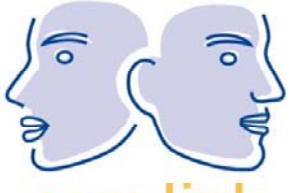
Policy

SITHS

RA-policy för utgivande av certifikat inom vård och omsorg

Version 2003-06-16



Carelink AB
Box 12713
112 94 Stockholm
Telefon: 08/650 62 10
Fax: 08/650 26 42
ISBN 91-7188-581-1

Mall för upprättande av RAPS för utfärdande av certifikat inom vård och omsorg (HCC).

INNEHÅLLSFÖRTECKNING

Figurer

Bilagor

RA-policy för utfärdande av certifikat inom vård och omsorg (HCC)

Detta dokument innehåller SITHS RA-policy för utgivning av certifikat för vård och omsorg i Sverige, s.k. Healthcare Certificate (HCC) eller certifikat för vård och omsorg.

Den allmänna PKI-struktur i vilka dessa certifikat är en central del finns beskriven i dokumentet Infrastruktur för informationssäkerhet i svensk hälso- och sjukvård [INFRA].

HCC finns specificerat i Implementering av hälso- och sjukvårdscertifikat [IMPL] samt i Certifikat för svensk vård och omsorg HCC, Version 1A [HCC1A].

Detta dokument har försetts med namn och objektidentifierare (OID). Dessa framgår av avsnitt 1.3.

Denna RA-policy kräver upprättande av ett separat dokument, RA-policy Practice Statement, RAPS. Mall för upprättande av RAPS finns framtagande av Carelink och skall användas. [RAPSmall].

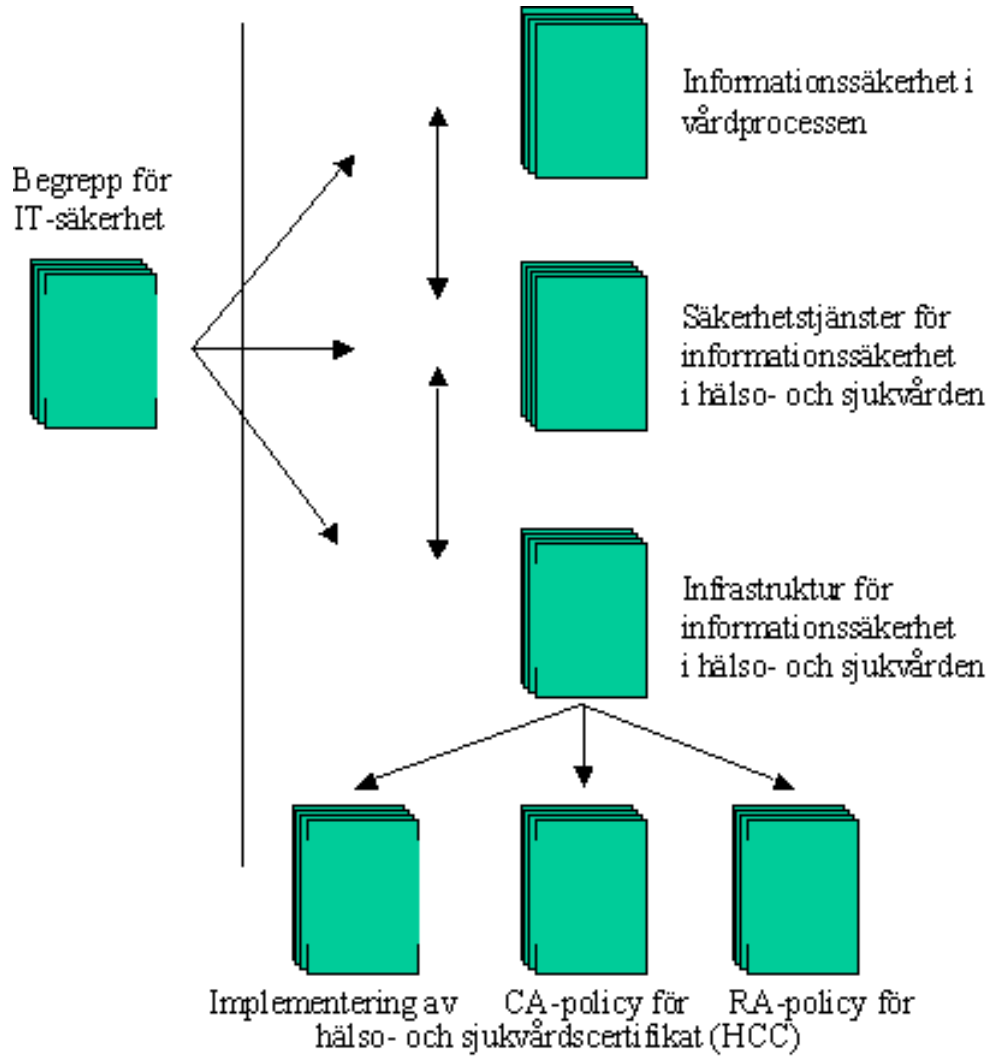
Detta dokument ägs och förvaltas av Carelink AB.

