Certifikatspecifikation för Sveriges kommuner och landsting med samarbetspartners

HCC

inera

Innehållsförteckning

inera

Revisionshistorik

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 ”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.
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.
3.10	2016-10-04	Anpassat för att en person inte behöver ha förnamn. Justerat beskrivningen av enhancedKeyUsage. Slagit ihop beskrivningen av HCC Funktion SHA1 och HCC Funktion SHA512. Justerat kapitlet med kommentar för attributen så att det stämmer på alla ställen.
3.11	2018-04-11	Lagt till localityName för funktionscertifikat. Lagt till Organization validation policy identifier.

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.

Observera att HCC Funktion 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

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	*Max längd*	*Värde*	*Exempel*	*Källa*	*Optional/ Mandatory*	*Critical/ Non-critical*
version	1	2		CA	M	N/A
serialNumber	64		00d9b4778ba5ed51e811f2a664a793ae3a19168381 26543008963190214768545544657 40	CA	M	N/A
signatureAlgorithm		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA	M	N/A
issuer						N/A
countryName	2	SE		CA	M	
organizationName	64	Inera AB		CA	M	
commonName	64	SITHS Type 1 CA v1		CA	M	
validity						N/A
notBefore	13		051108084459Z	CA	M	
notAfter	13		101108084459Z	CA	M	
subject						N/A
title	64		Sjukskötare	RA (HSA)	O	
emailAddress	255		rane.l.ramberg@test.lvn.se	RA (HSA)	O	
serialNumber	64		SE5565968202-3PCH	RA (HSA)	M	
givenName	64		Rane	RA (HSA)	O	
surName	64		Larsson Ramberg	RA (HSA)	M	
commonName	64		Rane Larsson Ramberg	RA (HSA)	M	
organizationName	64		Landstinget Västernorrland	RA (HSA)	M	
localityName	128		Sundsvall	CA	O	
countryName	2		SE	RA (HSA)	M	
cardNumber		*CardNumber enligt svensk standard SS614331*	9752269875705018685	CA	M	NC
subjectDirectoryAttributes						NC
title			Sjukskötare	RA (HSA)	M	
subjectPublicKeyInfo						N/A
algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M	
subjectPublicKey				CA	M	
cRLDistributionPoints		[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] 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		{2.5.29.17}				NC
userPrincipalName	255	{1.3.6.1.4.1.311.20.2.3}	rlrg@test.lvn.se	RA (HSA)	O	
rfc822Name	255		rane.l.ramberg@test.lvn.se	RA (HSA)	O	
certificatePolicies						NC
policyIdentifer		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID>		CA	M	

Attribut	*Max längd*	*Värde*	*Exempel*	*Källa*	*Optional/ Mandatory*	*Critical/ Non-critical*
		[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html				
enhancedKeyUsage					O	NC
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						NC
keyIdentifier				CA	M	
authorityKeyIdentifier **keyIdentifier**		*subjectKeyIdentifier för utfärdande CA*		CA	M	NC
keyUsage		digitalSignature, keyEncipherment		CA	M	C
Signature		*RSA-signatur över SHA1*		CA	M	N/A

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	

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	*Max Längd*	*Värde*	*Exempel*	*Källa*	*Optional/ Mandatory*	*Critical/ Non-critical*
version	1	2		CA	M	N/A
serialNumber	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA	M	N/A
signatureAlgorithm		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA	M	N/A
issuer						N/A
countryName	2	SE		CA	M	
organizationName	64	Inera AB		CA	M	
commonName	64	SITHS Type 1 CA v1		CA	M	
validity						N/A
notBefore	13		051108084459Z	CA	M	
notAfter	13		101108084459Z	CA	M	
subject						N/A
title	64		Sjukskötare	RA (HSA)	O	
emailAddress	255		rane.l.ramberg@test.lvn.se	RA (HSA)	O	
serialNumber	64		SE5565968202-3PCH	RA (HSA)	M	
givenName	64		Rane	RA (HSA)	O	
surname	64		Larsson Ramberg	RA (HSA)	M	
commonName	64		Rane Larsson Ramberg	RA (HSA)	M	
organizationName	64		Landstinget Västernorrland	RA (HSA)	M	
localityName	128		Sundsvall	CA	O	
countryName	2		SE	RA (HSA)	M	
subjectPublicKeyInfo						N/A
algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M	
subjectPublicKey				CA	M	
cardNumber		*CardNumber enligt svensk standard SS614331*	9752269875705018685	CA	M	NC
subjectDirectoryAttributes						NC
title			Sjukskötare	RA (HSA)	M	
cRLDistributionPoints		[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] 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		{2.5.29.17}				NC
rfc822Name	255		rane.l.ramberg@test.lvn.se	RA (HSA)	O	
certificatePolicies						NC
policyIdentifer		[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	

