



# Certifikatspecifikation för Sveriges kommuner och landsting med samarbetspartners

## HCC



## Innehållsförteckning

<b>Tabellförteckning</b> .....	<b>3</b>
<b>Revisionshistorik</b> .....	<b>3</b>
<b>Inledning</b> .....	<b>4</b>
<b>HCC Person</b> .....	<b>5</b>
Översikt HCC Person för legitimering och kryptering.....	5
HCC Person för legitimering och kryptering - attribut för attribut .....	6
Översikt HCC Person för underskrift .....	8
HCC Person för underskrift - attribut för attribut.....	9
<b>HCC Funktion SHA1</b> .....	<b>11</b>
Översikt HCC Funktion SHA1 för legitimering och kryptering.....	11
HCC Funktion SHA1 för legitimering och kryptering - attribut för attribut .....	12
Översikt HCC Funktion SHA1 för underskrift .....	14
HCC Funktion SHA1 för underskrift - attribut för attribut.....	15
<b>HCC Funktion SHA512</b> .....	<b>17</b>
Översikt HCC Funktion SHA512 för legitimering och kryptering.....	17
HCC Funktion SHA512 för legitimering och kryptering - attribut för attribut .....	18
Översikt HCC Funktion SHA512 för underskrift .....	20
HCC Funktion SHA512 för underskrift - attribut för attribut.....	21
<b>Kommentarer attribut för attribut</b> .....	<b>23</b>
<b>Översikt mappning av certifikatinnehållet och HSA-innehåll</b> .....	<b>27</b>
HCC Person.....	27
HCC Funktion .....	27



## Tabellförteckning

### Revisionshistorik

Revisionshistorik finns sedan SITHS start, 2001-01-30. Mindre ändringar fram till denna version (3.0) redovisas i arkiverad ”HCC specifikation” (<http://www.inera.se/infrastrukturtjanster/siths/dokument-for-siths/rootcertifikat-siths-ca/>).

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 <i>enhancedKeyUsage</i> (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 ”middleName” 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.



## 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). Både HCC Person för legitimering och för underskrift finns numera endast i en variant var.

## 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:

	<u>OID</u>
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
organizationalUnitName	2.5.4.11
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
policyIdentifier	
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	



## 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 förekom.	Max- längd	Värde	Exempel	Källa	HSA	Optional/ Mandatory	Critical/ Non-critical
version	1	1	2		CA		M	N/A
serialNumber	1	64		00d9b4778ba5ed51e811f2a664a793ae3a191683812654300896319021476854554465740	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		101108084459Z021117175720Z	CA		M	
subject								N/A
title*	1	64		Sjukskötare	RA	X	O	
emailAddress	1	255		<a href="mailto:rane.l.ramberg@test.lvn.se">rane.l.ramberg@test.lvn.se</a>	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	
organizationalUnitName*	10	64		Länssjukhuset Sundsvall	RA	X	O	
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://cr1.siths.se/sithstype1cav1.cr1 [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://cr2.siths.sjunet.org/sithstype1cav1.cr1		CA		M	NC



<b>authorityInformationAccess</b>	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
<b>subjectAltName</b>			{OID= 2.5.29.17}					NC
<b>userPrincipalName</b>	1	255	{OID= 1.3.6.1.4.1.311.20.2.3}	<a href="mailto:r1rg@test.lvn.se">r1rg@test.lvn.se</a>	RA	X	O	
<b>rfc822Name</b>	1	255		<a href="mailto:rane.l.ramberg@test.lvn.se">rane.l.ramberg@test.lvn.se</a>	RA	X	O	
<b>certificatePolicies</b>								NC
<b>policyIdentifier</b>	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.html</a>		CA		M	
<b>enhancedKeyUsage</b>								NC
<b>clientAuthentication</b>	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
<b>smartCardLogon</b>	1		{OID= 1.3.6.1.4.1.311.20.2.2}		CA		O	
<b>emailProtection</b>	1		{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
<b>subjectKeyIdentifier</b>								NC
<b>keyIdentifier</b>	1		<octet string>		CA		M	
<b>authorityKeyIdentifier</b>								NC
<b>keyIdentifier</b>	1		<subjectKeyIdentifier för utfärdande CA>		CA		M	
<b>keyUsage</b>	1		digitalSignature, keyEncipherment		CA		M	C
<b>Signature</b>	1		<RSA-signatur över SHA1>		CA		M	N/A

