carelink

Certifikat

för

svensk vård och omsorg

HCC

Version 2.34

2007-12-14

Innehåll

Revisionshistorik

Version	Datum	Kommentar
1	2001-01-30	Första fastställda versionen. Beskriver minimiformatet för HCC.
1A	2002-12-13	Mindre korrigering av version 1 rörande innehållet i certifikatsattributet **subject**, **commonName** i objektklassen **OrganizationalPerson**. Ändringen införd i beskrivningen av **commonName** i avsnitt 2.2, sid 21. Uttrycket ”hälso- och sjukvård” bytts ut mot ”vård och omsorg”
1B	2003-10-15	Attribut för Netscape tillagt.
1C	2005-10-28	Format på certifikatserienummer (**serialNumber**) ändrat. Attribut för organisationsnummer (**orgNo**), kortserienummer (**cardNumber**), OCSP-adress (**AuthorityInfoAccess**) tillagt. Längd på attributet för HSA-id (**serialNumber**) ändrat.
1D	2006-01-11	HSA-attributet **personIdentityNumber** namnändrat till **personalIdentityNumber**
2	2006-01-23	Tabell över OID för ingående attribut tillagd. Attribut för epostadress i Subject ändrat till EmailAddress. Notation för CardNumber ändrat från CardNumber::=CardNumber till enbart CardNumber.
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. Borttag av attributet CardNumber för HCC Funktion. Borttag av attributet NetscapeCertificateType från samtliga certifikattyper. Tillägg av EnhancedKeyUsage i HCC Funktion för att följa de facto-standard för servercertifikat. HCC Funktion för autentisering/kryptering separeras från HCC Funktion för signering, eftersom de inte kan dela samma definition för EnhancedKeyUsage. Ändring av tabell som illustrerar informationskälla för data i certifikaten. Attributen i certifikatet som sätts genom val av administratör är märkta med Mandatory eller Optional.
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. Kapitelindelning har gjorts tydligare, med en HCC-typ i varje kapitel. Mappning mellan HSA och SITHS är uppdaterad och uppsnyggad. Referenser till HSA-dokumentation uppdaterad.
2.33	2007-11-12	Borttag av kolumnen IDC ur HCC Person och HCC Organisation. Mappning mellan det s.k. primärcertifikatet och HCC berörs inte längre i HCC-specifikationen.
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. Signering av e-post berörs ej, då HCC Funktion för signering ej innehåller enhanced key usage.

1 Inledning

Detta dokument specificerar certifikat för vård och omsorg inom ramen för SITHS-modellen; HCC Person, HCC Organisation och HCC Funktion.

Observera att skilda katalogstrukturer i HSA-katalogen används för HCC Person/Organisation 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.

2 HCC Person

HCC Person består av ett certifikat för identifiering (autentisering) och ett certifikat för signering.

HCC Person för identifiering finns i två varianter, en grundvariant och en variant som är anpassad för inloggning till Microsoft Windows och Active Directory. Dessa kallas då HCC Person och HCC Person för MS Windows.

HCC Person för signering finns bara i en variant.

2.1 Översikt HCC Person

HCC Person i grundvarianten 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	
countryName	**2.5.4.6**
localityName	**2.5.4.7**
organizationName	**2.5.4.10**
organizationalUnitName	**2.5.4.11**
commonName	**2.5.4.3**
surname	**2.5.4.4**
givenName	**2.5.4.42**
title	**2.5.4.12**
emailAddress	**1.2.840.113549.1.9.1**
serialNumber	**2.5.4.5**
subjectPublicKeyInfo	
algorithm	
subjectPublicKey	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
keyUsage	**2.5.29.15**
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectAltName	**2.5.29.17**
rfc822Name	
subjectDirectoryAttributes	
title	**2.5.4.12**
authorityInformationAccess	
ocsp	**1.3.6.1.5.5.7.48.1**
cRLDistributionPoints	**2.5.29.31**
cardNumber	**1.2.752.34.2.1**
Signature	