Revisionshistorik

Version	**Status**
2000-05-15	Slutligt förslag från SITHS-projektet.
2003-04-04 remissversion	**Ny version med anledning av upprättande av RAPS-mall** • Definitioner genomgångna och placerade längst fram i dokumentet i enlighet med CA-policyn. Gamla bilaga 1 har utgått. • Förkortningar genomgångna och placerade längst fram i dokumentet efter definitionerna i enlighet med CA-policyn. Gamla bilaga 2 har utgått. • Identifikation tillagt i avsnitt 1.3. Gamla 1.3 har blivit 1.4. • Termen ”HC-DIR” ändrad till ”HSA”. • Referens till HSA:s katalogpolicy har lagts till. • Referens till RAPS-mall har lagts till. • Begreppet ”hälso- och sjukvård” utbytt mot ”vård och omsorg” där det används generellt (dvs. ej i förkortningar och i namn) • Hänvisning till att nyckelinnehavaren själv kan spärra sitt certifikat har strukits i avsnitten 3.2 *Begäran om spärrning av certifikat* och 4.3 *Spärrning av certifikat.* Texten kvar, men överstruken. Återstår att göra: Kontroll av referenserna till CA-policyn.

SITHS-konceptet
Rapportserie, uppdatering och versionshantering

Föreliggande rapport ingår i en serie om sju rapporter om SITHS-konceptet. Dessa rapporter och deras inbördes relationer framgår av följande bild:



Rapporterna kan beställas från Landstingsförbundets rapportförlag eller hämtas direkt via Internet, i form för Adobe Reader (pdf), och från Carelinks webbsida: www.carelink.se.

Rapporterna har åsatts en versionsbeteckning och nya versioner planeras efterhand som teknik och marknad utvecklas och erfarenheter kommer fram.

DEFINITIONER

Endast begrepp och termer som används i detta dokument tas upp nedan. Begreppen är avstämda mot Terminologi för Informationssäkerhet Rapport ITS 6 [ITS6], SEIS Certificate Policy SEIS – S10 [SEIS] och den svenska version som utgivits av Posten Sverige AB [Posten] samt rapporten Begrepp för IT-säkerhet [SÄKBRP].

Autenticering: Kontroll av uppgiven identitet, t ex vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelanden mellan användare. Allmänt: styrkande av äkthet.

Behörig representant: Anställd hos uppdragsgivare som har befogenhet att beställa och spärra certifikat hos CA.

Certifikatpolicy: En namngiven uppsättning regler för framställning, utgivning och spärrning av certifikat och som reglerar tillämpligheten av certifikaten inom ett specifikt användningsområde.

CA: Organisation som utfärdar certifikat genom att signera certifikat med sin privata CA-nyckel. Förkortning av Certification Authority.

CA-nyckel: Nyckelpar där den privata nyckeln används av CA för att signera certifikat och där den publika nyckeln används för att verifiera samma certifikat.

CA-certifikat: Certifikat som certifierar att en viss publik nyckel är publik nyckel för en specifik CA.

Certificate Revocation List: Se CRL.