\* - Attribut som nyttjar UTF8-encoding



## 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:

	<u>OID</u>
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
organizationalUnitName	2.5.4.11
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
policyIdentifier	
subjectKeyIdentifier	2.5.29.14
keyIdentifier	
authorityKeyIdentifier	2.5.29.35
keyIdentifier	
keyUsage	2.5.29.15
nonRepudiation	
Signature	





## 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 förekomster	Maxlängd	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		<a href="mailto:rane.l.ramberg@test.lvn.se">rane.l.ramberg@test.lvn.se</a>	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	
organizationalUnitName*	10	64		Länssjukhuset Sundsvall	RA	X	O	
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://cr1.siths.se/sithstyp1cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://cr2.siths.sjunet.org/sithstyp1cav1.crl		CA		M	NC



<b>authorityInformationAccess</b>	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
<b>subjectAltName</b>			{OID= 2.5.29.17}				NC
<b>rfc822Name</b>	1	255		<a href="mailto:rane.l.ramberg@test.lvn.se">rane.l.ramberg@test.lvn.se</a>	RA	X	O
<b>certificatePolicies</b> <b>policyIdentifier</b>	1		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.html</a>	CA		M	NC
<b>subjectKeyIdentifier</b> <b>keyIdentifier</b>	1		<octet string>	CA		M	NC
<b>authorityKeyIdentifier</b> <b>keyIdentifier</b>	1		<subjectKeyIdentifier för utfärdande CA>	CA		M	NC
<b>keyUsage</b>	1		Nonrepudiation	CA		M	C
<b>Signature</b>	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.

	<u>OID</u>
<b>Version</b>	
serialNumber	
signatureAlgorithm	
<b>Issuer</b>	
countryName	2.5.4.6
organizationName	2.5.4.10
commonName	2.5.4.3
<b>Validity</b>	
notBefore	
notAfter	
<b>Subject</b>	
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
organizationalUnitName	2.5.4.11
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	
certificatePolicies	2.5.29.32
policyIdentifier	
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	
<b>Signature</b>	



## 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		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationalUnitName	10	64		webbservers	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				CA		M	NC
			[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					



<b>authorityInformationAccess</b>	1		<p>[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</p> <p>[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.sjune t.org</p> <p>[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/sithst ype2cav1.cer</p> <p>[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.o rg/sithstype2cav1.cer</p>		CA		M	NC
<b>subjectAltName</b> rfc822Name	1	255		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	NC
<b>certificatePolicies</b>								NC
<b>policyIdentifier</b>	1		<p>[1]Certificate Policy: Policy Identifier=&lt;ISSUANCE POLICY OID&gt; [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.ht ml</a></p>		CA		M	
<b>enhancedKeyUsage</b>					CA		M	NC
<b>clientAuthentication</b>	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
<b>serverAuthentication</b>	1		{OID= 1.3.6.1.5.5.7.3.1}		CA		M	
<b>emailProtection</b>			{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
<b>subjectKeyIdentifier</b> keyIdentifier	1		<octet string>		CA		M	NC
<b>authorityKeyIdentifier</b> keyIdentifier	1		<octet string>		CA		M	NC
<b>keyUsage</b>			digitalSignature, keyEncipherment		CA		M	C
<b>Signature</b>	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.

	<u>OID</u>
<b>Version</b>	
<b>serialNumber</b>	
<b>signatureAlgorithm</b>	
<b>Issuer</b>	
countryName	2.5.4.6
organizationName	2.5.4.10
commonName	2.5.4.3
<b>Validity</b>	
notBefore	
notAfter	
<b>Subject</b>	
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
organizationalUnitName	2.5.4.11
organizationName	2.5.4.10
DC	0.9.2342.19200300.100.1.25
countryName	2.5.4.6
<b>subjectPublicKeyInfo</b>	
algorithm =RSA Encryption	1.2.840.113549.1.1.1
subjectPublicKey	
<b>cRLDistributionPoints</b>	2.5.29.31
<b>authorityInformationAccess</b>	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
<b>subjectAltName</b>	2.5.29.17
Rfc822Name	
<b>certificatePolicies</b>	2.5.29.32
policyIdentifier	
<b>subjectKeyIdentifier</b>	2.5.29.14
keyIdentifier	
<b>authorityKeyIdentifier</b>	2.5.29.35
keyIdentifier	
<b>keyUsage</b>	2.5.29.15
nonRepudiation	
<b>Signature</b>	



## HCC Funktion SHA1 för underskrift - attribut för attribut

Tabell 4. HCC Funktion (sha1) för underskrift.