2.2 HCC Person, attribut för attribut

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

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
version	1	1	2		CA		M
serialNumber	1	64		191683812654300896319021476854554465740	CA		M
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M
issuer							
countryName	1	2	SE		CA		M
organizationName	1	64	Carelink		CA		M
commonName	1	64	SITHS CA v3		CA		M
validity							
notBefore		13		001201080000Z	CA		M
notAfter		13		021117175720Z	CA		M
subject							
countryName	1	2		SE	RA	HSA	M
localityName	1	128		Dalarnas län	RA	HSA	O
organizationName	1	64		Landstinget Dalarna	RA	HSA	M
organizationalUnitName	10	64		Falu lasarett	RA	HSA	O
commonName	1	64		Legitimis Andersson	RA	HSA	M
surName	1	64		Andersson	RA	HSA	M
givenName	1	64		Legitimis	RA	HSA	M
title	1	64		Klinikchef	RA	HSA	O
emailAddress	1	255		legitmis.andersson@ltdalarna.se	RA	HSA	O
serialNumber	1	64		SE162321100107-2XKN	RA	HSA	M
subjectPublicKeyInfo	1						
algorithm	1		rsaEncryption {1.2.840.113549.1.1.1}		CA		M
subjectPublicKey	1		<bit string>		CA		M
authorityKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
subjectKeyIdentifier **keyIdentifier**	1		<octet string>		CA		M
keyUsage	1		alt 1: digitalSignature, keyEncipherment alt 2: nonRepudiation		CA		M
certificatePolicies **policyIdentifer**	1		{OID= 1.2.752.74.1.1.3 }		CA		M
subjectAltName **rfc822Name**	1	255		legitmis.andersson@ltdalarna.se	RA	HSA	O
subjectDirectoryAttributes **title**	1			Leg Läkare	RA	HSA	M
authorityInformationAccess	1						
			access Method=On-line Certificate Status Protocol		CA		M
			alternative Name:	[1] OCSP (se nedan)	CA		M
cRLDistributionPoints	1			[2] LDAP [3] HTTP (se nedan)	CA		M
cardNumber [4]	1			9752222515400112222	CA		M
Signature	1				CA		M

[1] Anger HTTP-adressen till OCSP enligt följande format (exempel): URL= http://sithsocsp.trust.telia.com

[2] Anger LDAP-adressen till CRL enligt följande format (exempel): URL=ldap://sithscrl.carelink.sjunet.org/c%3DSE?certificateRevocationList

[3] Anger HTTP-adressen till CRL enligt följande format (exempel): URL=http://www.carelink.se/siths-ca/ca001.crl

[4] CardNumber enligt svensk standard SS614331

2.3 Översikt HCC Person för MS Windows

HCC Person för MS Windows kan ha följande innehåll. Observera att HCC Person för MS Windows endast skiljer sig från HCC Person vad gäller certifikatet för identifiering (autentisering).

I HCC för MS Windows är attributen *enhancedKeyUsage*, med värdena *SmartCardLogon, clientAuthentication och emailProtection*, och *userPrincipalName* tillagda.

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	
countryName	**2.5.4.6**
localityName	**2.5.4.7**
organizationName	**2.5.4.10**
organizationalUnitName	**2.5.4.11**
commonName	**2.5.4.3**
surname	**2.5.4.4**
givenName	**2.5.4.42**
title	**2.5.4.12**
emailAddress	**1.2.840.113549.1.9.1**
serialNumber	**2.5.4.5**
subjectPublicKeyInfo	
algorithm	
subjectPublicKey	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
keyUsage	**2.5.29.15**
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**
subjectAltName	**2.5.29.17**
userPrincipalName	**1.3.6.1.4.1.311.20.2.3**
rfc822Name	
subjectDirectoryAttributes	
title	**2.5.4.12**
authorityInformationAccess	
ocsp	**1.3.6.1.5.5.7.48.1**
cRLDistributionPoints	**2.5.29.31**
cardNumber	**1.2.752.34.2.1**
signature	