Attribut	*Max Längd*	*Värde*	*Exempel*	*Källa*	*Optional/ Mandatory*	*Critical/ Non-critical*
subjectKeyIdentifier **keyIdentifier**				CA	M	NC
authorityKeyIdentifier **keyIdentifier**		*subjectKeyIdentifier för utfärdande CA*		CA	M	NC
keyUsage		Nonrepudiation		CA	M	C
Signature		*RSA-signatur över SHA1*		CA	M	N/A

HCC Funktion

Översikt HCC Funktion för legitimering och kryptering

HCC Funktion 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**
organizationName	**2.5.4.10**
localityName	**2.5.4.7**
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	

inera

HCC Funktion för legitimering och kryptering - attribut för attribut

Tabell 3. HCC Funktion för legitimering och kryptering.

Attribut	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
version	1	2		CA	M	N/A
serialNumber	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA	M	N/A
signatureAlgorithm		sha-512WithRSAEncryption {1.2.840.113549.1.1.13}		CA	M	N/A
issuer						N/A
countryName	2	SE		CA	M	
organizationName	64	Inera AB		CA	M	
commonName	64	SITHS Type 3 CA v1		CA	M	
validity						N/A
notBefore	13		051108084459Z	CA	M	
notAfter	13		071108084459Z	CA	M	
subject						N/A
serialNumber	64		SE5565594230-1000	RA (HSA)	M	
emailAddress	255		testsiths@inera.se	RA (HSA)	O	
commonName	64		test.siths.se	RA (HSA)	M	
organizationName	64		Inera AB	RA (HSA)	O	
localityName	128		Sundsvall	CA	O	
countryName	2		SE	RA (HSA)	M	
subjectPublicKeyInfo						N/A
algorithm		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA	M	
subjectPublicKey				CA	M	
cRLDistributionPoints		[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]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	255		testsiths@inera.se	RA (HSA)	O	
dNSName	255		test.siths.se	RA (HSA)	M	
certificatePolicies						NC
policyIdentifer		[1]Certificate Policy: Policy Identifier=<ISSUANCE POLICY OID> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://rpa.siths.se/sithsrpav1.html [2] Organization Validation (OV) certificate: Policy Identifier=2.23.140.1.2.2		CA	M	
enhancedKeyUsage				CA	M	NC
clientAuthentication		{1.3.6.1.5.5.7.3.2}		CA	M	
serverAuthentication		{1.3.6.1.5.5.7.3.1}		CA	M	

Attribut	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
emailProtection		{1.3.6.1.5.5.7.3.4}		CA	O	
subjectKeyIdentifier **keyIdentifier**				 CA	 M	NC
authorityKeyIdentifier **keyIdentifier**				 CA	 M	NC
keyUsage		digitalSignature, keyEncipherment		CA	M	C
Signature		<RSA-signatur över SHA512>		CA	M	N/A

Översikt HCC Funktion 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**
organizationName	**2.5.4.10**
localityName	**2.5.4.7**
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 för underskrift - attribut för attribut

Tabell 4. HCC Funktion för underskrift.

Attribut	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
version	1	2		CA	M	N/A
serialNumber	64		00d9b4778ba5ed51e811f2a664a793ae3a	CA	M	N/A
signatureAlgorithm		sha-512WithRSAEncryption {1.2.840.113549.1.1.13}		CA	M	N/A
issuer						N/A
countryName	2	SE		CA	M	
organizationName	64	Inera AB		CA	M	
commonName	64	SITHS Type 3 CA v1		CA	M	
validity						N/A
notBefore	13		051108084459Z	CA	M	
notAfter	13		071108084459Z	CA	M	
subject						N/A
serialNumber	64		SE5565594230-1000	RA (HSA)	M	
emailAddress	255		testsiths@inera.se	RA (HSA)	O	
commonName	64		www.testsiths.se	RA (HSA)	M	
organizationName	64		Inera AB	RA (HSA)	O	
localityName	128		Sundsvall	CA	O	
countryName	2		SE	RA (HSA)	M	
subjectPublicKeyInfo						N/A
algorithm		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA	M	
subjectPublicKey		<bit string>		CA	M	
cRLDistributionPoints		[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]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	255		testsiths@inera.se	RA (HSA)	O	
dNSName	255		test.siths.se	RA (HSA)	M	
certificatePolicies						NC
policyIdentifer		[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	