Attribut	Antal förekr.	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		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationalUnitName	10	64		webbservers	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://cr11.siths.se/sithstype2cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://cr12.siths.sjunet.org/sithstyp2cav1.crl		CA		M	NC



<b>authorityInformationAccess</b>	1		<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=<a href="http://ocsp1.siths.se">http://ocsp1.siths.se</a></p> <p>[2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=<a href="http://ocsp2.siths.sjunet.org">http://ocsp2.siths.sjunet.org</a></p> <p>[3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<a href="http://aia.siths.se/sithstype2cav1.cer">http://aia.siths.se/sithstype2cav1.cer</a></p> <p>[4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<a href="http://aia.siths.sjunet.org/sithstyp e2cav1.cer">http://aia.siths.sjunet.org/sithstyp e2cav1.cer</a></p>		CA		M	NC
<b>subjectAltName</b> <b>rfc822Name</b>	1	255		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	NC
<b>certificatePolicies</b> <b>policyIdentifier</b>	1		<p>[1]Certificate Policy: Policy Identifier=&lt;ISSUANCE POLICY OID&gt; [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.html</a></p>		CA		M	NC
<b>subjectKeyIdentifier</b>								NC
<b>keyIdentifier</b>	1		<octet string>		CA		M	
<b>authorityKeyIdentifier</b> <b>keyIdentifier</b>	1		<octet string>		CA		M	NC
<b>keyUsage</b>	1		Nonrepudiation		CA		M	C
<b>Signature</b>	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.

	<u>OID</u>
<b>Version</b>	
serialNumber	
signatureAlgorithm	
<b>Issuer</b>	
countryName	2.5.4.6
organizationName	2.5.4.10
commonName	2.5.4.3
<b>Validity</b>	
notBefore	
notAfter	
<b>Subject</b>	
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
organizationalUnitName	2.5.4.11
organizationName	2.5.4.10
DC	0.9.2342.19200300.100.1.25
countryName	2.5.4.6
<b>subjectPublicKeyInfo</b>	
algorithm =RSA Encryption	1.2.840.113549.1.1.1
subjectPublicKey	
<b>cRLDistributionPoints</b>	2.5.29.31
<b>authorityInformationAccess</b>	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
<b>subjectAltName</b>	2.5.29.17
Rfc822Name	
<b>certificatePolicies</b>	2.5.29.32
policyIdentifier	
<b>enhancedKeyUsage</b>	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
<b>subjectKeyIdentifier</b>	2.5.29.14
keyIdentifier	
<b>authorityKeyIdentifier</b>	2.5.29.35
keyIdentifier	
<b>keyUsage</b>	2.5.29.15
digital Signature, keyEncipherment	
<b>Signature</b>	



## HCC Funktion SHA512 för legitimering och kryptering - attribut för attribut

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

Attribut	Antal förekommer	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		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationalUnitName	10	64		webbservers	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://cr1.siths.se/sithstype3cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://cr2.siths.sjunet.org/sithstype3cav1.crl		CA		M	NC



<b>authorityInformationAccess</b>	1		[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= <a href="http://ocsp1.siths.se">http://ocsp1.siths.se</a> [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:  URL= <a href="http://ocsp2.siths.sjunet.org">http://ocsp2.siths.sjunet.org</a> [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL= <a href="http://aia.siths.se/sithstype3cav1.cer">http://aia.siths.se/sithstype3cav1.cer</a> [4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL= <a href="http://aia.siths.sjunet.org/sithstyp e3cav1.cer">http://aia.siths.sjunet.org/sithstyp e3cav1.cer</a>	CA		M	NC	
<b>subjectAltName</b>							NC	
<b>rfc822Name</b>	1	255		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	NC
<b>certificatePolicies</b>								NC
<b>policyIdentifier</b>	1		[1]Certificate Policy: Policy Identifier= <ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.html</a>	CA		M		
<b>enhancedKeyUsage</b>					CA		M	NC
<b>clientAuthentication</b>	1		{OID= 1.3.6.1.5.5.7.3.2}		CA		M	
<b>serverAuthentication</b>	1		{OID= 1.3.6.1.5.5.7.3.1}		CA		M	
<b>emailProtection</b>	1		{OID= 1.3.6.1.5.5.7.3.4}		CA		O	
<b>subjectKeyIdentifier</b>								NC
<b>keyIdentifier</b>	1		<octet string>		CA		M	
<b>authorityKeyIdentifier</b>								NC
<b>keyIdentifier</b>	1		<octet string>		CA		M	
<b>keyUsage</b>	1		digitalSignature, keyEncipherment		CA		M	C
<b>Signature</b>	1		<RSA-signatur över SHA512>		CA		M	N/A