Certification Authority: Se CA.

Certification Practice Statement: Se CPS.

Certifikat: Ett digitalt signerat intyg av en publik nyckels tillhörighet till en specifik nyckelinnehavare.

CPS: En dokumentation av hur en CA tillämpar en certifikatpolicy. En CPS kan vara gemensam för flera certifikatspolicies. Förkortning av Certification Practice Statement.

CRL: Förkortning för Certificate Revocation List. [ISO/IEC 14516-1&2]. Se spärrlista.

Dekryptering: Processen att omvandla krypterad (kodad) information till dekrypterad (läsbar) information. Se vidare kryptering.

Digital signatur: En form av elektronisk signatur som skapas genom att signatären signerar digital information med sin privata nyckel enligt en speciell procedur. Den digitala signaturen kan användas dels för att spåra vem som signerat informationen och dels för att verifiera att informationen inte förändrats sedan den signerades.

eID-kort: Elektroniska ID-kort i form av ett aktivt kort innehållande certifikat och nycklar samtidigt som kortets framsida kan utgöra en visuell ID-handling.

Elektronisk signatur: Generell beteckning på signatur som skapats med hjälp av IT. Digital motsvarighet till traditionell underskrift. Se också digital signatur.

Hälso- och sjukvården: Samlingsnamn för de organisationer som direkt eller indirekt arbetar med hälso- och sjukvård. Exempel är landstingsägda sjukhus, privatägda läkarhus. Se också vård och omsorg.

Identitetscertifikat: Certifikat utfärdat till fysisk person. Certifikatet innehåller en omisskännlig identitet, t.ex. personnummer.

Kryptering: Processen att omvandla tolkningsbar information (klartext) till krypterad information. Syftet med den krypterade informationen är att den inte skall kunna tolkas av någon som inte innehar exakt rätt nyckel (vid symmetrisk kryptering) eller exakt rätt privat nyckel (vid asymmetrisk kryptering) som krävs för att korrekt dekryptera informationen.

Lokal RA: En funktion som av RA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt därtill hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärrning, nyckelgenerering mm.

Logg: En sekventiell och obruten lista över händelser i ett system eller en process. En typisk logg innehåller loggposter för enskilda händelser vilka var och en innehåller information om händelsen, vem som initierade den, när den inträffade, vad den resulterade i etc.

LRA-område: Den del av en organisation inom vilken en LRA har rätt att utfärda certifikat.

Nyckelinnehavare: I detta sammanhang en person, en organisation, en organisatorisk enhet eller en funktion som innehar exklusiv kontroll av den privata nyckel vars publika motsvarighet certifieras i ett certifikat.

Omisskännlig identitet: En identitet bestående av en uppsättning attribut som på ett omisskännligt sätt relaterar till en specifik person. Den omisskännliga kopplingen mellan identiteten och personen kan vara beroende på sammanhang inom vilka identitetsbegreppen hanteras. Vissa av dessa sammanhang kan kräva hjälp från aktuell registerhållare av olika attribut.

Organisation: Juridisk person som bedriver vård och omsorg, eller som är inblandad i säkert informationsutbyte med sådan juridisk person.

Policy: på principer grundat handlande [SAOL] eller grundprinciper för ett företags eller en organisations handlande [NSVO]. I detta dokument avses principerna, inte själva handlandet, samt syftar man här antingen på RA-policy eller på CA-policy.

Privat nyckel: Den privata delen av ett nyckelpar som används inom asymmetrisk kryptering. Den privata nyckeln används främst för att skapa digitala signaturer samt för dekryptering av krypterad information.

Publik nyckel: Den publika delen av ett nyckelpar som används inom asymmetrisk kryptering. Den publika nyckeln används främst för att verifiera digitala signaturer samt för att kryptera information.

RA: En part som av CA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt därtill hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärrning, nyckelgenerering mm.

RAPS: En dokumentation av hur en RA tillämpar en RA-policy.

Registration Authority: Se RA.

Registration Authority Practice Statement: Se RAPS.

Spärrlista: En digitalt signerad lista över spärrade certifikat.