2.4 HCC Person för MS Windows, attribut för attribut

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

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
version	1	1	2		CA		M
serialNumber	1	64		191683812654300896319021476854554465740	CA		M
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M
issuer							
countryName	1	2	SE		CA		M
organizationName	1	64	Carelink		CA		M
commonName	1	64	SITHS CA v3		CA		M
validity							
notBefore		13		001201080000Z	CA		M
notAfter		13		021117175720Z	CA		M
subject							
countryName	1	2		SE	RA	HSA	M
localityName	1	128		Dalarnas län	RA	HSA	O
organizationName	1	64		Landstinget Dalarna	RA	HSA	M
organizationalUnitName	10	64		Falu lasarett	RA	HSA	O
commonName	1	64		Legitimis Andersson	RA	HSA	M
surName	1	64		Andersson	RA	HSA	M
givenName	1	64		Legitimis	RA	HSA	M
title	1	64		Klinikchef	RA	HSA	O
emailAddress	1	255		legitmis.andersson@ltdalarna.se	RA	HSA	O
serialNumber	1	64		SE162321100107-2XKN	RA	HSA	M
subjectPublicKeyInfo	1						
algorithm	1		rsaEncryption {1.2.840.113549.1.1.1}		CA		M
subjectPublicKey	1		<bit string>		CA		M
authorityKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
subjectKeyIdentifier **keyIdentifier**	1		<octet string>		CA		M
keyUsage	1		digitalSignature, keyEnci-pherment		CA		M
enhancedKeyUsage **clientAuthentication**[5] **smartCardLogon**[5] **emailProtection**[6]	 1 1 1		 {OID= 1.3.6.1.5.5.7.3.2} {OID= 1.3.6.1.4.1.311.20.2.2} {OID= 1.3.6.1.5.5.7.3.4}		 CA CA CA		 O O O
certificatePolicies **policyIdentifer**	1		{OID= 1.2.752.74.1.1.3 }		CA		M
subjectAltName **userPrincipalName**[5] **rfc822Name**	 1 1	 255 255	 {OID= 1.3.6.1.4.1.311.20.2.3}	 SE162321100107-2XKN@ltdalarna.se legitmis.andersson@ltdalarna.se	 RA RA	 HSA HSA	 O O
subjectDirectoryAttributes **title**	1			Leg Läkare	RA	HSA	M
authorityInformationAccess	1						
			access Method=On-line Certificate Status Protocol		CA		M
			alternative Name:	[1] OCSP (se nedan)	CA		M
cRLDistributionPoints	1			[2] LDAP [3] HTTP (se nedan)	CA		M
cardNumber [4]	1			9752222515400112222	CA		M
Signature	1				CA		M

[1] Anger HTTP-adressen till OCSP enligt följande format (exempel): URL= http://sithsocsp.trust.telia.com

[2] Anger LDAP-adressen till CRL enligt följande format (exempel): URL=ldap://sithscrl.carelink.sjunet.org/c%3DSE?certificateRevocationList

[3] Anger HTTP-adressen till CRL enligt följande format (exempel): URL=http://www.carelink.se/siths-ca/ca001.crl

[4] CardNumber enligt svensk standard SS614331

[5] Förekomsten av dessa attribut är kopplade till inloggning i MS Windows.

[6] emailProtection måste finnas i certfikat för kryptering och signering av e-post, om enhancedKeyUsage används.

3 HCC Organisation

HCC Organisation utfärdas till en organisation eller organisationsenhet.

3.1 Översikt HCC Organisation

HCC Organisation 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	
countryName	**2.5.4.6**
localityName	**2.5.4.7**
organizationName	**2.5.4.10**
organizationalUnitName	**2.5.4.11**
emailAddress	**1.2.840.113549.1.9.1**
serialNumber	**2.5.4.5**
subjectPublicKeyInfo	
Algorithm	
subjectPublicKey	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
keyUsage	**2.5.29.15**
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectAltName	**2.5.29.17**
rfc822Name	
subjectDirectoryAttributes	
Title	**2.5.4.12**
authorityInformationAccess	
Ocsp	**1.3.6.1.5.5.7.48.1**
cRLDistributionPoints	**2.5.29.31**
cardNumber	**1.2.752.34.2.1**
Signature	

3.2 HCC Organisation attribut för attribut

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

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
version	1	1	2		CA		M
serialNumber	1	64		191683812654300896319021476854554465740	CA		M
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M
issuer							
countryName	1	2	SE		CA		M
organizationName	1	64	Carelink		CA		M
commonName	1	64	SITHS CA v3		CA		M
validity							
notBefore		13		001201080000Z	CA		M
notAfter		13		021117175720Z	CA		M
subject							
countryName	1	2		SE	RA	HSA	M
localityName	1	128		Dalarnas län	RA	HSA	O
organizationName	1	64		Landstinget Dalarna	RA	HSA	M
organizationalUnitName	10	64		Falu lasarett	RA	HSA	O
emailAddress	1	255		falulasarett@ltdalarna.se	RA	HSA	O
serialNumber	1	64		SE162321100107-2KNX	RA	HSA	M
subjectPublicKeyInfo	1						
algorithm	1		rsaEncryption {1.2.840.113549.1.1.1}		CA		M
subjectPublicKey	1		<bit string>		CA		M
authorityKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
subjectKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
keyUsage	1		alt 1: digitalSignature, keyEncipherment		CA		M