\* - Attribut som nyttjar UTF8-encoding



## Översikt HCC Funktion SHA512 för underskrift

HCC Funktion SHA512 för underskrift (signering/oavvislighet) kan ha följande innehåll. Objektidentifierare (OID) för utvalda attribut framgår av den högra kolumnen.

	<u>OID</u>
<b>Version</b>	
<b>serialNumber</b>	
<b>signatureAlgorithm</b>	
<b>Issuer</b>	
countryName	2.5.4.6
organizationName	2.5.4.10
commonName	2.5.4.3
<b>Validity</b>	
notBefore	
notAfter	
<b>Subject</b>	
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
organizationalUnitName	2.5.4.11
organizationName	2.5.4.10
DC	0.9.2342.19200300.100.1.25
countryName	2.5.4.6
<b>subjectPublicKeyInfo</b>	
algorithm =RSA Encryption	1.2.840.113549.1.1.1
subjectPublicKey	
<b>cRLDistributionPoints</b>	2.5.29.31
<b>authorityInformationAccess</b>	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
<b>subjectAltName</b>	2.5.29.17
Rfc822Name	
<b>certificatePolicies</b>	2.5.29.32
policyIdentifier	
<b>subjectKeyIdentifier</b>	2.5.29.14
keyIdentifier	
<b>authorityKeyIdentifier</b>	2.5.29.35
keyIdentifier	
<b>keyUsage</b>	2.5.29.15
nonRepudiation	
<b>Signature</b>	



## 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		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	
commonName	1	64		www.testsiths.se	RA	X	M	
orgNo	1	12		556559-4230	RA	X	O	
organizationalUnitName	10	64		webbservers	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://cr1.siths.se/sithstype3cav1.crl [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://cr2.siths.sjunet.org/sithstype3cav1.crl		CA		M	NC



<b>authorityInformationAccess</b>	1		<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=<a href="http://ocsp1.siths.se">http://ocsp1.siths.se</a></p> <p>[2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=<a href="http://ocsp2.siths.sjunet.org">http://ocsp2.siths.sjunet.org</a></p> <p>[3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<a href="http://aia.siths.se/sithstype3cav1.cer">http://aia.siths.se/sithstype3cav1.cer</a></p> <p>[4]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<a href="http://aia.siths.sjunet.org/sithstype3cav1.cer">http://aia.siths.sjunet.org/sithstype3cav1.cer</a></p>		CA		M	NC
<b>subjectAltName</b> rfc822Name	1	255		<a href="mailto:testsiths@inera.se">testsiths@inera.se</a>	RA	X	O	NC
<b>certificatePolicies</b>								NC
<b>policyIdentifier</b>	1		<p>[1]Certificate Policy: Policy Identifier=&lt;ISSUANCE POLICY OID&gt; [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://rpa.siths.se/sithsrpav1.html">http://rpa.siths.se/sithsrpav1.html</a></p>		CA		M	
<b>subjectKeyIdentifier</b> keyIdentifier	1		<octet string>		CA		M	NC
<b>authorityKeyIdentifier</b> keyIdentifier	1		<octet string>		CA		M	NC
<b>keyUsage</b>	1		Nonrepudiation		CA		M	C
<b>Signature</b>	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 certifikatsutfärdaren till *notAfter* i primärcertifikatet eller till 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 objektlassen Locality. Förteckning över namn på län fästställs 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**

Detta attribut innehåller organisationsnummer för organisations som innehar HCC Funktion. Detta attribut skall matcha det registrerade organisationsnumret hos bolagsverket 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 objektclass: Organizational Person för Person HCC, Organizational Role för Funktion HCC. Del av Subject. Hämtas ur HSA.

