attribut SKALL finnas i samtliga HCC Funktion som har *enhancedKeyUsage=serverAuthentication.*

certificatePolicies

policyIdentifer
Här anges OID för issuance policy för aktuellt certifikatpolicy samt en länk till SITHS Relying Party Agreement. Reflekterar tillitsnivån av certifikatet. Sätts av certifikatsutfärdaren.

enhancedKeyUsage
Tilldelas samtliga HCC för legitimering, innehåller alltid något eller flera av nedanstående utökade syften.
HCC för signering använder inte attributet *enhancedKeyUsage***.**

serverAuthentication

Certifikat med syfte kan användas som identifiering av en server som tar emot anrop av en klient (användare/annat system). Tilldelas samtliga HCC Funktion för legitimering.

clientAuthentication

Certifikat med detta syfte kan användas för att identifiera en användare eller ett klientsystem som anropar en server. Detta syfte kan tilldelas till:

- HCC Funktion för legitimering
- HCC Person för legitimering.

emailProtection

Certifikat med detta syfte kan användas för säker e-post. Detta syfte krävs för att det ska vara möjligt att kryptera och signera e-post i de fall e-postsystemet kräver förekomst av detta syfte i certifikatet (gäller speciellt MS Exchange/Outlook).

OBS! Detta värde tilldelas endast under **förutsättning** att objektet har fältet *mail* ifyllt i HSA-katalogen. Informationen i fältet *mail* måste även finnas som *rfc822Name* under *subjectAltName* och som *emailAddress* under *Subject*
Detta syfte kan tilldelas till:

- HCC Funktion för legitimering
- HCC Person för legitimering.

smartcardLogon

Certifikat med detta syfte används för att möjliggöra inloggning till MS Windows/Active Directory. Detta syfte tilldelas samtliga HCC Person för legitimering.

subjectKeyIdentifier

keyIdentifier
Detta attribut skall ingå i HCC certifikat och utgör ett sätt att avgöra om en viss publik nyckel har använts i certifikatet. För mera information hänvisas till RFC3280.

authorityKeyIdentifier

keyIdentifier
Detta attribut innehåller en identifierare som pekar ut den publika nyckel som certifikatsutfärden har använt vid signering av certifikatet. Detta möjliggör att det kan finnas flera samtidigt gällande publika CA-nycklar. Identifieraren genereras från den publika nyckeln på sådant sätt att identifieraren blir unik, vanligtvis genom en hash algoritm.

keyUsage
I detta attribut definieras hur den publika nyckel (och den privata) får användas. Detta fält kan ha två olika värden:
a) *digitalSignature + keyEncipherment*
b) nonRepudiation

digitalSignature
anger att nyckeln används för att verifiera autentiseringsdata, till exempel vid inloggning.

keyEncipherment
anger att nyckeln används för kryptering/dekryptering, till exempel vid nyckelutbyte.

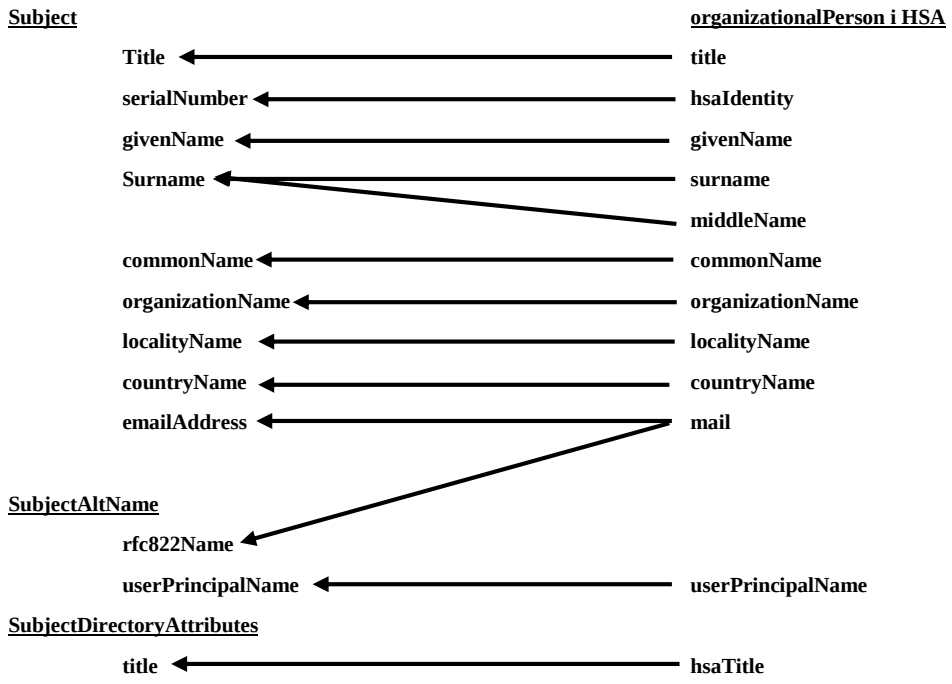
nonRepudiation
anger att nyckeln används för att verifiera elektroniska signaturer.

Vid begäran om ett HCC Person utfärdas två certifikat, ett med *keyUsage = digitalSignature + keyEncipherment*, detta certifikat kan således användas både för autentisering och kryptering/dekryptering, och ett med *keyUsage = nonRepudiation*, detta certifikat kan bara användas för elektroniska signaturer.

Vid begäran av HCC Funktion kan man välja för vilket ändamål certifikatet ska användas,
keyUsage = digitalSignature + keyEncipherment alternativt *keyUsage = nonRepudiation.*

Översikt mappning av certifikatinnehållet och HSA-innehåll

HCC Person



HCC Funktion