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
			alt 2: nonRepudiation				
certificatePolicies **policyIdentifer**	1		{OID= 1.2.752.74.1.1.3 }		CA		M
subjectAltName **rfc822Name**	1	255		legitmis.andersson@ltdalarna.se	RA	HSA	O
authorityInformationAccess	1						
			access Method=On-line Certificate Status Protocol		CA		M
			alternative Name:	[1] OCSP (se nedan)	CA		M
cRLDistributionPoints	1			[2] LDAP [3] HTTP (se nedan)	CA		M
cardNumber [4]	1			9752222515400112222	CA		O
Signature	1				CA		M

[1] Anger HTTP-adressen till OCSP enligt följande format (exempel): URL= http://sithsocsp.trust.telia.com

[2] Anger LDAP-adressen till CRL enligt följande format (exempel): URL=ldap://sithscrl.carelink.sjunet.org/c%3DSE?certificateRevocationList

[3] Anger HTTP-adressen till CRL enligt följande format (exempel): URL=http://www.carelink.se/siths-ca/ca001.crl

[4] CardNumber enligt svensk standard SS614331. CardNumber förekommer endast i HCC Organisation som lagras på kort.

4 HCC Funktion

4.1 Översikt HCC Funktion för autentisering och kryptering

HCC Funktion för 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	
countryName	**2.5.4.6**
DC	**0.9.2342.19200300.100.1.25**
organizationName	**2.5.4.10**
organizationalUnitName	**2.5.4.11**
commonName	**2.5.4.3**
emailAddress	**1.2.840.113549.1.9.1**
serialNumber	**2.5.4.5**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
keyUsage	**2.5.29.15**
digital Signature, keyEncipherment	
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**
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectAltName	**2.5.29.17**
Rfc822Name	
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
access Method=On-line Certificate Status Protocol	**1.3.6.1.5.5.7.48.1**
alternative Name = <adress till OCSP-tjänst>	
cRLDistributionPoints	**2.5.29.31**
Signature	

4.2 HCC Funktion för autenticering och kryptering attribut för attribut

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
version	1	1	2		CA		M
serialNumber	1	64		191683812654300896319021476854554465740	CA		M
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M
issuer							
countryName	1	2	SE		CA		M
organizationName	1	64	Carelink		CA		M
commonName	1	64	SITHS CA v3		CA		M
validity							
notBefore		13		001201080000Z	CA		M
notAfter		13		021117175720Z	CA		M
subject							
countryName	1	2		SE	RA	HSA	M
DC	2			[4]DC=Services, DC=Nod1	RA	HSA	O
organizationName	1	64		[4]232100000016	RA	HSA	O
organizationalUnitName	10	64		[4]E-recept	RA	HSA	O
commonName	1	64		e-recept.lsf.se	RA	HSA	M
emailAddress	1	255		[4]e-recept@lsf.se	RA	HSA	O
serialNumber	1	64		SE162321100107-KNX2	RA	HSA	M
subjectPublicKeyInfo	1						
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M
subjectPublicKey	1		<bit string>		CA		M
authorityKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
subjectKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
keyUsage			digitalSignature, keyEnci-pherment		CA		M
enhancedKeyUsage			serverAuthentication, clien-		CA		M

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
			tAuthentication				
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		M
certificatePolicies							
policyIdentifer	1		{OID= 1.2.752.74.1.1.3 }		CA		M
subjectAltName							
rfc822Name	1	255		e-recept@lsf.se	RA	HSA	O
authorityInformationAccess	1						
			access Method=On-line Certificate Status Protocol		CA		M
			alternative Name:	[1]OCSP (se nedan)	CA		M
cRLDistributionPoints	1			[2] LDAP [3] HTTP (se nedan)	CA		M
cardNumber [5]	1			9752222515400112222	CA		O
signature	1				CA		M

[1] Anger HTTP-adressen till OCSP enligt följande format (exempel): URL= http://sithsocsp.trust.telia.com

[2] Anger LDAP-adressen till CRL enligt följande format (exempel): URL=ldap://sithscrl.carelink.sjunet.org/c%3DSE?certificateRevocationList

[3] Anger HTTP-adressen till CRL enligt följande format (exempel): URL=http://www.carelink.se/siths-ca/ca001.crl

[4] Subject för HCC Funktion kan återge en adress till både det i HSA definierade Service-trädet eller i Organisationsträdet.

[5] CardNumber enligt svensk standard SS614331. CardNumber förekommer endast i HCC Funktion som lagras på kort.