Spärrning: Processen att spärra ett certifikat genom att lägga in information om certifikatet i en spärrlista.

Skriftlig: Där denna policy specificerar att information skall vara skriftlig, tillgodoses detta krav generellt även av digitala data under förutsättning att dess informationsinnehåll är tillgängligt på ett sådant sätt att det är användbart för involverade parter.

Uppdragsgivare: Den organisation inom vård och omsorg som genom avtal ger i uppdrag till en CA att utfärda certifikat för organisationens anställda, vårdgivare som arbetar på organisationens uppdrag samt organisatoriska enheter och funktioner.

Verifiering: Processen att säkerställa att ett antagande är korrekt. Detta begrepp avser främst processen att säkerställa att en digital signatur är framställd av den som av den signerade informationen framstår som dess utställare.

Vård och omsorg: Samlingsnamn för de organisationer som direkt eller indirekt arbetar med vård och omsorg. Exempel är landstingsägda sjukhus, privatägda läkarhus, äldrevård i kommunal regi och kommunal omsorgsverksamhet. Jfr hälso- och sjukvård.

FÖRKORTNINGAR

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List, på svenska spärrlista
eID	Elektroniskt ID-kort
HCC	Healthcare Certificate eller Hälso- och sjukvårdscertifikat, certifikat för svensk vård och omsorg. se [HCC]
HSA	Hälso- och sjukvårdens adressregister [HSA]
IDC	Identitetscertifikat
LRA	Lokal RA
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RAPS	Registration Authority Practice Statement
SEIS	Säker Elektronisk Information i Samhället
SITHS	Säker IT i Hälso- och sjukvården

1 INLEDNING

1.1 ÖVERSIKT

Denna policy beskriver de procedurer och rutiner som tillämpas vid registrering av uppgifter och upprättande av underlag för certifikat för personer, organisationer och funktioner inom vård och omsorg i Sverige, s.k. Health Care Certificates (HCC) eller hälso- och sjukvårdscertifikat.

Denna policy skall kompletteras med ett s.k. Registration Authority Practice Statement, RAPS, som beskriver hur policyn tillämpas inom organisationen.

Organisationen är skyldig att avsätta tillräckliga resurser, personella och monetära, för att kunna fullgöra sina åtaganden enligt denna policy.

I bilaga 3 till denna policy finns en översiktlig beskrivning av relationerna mellan certifikatutfärdaren (CA), registreringsansvarig (RA), s.k. lokala registreringsansvariga (LRA) och den vård och omsorgsorganisation för vilken certifikat avses utfärdas, här kallad uppdragsgivaren.

1.2 MÅLGRUPPER OCH TILLÄMPLIGHET FÖR RA-POLICY

1.2.1 CERTIFICATION AUTHORITY (CA)

CA är en organisation som genererar och ger ut HC-certifikat. CA arbetar i enlighet med en CA-policy för HCC.

1.2.2 REGISTRATION AUTHORITY (RA)

RA åtar sig att tillämpa denna RA-policy inom den egna organisationen i enlighet med en särskilt fastställd tillämpningsanvisning kallad Registration Authority Practice Statement (RAPS).

RAPS skall bl.a. återspegla organisationens struktur.

Den organisation som tecknar avtal med CA utser en RA och delegerar till RA ansvar och befogenheter för att fullfölja kraven enligt CA-policy. Organisationen ansvarar för att RAPS utarbetas för tillämpning av RA-policy.

1.2.3 RA:S ÅTAGANDE

RA beställer, utlämnar och spärrar certifikat för följande typer av nyckelinnehavare:

Typ av nyckelinnehavare	Certifikatstyp	Certifikatsform
Person med IDC	Person HCC	Sekundärcertifikat
Person utan svenskt personnummer	Person HCC	Primärcertifikat
Person utan IDC (reservkort)	Person HCC	Primärcertifikat
Organisation	Organisation HCC	Primärcertifikat
Organisationsenhet	Organisation HCC	Primärcertifikat
Verksamhetsfunktion	Funktion HCC	Primärcertifikat
System eller tjänst	Funktion HCC	Primärcertifikat

Oberoende av vilken typ av certifikat som utfärdas gäller att alla uppgifter som ingår i certifikatet ska kunna verifieras.