Attribut	Max längd	Värde	Exempel	Källa	Optional/ Mandatory	Critical/ Non-critical
		[2] Organization Validation (OV) certificate: Policy Identifier=2.23.140.1.2.2				
subjectKeyIdentifier **keyIdentifier**		<octet string>		CA	M	NC
authorityKeyIdentifier **keyIdentifier**		<octet string>		CA	M	NC
keyUsage		Nonrepudiation		CA	M	C
Signature		<RSA-signatur över SHA512>		CA	M	N/A

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 hash-algoritm som agerar underlag för signatur.

Issuer

I detta objekt anges utfärdarens identitet. Sätts av certifikatsutfärdaren.

countryName

Detta attribut skall alltid vara “SE” och anger att certifikatsutfärdaren är en organisation registrerad i Sverige. Anges som printable_string.

organizationName

Namnet på certifikatsutfärdaren. Anges som UTF8_string.

commonName

Utfärdande CA. Anges som UTF8_string.

Validity

Detta objekt 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 objekt anges egenskaper hos nyckelinnehavaren (subjektet).

countryName

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

localityName

Detta attribut innehåller namn på ort i klartext. Namnet hämtas från en lista som SITHS Förvaltning underhåller. För HCC Funktion är localityName sätet för den organisation som äger domännamnet för servern/e-postadressen. För HCC Person är localityName

sätet för den organisation som har ansvaret för utgivningsprocessen[1]. Anges som UTF8string.

För HCC Funktion hämtas värdet från domänvalideringsverktyget

organizationName

Detta attribut innehåller namn på huvudman eller motsvarande. Skall vara en juridisk person med organisationsnummer. Hämtas ur HSA från, i respektive objektklass, organizationalPerson för Person HCC, organizationalRole för Funktion HCC. Anges som UTF8_string.

För HCC Funktion hämtas värdet från domänvalideringsverktyget

commonName

För personer är det normalt bildat av givenName följt av surName. För funktioner är det ett DNS-namn alternativt en ip-adress. Hämtas ur HSA. Anges som UTF8_string. För HCC Funktion kontrolleras värdet mot godkända domännamn i domänvalideringsverktyget innan certifikat tillåts utfärdas.

surName

Attributet surName förekommer endast i Person HCC. I de fall en person har ett mellannamn (middleName i HSA) används även det i surName i HCC. Hämtas ur HSA. Anges som UTF8_string.

givenName

Attributet givenName förekommer endast i Person HCC. Det är obligatoriskt om det finns i folkbokföringen, om det inte finns lämnas attributet tomt. Hämtas ur HSA. Anges som UTF8_string.

title

Detta attribut förekommer endast i Person HCC. Hämtas från attributet *title* i HSA. Anges som UTF8_string.

serialNumber

Subjektets HSA-id. Hämtas ur HSA. Anges som printable_string.

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.

För HCC Funktion kontrolleras värdet mot godkända e-postadresser i domänvalideringsverktyget innan certifikat tillåts utfärdas.

Anges som IA5_string.

subjectPublicKeyInfo

Detta objekt innehåller två attribut som definierar den publika nyckeln i certifikatet.

---

[1] *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.*

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}. Sätts av certifikatsutfärdaren.

subjectPublicKey
Detta attribut innehåller den publika nyckeln. Genereras av certifikatsutfärdaren. Anges som bit string.

cardNumber
Innehåller kortets serienummer. CardNumber skall alltid finnas om ett kort är bärare av den/de privata nycklarna. Hämtas ur e-legitimationen på kortet alternativt ur kortets transportcertifikat. Anges som printable_string.

subjectDirectoryAttributes

title
I detta attribut kan den legitimerade yrkesrollen anges. Hämtas från attributet *hsaTitle i* HSA. Anges som UTF8_string.

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 objektet eller personens e-postadress då en sådan förekommer i HSA-katalogen. . **Observera** att detta attribut SKALL finnas om attributet *emailAddress* är använt i *Subject.* Hämtas ur HSA. Anges som UTF8_string.

För HCC Funktion kontrolleras värdet mot godkända e-postadresser i domänvalideringsverktyget innan certifikat tillåts utfärdas.

userPrincipalName

Detta attribut används då HCC ska användas för inloggning mot MS Active Directory. Hämtas ur HSA. Anges som UTF8_string.

dNSName

Används för HCC Funktion och anger DNS-namnet. Samma innehåll som i attributet *commonName*. Observera att detta attribut SKALL finnas i samtliga HCC Funktion som har *enhancedKeyUsage=serverAuthentication.* Anges som UTF8_string.