4.3 Översikt HCC Funktion för signering

HCC Funktion för signering 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	
countryName	**2.5.4.6**
DC	**0.9.2342.19200300.100.1.25**
organizationName	**2.5.4.10**
organizationalUnitName	**2.5.4.11**
commonName	**2.5.4.3**
emailAddress	**1.2.840.113549.1.9.1**
serialNumber	**2.5.4.5**
subjectPublicKeyInfo	
algorithm =RSA Encryption	**1.2.840.113549.1.1.1**
subjectPublicKey	
authorityKeyIdentifier	**2.5.29.35**
keyIdentifier	
subjectKeyIdentifier	**2.5.29.14**
keyIdentifier	
keyUsage	**2.5.29.15**
nonRepudiation	
certificatePolicies	**2.5.29.32**
policyIdentifer	
subjectAltName	**2.5.29.17**
rfc822Name	
authorityInformationAccess	**1.3.6.1.5.5.7.1.1**
access Method=On-line Certificate Status Protocol	**1.3.6.1.5.5.7.48.1**
alternative Name = <adress till OCSP-tjänst>	
cRLDistributionPoints	**2.5.29.31**
Signature	

4.4 HCC Funktion för signering attribut för attribut

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
version	1	1	2		CA		M
serialNumber	1	64		191683812654300896319021476854554465740	CA		M
signatureAlgorithm	1		sha-1WithRSAEncryption {1.2.840.113549.1.1.5}		CA		M
issuer							
countryName	1	2	SE		CA		M
organizationName	1	64	Carelink		CA		M
commonName	1	64	SITHS CA v3		CA		M
validity							
notBefore		13		001201080000Z	CA		M
notAfter		13		021117175720Z	CA		M
subject							
countryName	1	2		SE	RA	HSA	M
DC	2			[4]DC=Services, DC=Nod1	RA	HSA	O
organizationName	1	64		[4]232100000016	RA	HSA	O
organizationalUnitName	10	64		[4]E-recept	RA	HSA	O
commonName	1	64		e-recept.lsf.se	RA	HSA	M
emailAddress	1	255		[4]e-recept@lsf.se	RA	HSA	O
serialNumber	1	64		SE162321100107-456000305	RA	HSA	M
subjectPublicKeyInfo	1						
algorithm	1		rsaEncryption {1. 2. 840. 113549. 1. 1. 1}		CA		M
subjectPublicKey	1		<bit string>		CA		M
authorityKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
subjectKeyIdentifier							
keyIdentifier	1		<octet string>		CA		M
keyUsage			nonRepudiation		CA		M
certificatePolicies							
policyIdentifer	1		{OID= 1.2.752.74.1.1.3 }		CA		M

Attribut	Antal förek.	Max-längd	Värde	Exempel	Källa	HSA	Optio-nal/Manda-tory
subjectAltName **rfc822Name**	1	255		e-recept@lsf.se	RA	HSA	O
authorityInformationAccess	1						
			access Method=On-line Certificate Status Protocol		CA		M
			alternative Name:	[1]OCSP (se nedan)	CA		M
cRLDistributionPoints	1			[2] LDAP [3] HTTP (se nedan)	CA		M
cardNumber [5]	1			9752222515400112222	CA		O
signature	1				CA		M

[1] Anger HTTP-adressen till OCSP enligt följande format (exempel): URL= http://sithsocsp.trust.telia.com

[2] Anger LDAP-adressen till CRL enligt följande format (exempel): URL=ldap://sithscrl.carelink.sjunet.org/c%3DSE?certificateRevocationList

[3] Anger HTTP-adressen till CRL enligt följande format (exempel): URL=http://www.carelink.se/siths-ca/ca001.crl

[4] Subject för HCC Funktion kan återge en adress till både det i HSA definierade Service-trädet eller i Organisationsträdet.

[5] CardNumber enligt svensk standard SS614331. CardNumber förekommer endast i HCC Funktion som lagras på kort.

5 Kommentarer attribut för attribut

version
Anger version av X.509 certifikatsstandard. Skall alltid vara 2 (d.v.s. version 3). Detta attribut sätts av certifikatsutfärdaren.

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 att algoritmerna RSA och SHA-1 används av certifikatsutfärdaren vid framställning av hashsummor. I exemplet ovan anges både objektnamnet och värdet.

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.

commonName
Sätts av certifikatsutfärdaren. Del av Issuer.

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 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 fästställs och tillhandahålls av Carelink. Se vidare [B11]. 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.