Beskrivning av certifikatstyp framgår av CA-policy kapitel 1.3.3.

Certifikatsinnehåll framgår av CA-policy kapitel 3.1.

Parter och avtal kring CA- och RA-policy framgår av Figur 3 i Bilaga 2.

1.2.4 TILLÄMPLIGHET

RA-policyn är relevant för:

- Organisationer som CA och RA ska betjäna
- Den CA som RA har avtal med
- Utsedd RA
- Av RA eventuellt utsedd LRA
- Organisation som svarar för hälso- och sjukvårdskatalog (HSA) och dess innehåll
- IT-infrastukturorganisation (i förekommande fall)
- Arkiveringsorganisation (i förekommande fall)
- Nyckelinnehavare

1.3 IDENTIFIERING

De rutiner och åtaganden som finns i denna RA-policy är tillämpliga i samband med certifikat där nedanstående CA-policy gäller.

CA-policynamn `{SE-SITHS-CA-Policy-2}.`
Objektidentifierare (OID) `{1.2.752.74.1.1.2}.`

Denna RA-policy har namn och identifikation enligt nedan.

RA-policynamn `{SE-SITHS-RA-policy-2}`
Objektidentifierare (OID): `{1.2.752.74.1.2.2}`

1.4 KONTAKTUPPGIFTER

1.4.1 ADMINISTRATIONSANSVARIG

Organisationen är ansvarig för förvaltning, administration och tillämpning av denna RApolicy.

1.4.2 KONTAKTPERSON

Frågor, synpunkter och förslag rörande denna RA-policy skickas till:

Organisation: Carelink AB
Adress: Box 12713
Postnummer: 112 94
Ort: Stockholm
Telefon: 08/650 62 10
Fax: 08/650 26 42
E-post: carelink@carelink.se
Web: www.carelink.se

2 ALLMÄNNA VILLKOR

2.1 FÖRPLIKTELSER

2.1.1 FÖRPLIKTELSER FÖR RA GENTEMOT CA

RA åtar sig i enlighet med denna policy:

- att samla in och verifiera uppgifter till HCC
- att beställa HCC från CA
- att lämna ut privata nycklar i förekommande fall
- att skicka begäran om spärrning av HCC till CA
- att tillhandahålla elektronisk katalog för förvaring av HCC och spärrlistor för HCC
- att tillse att arkivering sker enligt kapitel 4 nedan
- att i övrigt följa CA-policyn i de delar som anges nedan.
- att utformning av uppgifter till HCC görs enligt kapitel 1.3 i CA-policy
- att regler för certifikatbeställning följs enligt kapitel 3 och 4 nedan
- att rutiner vid utlämnande av privata nycklar följs enligt kapitel 3 nedan (gäller enbart organisations- och funktions HCC)
- att specifikationer av certifikatsinnehåll är giltiga med avseende på certifikatstyp, enligt kapitel 1 ovan och avseende uppgifter om nyckelinnehavare, enligt kapitel 3 nedan
- operationella krav enligt kapitel 4.

2.1.2 FÖRPLIKTELSER AVSEENDE LRA

RA har följande förpliktelser avseende sina LRA:

- att upprätta och följa rutiner för LRA, t.ex. för arkivering och loggning
- att upprätta och följa rutiner för hantering av LRA:s certifikat vid utbyte av person som innehar ett LRA-uppdrag
- att LRA-organisationen är bemannad med personer som har adekvat utbildning och tid avsatt för uppgiften

2.1.3 REGLER OCH RUTINER SOM SKALL INGÅ I RAPS

Följande regleras i separat dokument som upprättas av uppdragsgivaren och godkänns av CA i samband med tecknande av avtal mellan uppdragsgivaren och CA:

- rutiner beträffande utlämnande och mottagande av certifikat
- reservrutiner
- regelverk för verifiering av alla uppgifter som RA lämnar till CA
- regler beträffande kataloguppgifternas kvalitet, aktualitet samt krav på kataloghistorik gentemot den som ansvarar för lagring av certifikat i katalog enligt policy för HSA [HSApolicy].