För HCC Funktion kontrolleras värdet mot godkända domännamn i domänvalideringsverktyget innan certifikat tillåts utfärdas.

certificatePolicies

policyIdentifer
OID för issuance policy för utfärdande CA samt en länk till SITHS Relying Party Agreement. Reflekterar tillitsnivån av certifikatet. Sätts av certifikatsutfärdaren.
För HCC funktion certifikat av klassen Organization Validation sätter certifikatsutfärdaren dessutom OID 2.23.140.1.2.2

enhancedKeyUsage

HCC Person

Tilldelas HCC Person för legitimering om UPN finns i HSA, innehåller nedanstående utökade syften.
HCC för signering använder inte attributet *enhancedKeyUsage***.**

clientAuthentication

Certifikat med detta syfte kan användas för att identifiera en användare som anropar en server.

emailProtection

Certifikat med detta syfte kan användas för säker e-post. En del e-postsystem kräver detta syfte för att det ska vara möjligt att kryptera och signera e-post (gäller speciellt MS Exchange/Outlook).

smartcardLogon

Certifikat med detta syfte kan användas för inloggning till MS Windows/Active Directory.

HCC Funktion

Tilldelas alltid HCC för legitimering, innehåller två eller tre av nedanstående utökade syften.
HCC för signering använder inte attributet *enhancedKeyUsage***.**

serverAuthentication

Certifikat med detta 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 ett klientsystem som anropar en server.

emailProtection

Certifikat med detta syfte kan användas för säker e-post. En del e-postsystem kräver detta syfte för att det ska vara möjligt att kryptera och signera e-post (gäller speciellt MS Exchange/Outlook).

OBS! Detta attribut sätts endast under **förutsättning** att objektet har attributet *mail* ifyllt i HSA. Informationen i fältet *mail* måste även finnas som *rfc822Name* under *subjectAltName* och som *emailAddress* under *Subject*

subjectKeyIdentifier

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

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. Anges som octet_string.

keyUsage
I detta attribut definieras hur den publika nyckel (och den privata) får användas. Anges som bit_string. Attributet 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.

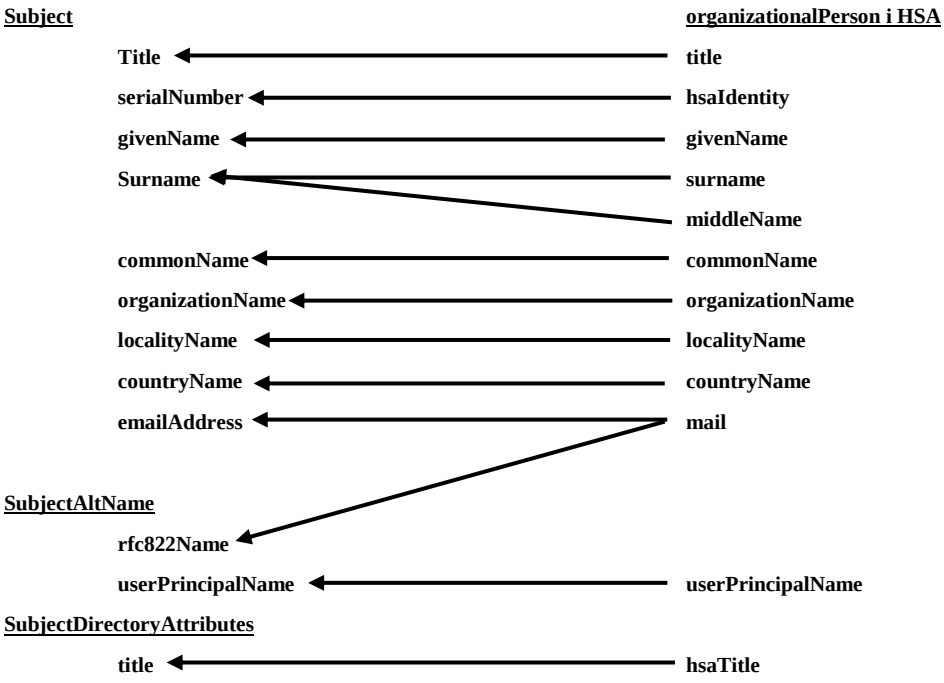
nonRepudiation
anger att nyckeln används för att verifiera elektroniska signaturer.

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