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: Organizational Person för Person HCC, Organizational Role för Funktion HCC, Organization för Organization 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 objektklassen Organizational Person om detta är ett Person HCC. För Funktion HCC används motsvarande attribut i objektklassen Organizational Role**.** Del av Subject. Hämtas ur HSA.

commonName

Detta attribut förekommer ej i Organisation HCC. Namnet hämtas av RA-klienten från motsvarande attribut i objektklassen Organizational Person i HSA-katalogen, som normalt är givenName följt av mellanslag följt av surName. För Funktion HCC används commonName i objektklassen 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.

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 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.

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.

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/Organisation 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. Se nedan för vidare beskrivning av detta.

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, policyIdentifer

Här anges OID för CA-policy beskriven i Certifikatpolicy för utfärdande av certifikat för vård och omsorg (HCC). 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. Attributets värdemängd framgår av [B10]. 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 i HSA och en på en av Carelinks driftad webbplats. Den första är således en LDAP-URL och är tänkt att användas av förlitande parter inom vård och omsorg som har HSA-katalog. Den andra är en HTTP-URL och är tänkt att användas av övriga parter utanför SJUNET med sedvanlig Internetaccess.

authorityInformationAccess
Innehåller adress till aktuell OCSP-tjänst (online certificate status protocol). Med OCSP-tjänsten kan frågor om enskilda certifikats giltighet ställas.

Attribut för inloggning till MS Windows/Active Directory

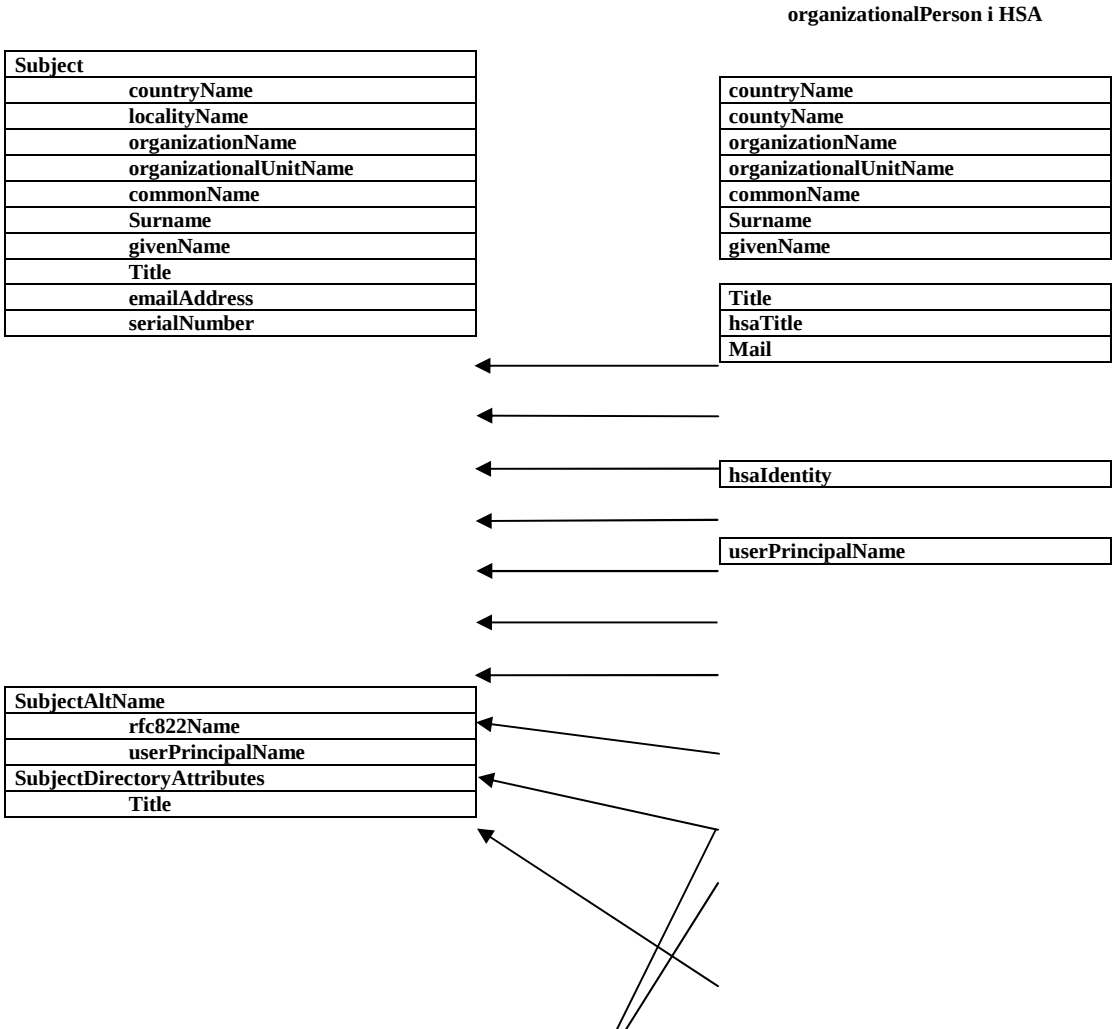
subjectAltName, userPrincipalName
Detta attribut används då HCC ska användas för inloggning mot MS Active Directory (Windows Server 2003 och tidigare versioner). Attributet userPrincipalName bör hämtas ur HSA-katalogen.