2.1.4 FÖRPLIKTELSE FÖR NYCKELINNEHAVARE

Nyckelinnehavare som tilldelas HCC förpliktigar sig att:

- vid beställning, mottagande och spärrning av HCC (person-, organisations- och funktions-) uppfylla sin del i registrerings- och identifieringsprocesser enligt CA-policy kapitel 3 och 4
- som nyckelinnehavare för organisations HCC och funktions HCC ansvara för att den privata nyckel inte används för annat än de syften och ändamål som den är utfärdad för
- som nyckelinnehavare för organisations HCC och funktions HCC skydda den privata nyckeln i enlighet med CA-policy kapitel 2.

2.2 ANSVAR

2.2.1 RA:S ANSVAR INOM UPPDRAGSGIVARENS ORGANISATION

RA ansvarar inom sin uppdragsgivares organisation för:

- att CA-policy följs i tillämpliga delar
- att RA-policy följs
- att LRA-arbetsplatser finns i sådan omfattning att man har lokal kännedom om de personer vars HCC man administrerar via arbetsplatsen
- att ekonomiska resurser finns avsatta för införande och användning av HCC
- att informationssäkerhet, tillgänglighet, sekretess, riktighet och spårbarhet, tillgodoses vid användning av HCC, inkluderande katastrofplan
- att kvalitetssäkring av användningen av HCC görs genom regelbunden kontroll och uppföljning
- att arkivering sker enligt CA-policy kapitel 4 och enligt den egna organisationens regler
- att uppgifterna i ett utfärdat certifikat är kontrollerade och korrekta i enlighet med CA-policy kapitel 3 och 44.

2.2.2 FRISKRIVNINGAR

RA ansvarar inte för följder eller skada av:

- att någon nyckel ändras på otillbörligt sätt
- att nyckelinnehavare använder certifikat på otillbörligt sätt
- felaktigheter i CA:s certifikatsutfärdande.

2.3 TOLKNING OCH VERKSTÄLLIGHET

Vid tolkning av denna policy och vid bedömning av RA:s agerande i samband med certifikatshantering inom organisationen enligt denna policy skall svensk lag tillämpas.

Denna policy ska vara tillgänglig för berörda parter med angivande av datum för publicering och versionsbeteckning.

2.4 ÅTKOMSTKONTROLL

Certifikat och spärrlistor skall publiceras i enlighet med vård och omsorgsorganisationens bestämmelser vilket bl.a. regleras i gällande katalogpolicy (HSApolicy).

2.5 REVISION

RA genomför löpande intern revision för att belägga att denna policy efterlevs.

Vid upptäckt av brister eller behov av förändringar skall RA vidta lämpliga åtgärder i form av att förändra tillämpade rutiner och/eller initiera uppdatering av denna policy.

Om denna policy uppdateras på sådant sätt att den nya policyn bedöms medföra en förändrad säkerhetsgrad så utgör detta inte en versionsuppdatering utan upprättande av en ny policy.

2.6 KONFIDENTIALITET

Frågan om konfidentialitet beträffande uppgifter om den vård och omsorgspersonal för vilka certifikat utfärdas regleras av bl. a. i tryckfrihetsförordningen, sekretesslagen och lagen om yrkesverksamma inom hälso- och sjukvårdsområdet (LYHS).

Denna policy skall tillämpas så att gällande lag om konfidentialitet uppfylls.

2.7 AVTAL/ÖVERENSKOMMELSER

2.7.1 AVTAL MED CA

Organisation som avser att använda HCC ska sluta avtal med CA angående förpliktelser, ansvar etc.

I avtalet skall ingå att RA skall följa CA-policy och former för samverkan ska fastställas.