#### **organizationalUnitName**

Detta attribut innehåller namn på organisatorisk enhet. Upp till 10 nivåer. Namnet hämtas av RA-klienten från HSA-katalogen. Namnet hämtas från objektclassen Organizational Person om detta är ett Person HCC. För Funktion HCC används motsvarande attribut i objektclassen Organizational Role. Del av Subject. Hämtas ur HSA.

#### **commonName**

Namnet hämtas av RA-klienten från motsvarande attribut i objektclassen Organizational Person i HSA-katalogen, som normalt är givenName följt av surName. För Funktion HCC används commonName i objektclassen Organizational Role. Del av Subject. Hämtas ur HSA.

#### **surName**

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

#### **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 epostadress, om detta önskas i *Subject*. Observera att om emailAddress finns i Subject, SKALL attributet RFC822Name återfinnas i *SubjectAltName* (se även RFC 3280). Del av Subject. Hämtas ur HSA.

#### **subjectPublicKeyInfo**

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





### Algorithm

En identifierare som anger vilken algoritm som skall användas 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 är en bitsträng som innehåller den publika nyckeln. Genereras av certifikatsutfärdaren.

### authorityKeyIdentifier, keyIdentifier

Detta attribut innehåller en identifierare som pekar ut den publika nyckel som certifikatsutfärdaren 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.

### 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.

### 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 autenticeringsdata, 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 autenticering 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*.

### enhancedKeyUsage

De bägge värdena *serverAuthentication*, *clientAuthentication* anger att HCC Funktion kan användas både för att agera server och klient i säkra uppkopplingar mellan klient-server eller server-server. Kan ej användas ihop med *keyUsage := nonRepudiation*.

*enhancedKeyUsage* används även för att möjliggöra inloggning till MS Windows/Active Directory med HCC Person med värdet *smartCardLogon*.

*emailProtection* anger att ett HCC Person kan användas för säker e-post. Detta attribut krävs för att det ska vara möjligt att kryptera och signera e-post då *enhancedKeyUsage* använts i certifikatet (gäller speciellt MS Exchange/Outlook).

### certificatePolicies, policyIdentifier

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

**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.

**subjectDirectoryAttributes, title**

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

**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.

**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.

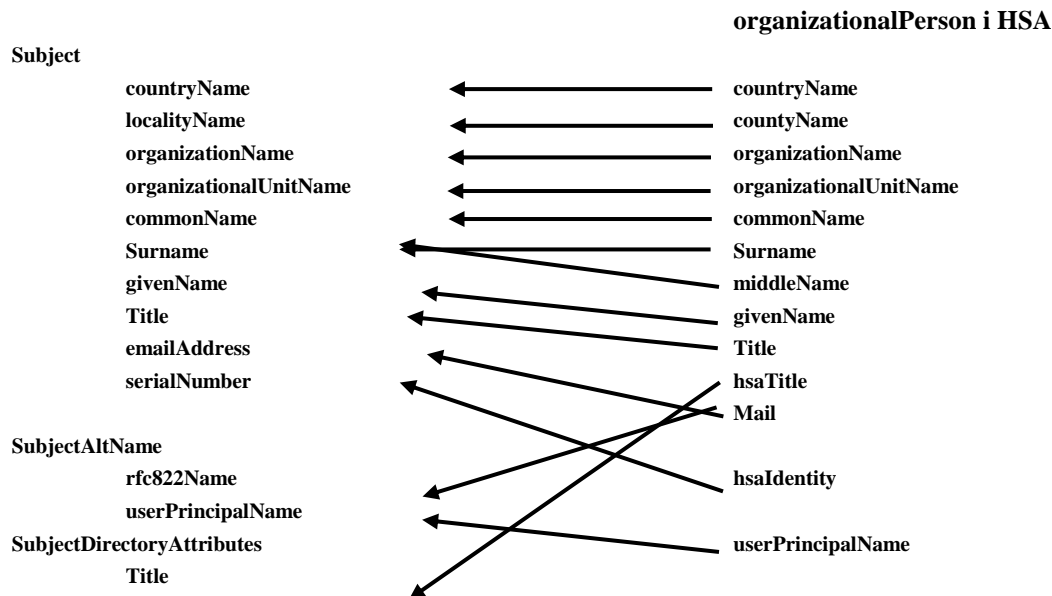
**subjectAltName, userPrincipalName**

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



## Översikt mappning av certifikatinnehållet och HSA-innehåll

### HCC Person



### HCC Funktion