enhancedKeyUsage, clientAuthentication
Detta attribut används då HCC ska användas för inloggning mot MS Active Directory (Windows Server 2003 och tidigare versioner). Attributet clientAuthentication sätts av CA och kan inte ändras manuellt.

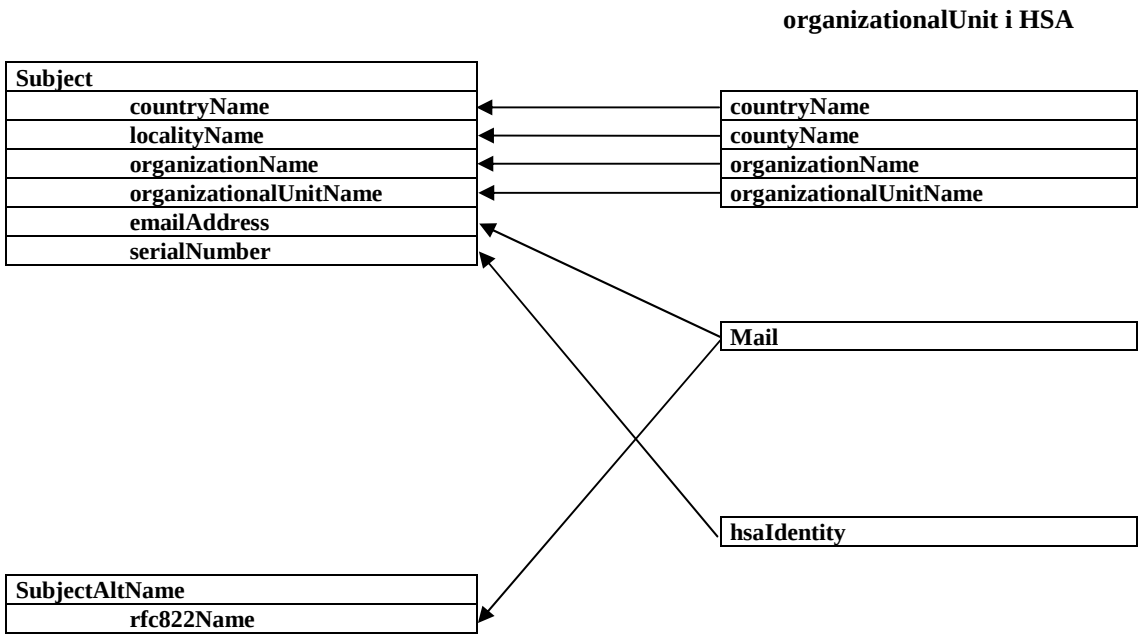
enhancedKeyUsage, smartCardLogon
Detta attribut används då HCC ska användas för inloggning mot MS Active Directory (Windows Server 2003 och tidigare versioner). Attributet smartCardLogon sätts av CA och kan inte ändras manuellt.