2.7.2 ÖVERENSKOMMELSE MED DEN ORGANISATION SOM RA OCH LRA TILLHÖR

Följande dokumenterade överenskommelser/beslut skall finnas inom den organisation som RA resp. LRA tillhör avseende den verksamhet som RA respektive LRA bedriver:

- överenskommelse/beslut avseende krav och skyldigheter för RA
- överenskommelse/beslut med LRA-s verksamhetschef (i enlighet med organisationens beslutsordning)
- överenskommelse/beslut med ansvariga för organisationens IT-infrastuktur
- överenskommelse/beslut med ansvariga för katalog i enligt med organisationens beslutsordning
- överenskommelse/beslut med arkivansvarig.

3 IDENTIFIERING OCH AUTENTICERING

3.1 IDENTIFIERING VID REGISTRERING

3.1.1 ALLMÄNT

Vad gäller identifiering och autenticering vid beställning av HCC skall RA följa CA-policy, avsnitt 3.1.

3.1.2 IDENTIFIERINGSPROCEDUR GENOMFÖRD AV RA/LRA

RA ska tillse att det finns rutiner beskrivna och fastställda beträffande:

- kontroll av behörig beställare av certifikat
- upprättande av underlag för certifikatsbeställning
- utlämning och spärrning av certifikat.

RA/LRA skall upprätta underlag för certifikatsbeställning verifierade mot adekvat ansökan beslutad av verksamhetsansvarig.

Vid certifikatsbeställning görs identitetskontroll enligt någon av nedanstående procedurer:

- vid person HCC genom personlig närvaro och med eID-kort som underlag vid första beställningstillfället av ett certifikat, vid efterföljande certifikatsbeställningar behövs ej någon personlig identifiering eftersom personen är elektroniskt känd
- vid organisations HCC och funktions HCC genom personlig närvaro av behörig representant som uppvisar godkänd och giltig legitimationshandling vid första tillfället.

3.1.3 KRAV PÅ PERSONLIG NÄRVARO

RA/LRA utlämnar privata nycklar samt tillämpliga lösenord eller PIN-koder vid organisations HCC och funktions HCC. Utlämnandet sker personligen till behörig representant mot uppvisande av godkänd och giltig legitimation.

Dessa rutiner beskrivs närmare i RAPS.

3.1.4 AUTENTICERING AV ORGANISATION OCH FUNKTION INOM EN ORGANISATION

Vid beställning av certifikat av typerna organisations HCC och funktions HCC, samt vid distribution av privata nycklar och koder kopplade till dessa ska finnas en ansökan från behöriga representanter inom organisationen.

Behöriga representanter specificeras alltid i organisationens avtal med CA. Där framgår i vilka avseende dessa representanter har rätt att företräda organisationen.

3.2 BEGÄRAN OM SPÄRRNING AV CERTIFIKAT

Spärrning av certifikat kan initieras av:

- organisationen genom initiativ från RA/LRA (t.ex. då anställning upphör; organisation förändras)
- ~~certifikatsinnehavaren (t.ex. vid förlust av mot certifikat svarande personlig nyckel)~~
- RA t.ex. vid misstanke om missbruk av certifikat eller nycklar
- CA enligt CA-policy kapitel 4.4.1.

Rutiner och reservrutiner vid spärrning av certifikat ska beskrivas i RAPS.

4 OPERATIONELLA KRAV

De operationella kraven reglerar:
- beställning av certifikat
- utlämnande av certifikat och i vissa fall nycklar och koder
- spärrning av certifikat.

Dessa uppgifter för RA eller LRA skall beskrivas mer detaljerat i RAPS.

Denna policy definierar de operationella krav som rör:
- CA
- organisationen
- RA-organisationen inklusive (eventuella) LRA
- katalogorganisationen
- organisationen som ansvarar för IT-infrastruktur
- arkiveringsorganisationen.

4.1 BESTÄLLNING AV CERTIFIKAT

Vid beställning av HCC genomförs följande:

- verksamhetsansvarig beslutar vilka som ska ha certifikat.
- verksamhetsansvarig eller av denne utsedd person fyller i, undertecknar och signerar ett beställningsunderlag. Därvid accepterar nyckelinnehavaren CA-policyns krav på certifikatsanvändning. I denna process uppger verksamhetsansvarig samtliga relevanta uppgifter enligt CA-policy och RAPS.
- inkommen beställningen kontrolleras av RA/LRA (nyckelinnehavarens lämnade personuppgifter verifieras t.ex. mot PA-system, befolkningsregister, socialstyrelsens Yrkesregister). RA/LRA beställer certifikat hos CA.
- beställningshandlingar arkiveras enligt RAPS.