6 Översikt mappning av certifikatinnehållet och HSA-innehåll

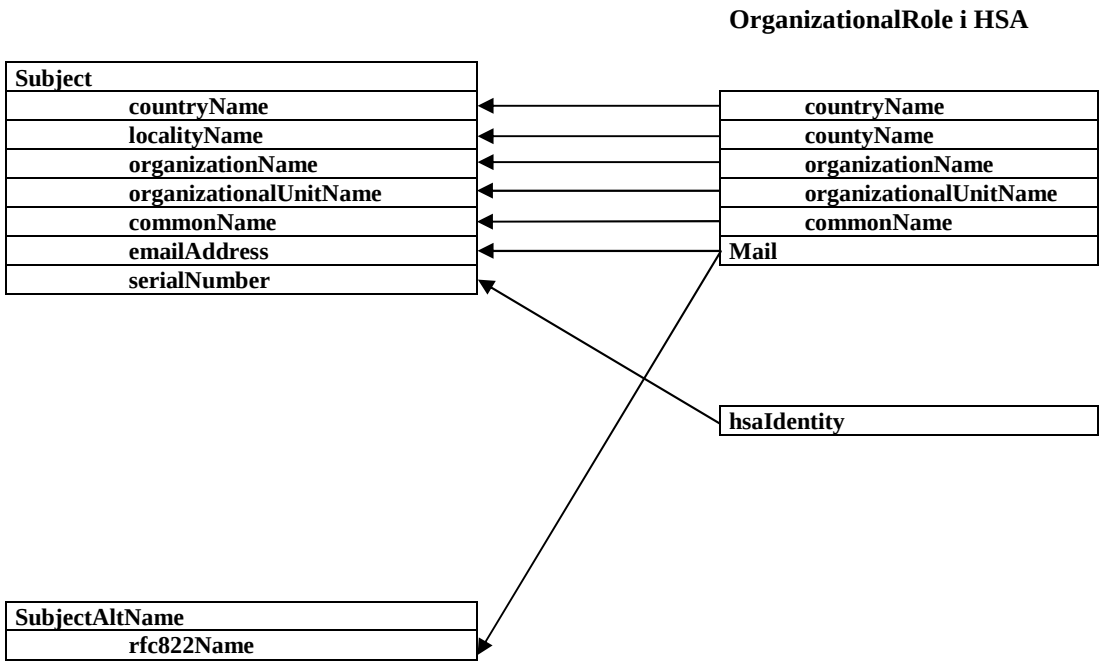
HCC Person



HCC Organisation



HCC Funktion



7 Jämförelse mellan de olika varianterna av HCC

✓ = obligatoriskt, (✓) = frivilligt

Attribut	Person HCC	Organisation HCC	Funktion HCC
Version	✓	✓	✓
serialNumber	✓	✓	✓
Signature	✓	✓	✓
Issuer			
countryName	✓	✓	✓
organizationName	✓	✓	✓
commonName	✓	✓	✓
Validity			
notBefore	✓	✓	✓
notAfter	✓	✓	✓
Subject			
countryName	✓	✓	✓
domainComponent, DC			(✓)
localityName	(✓)	(✓)	(✓)
organizationName	✓	✓	(✓)
organizationalUnitName	(✓)	(✓)	(✓)
commonName	✓		✓
Surname	✓		
givenName	✓		
Title	(✓)		
emailAddress	(✓)	(✓)	(✓)
serialNumber	✓	✓	✓
subjectPublicKeyInfo			
Algorithm	✓	✓	✓
subjectPublicKey	✓	✓	✓
authorityKeyIdentifier			
keyIdentifier	✓	✓	✓
subjectKeyIdentifier			
keyIdentifier	✓	✓	✓
keyUsage	✓	✓	✓
enhancedKeyUsage	[1]: ✓		[2]: ✓
certificatePolicies			
policyIdentifer	✓	✓	✓
subjectAltName			
rfc822Name	(✓)	(✓)	(✓)
subjectDirectoryAttributes			
Title	(✓)		
authorityInformationAccess	✓	✓	✓
cRLDistributionPoints	✓	✓	✓
cardNumber	✓	(✓)	(✓)

[1] för begränsningar, se Kap 2: HCC Person

[2] för begränsningar, se Kap 4: HCC Funktion attribut för attribut

Kommentarer:

Attributet **rfc822Name** i tillägget **subjectAltName är** frivilligt för alla certifikatstyper, men SKALL finnas om attributet **emailAddress** används.

Notera att det inte finns något fält för certifikatstyp, HCC Person/Organisation/Funktion, utan denna måste bestämmas genom att analysera attributförekomsterna i certifikatet.

8 Referenser

B10 **Bilaga 10 – HSA Innehåll, bilaga Legitimerade yrkesgrupper, version 3.0**
HSA-specifikation. Tillgänglig på http://www.carelink.se

B11 **Bilaga 11 – HSA Innehåll, bilaga Länskoder, version 3.0**
HSA-specifikation. Tillgänglig på http://www.carelink.se

HSA **HSA Struktur och innehåll, version 3.0**
HSA-specifikation. Slutlig utgåva. Version 2.0, 2001-03-01.
Tillgänglig på http://www.carelink.se

RFC3280 **Internet X.509 Public Key Infrastructure. Certificate and CRL Profile.**
Request for Comments: 3280, April 2002. Ersätter RFC 2459.

X.509 **ITU-T Recommendation X.509.**
Information Technology – Open Systems Interconnection –The Directory: Authentication Framework. ITU-T 06/97.