4.2 UTLÄMNANDE AV CERTIFIKAT

Utfärdandet av ett certifikat representerar CA:s acceptans av RA/LRAs beställning.

Vid utlämnande av organisations HCC och funktions HCC fullföljs följande moment:

- RA/LRA mottar certifikat samt privata nycklar och koder/lösenord från CA
- RA/LRA ansvarar för att utlämnandet av certifikat, privata nycklar och koder sker vid personlig kontakt med nyckelinnehavare och att denne identifieras enligt CA-policy kapitel 3.1.

4.3 SPÄRRNING AV CERTIFIKAT

- Spärrning av HCC kan beslutas av verksamhetsansvarig.
- RA/LRA ombesörjer och ansvarar för att spärrningsbegäran skickas till CA.
- ~~Nyckelinnehavare kan begära spärrning, av HCC direkt till CA enligt CA-policy. I detta fall åligger det nyckelinnehavaren att snarast informera RA/LRA om att spärrning har begärts.~~
- Orsaker till spärrning regleras och beskrivs i CA-policy och RAPS.
- RA/LRA ansvarar för att verksamhetsansvarig och nyckelinnehavare informeras om spärrning av HCC i enlighet med CA-policy.
- Spärrningsbegäran från RA/LRA skall ske enligt CA-policy 4.4.3.

4.4 PROCEDURER FÖR SÄKERHETSREVISION AV LRAARBETSPLATSER

För LRA-arbetsplatser som finns inom RA-organisationen kopplade till CA ska CA-policyns krav på säkerhetsrevision i kapitel 4.5 följas.

4.5 ARKIVERING

- Den information som lagras hos CA arkiveras enligt CA-policyn kapitel 4.6.
- LRA ansvarar för att arkivera beställningsunderlag och annan certifikatsdokumentation som inte lagras hos CA.
- Arkiveringskrav beskrivs i enlighet med verksamhets- och CA-krav, i RAPS.
- RA ställer som krav att organisationen måste kunna överta/garanteras åtkomst till sin egen information i CA:s arkiv ifall inte CA uppfyller kraven på lagring inom vård och omsorg.

Alternativt kan annat dokumentationssätt finnas inom organisationen (ex. loggar) som uppfyller kraven på lagring.

4.6 PLANERING FÖR KATASTROF

Katastrofplan skall finnas framtagen i enlighet med organisationens övriga krav på katastrofberedskap. Katastrofplanen för RA och LRA skall vara en del av RAPS.

Vid kompromettering av CA-nyckel skall RA informera sin organisation enligt CA-policy.

4.7 UPPHÖRANDE AV RAORGANISATION

Vid upphörande av RA/LRA organisationen åligger det RA att avveckla organisationen enligt följande procedurer:

- specifikt informera alla nyckelinnehavare och alla parter som RA har avtal och/eller överenskommelser med i enlighet med de krav på förvaringstid som återfinns i gällande avtal och överenskommelser
- avsluta alla rättigheter för RA-organisationen/avveckla RA-organisationen
- tillse att alla arkiv och loggar bevaras under angiven bevaringstid samt i enlighet med angivna föreskrifter.

Det åligger RA att inneha garantier för medel som täcker alla kostnader för åtgärderna under föreskriven tid.

5 FYSISK, PROCEDURORIENTERAD OCH PERSONALORIENTERAD SÄKERHET

5.1 FYSISK SÄKERHET

RA/LRA skall uppfylla krav på fysisk säkerhet enligt CA-policyn 5.1.4 vilken beaktar lokalens läge, skalskydd och media.

Vid identifiering av nyckelinnehavare, vid ansökan som kräver personlig närvaro, samt vid utlämnande av nycklar och koder skall den fysiska säkerheten beaktas så att inga uppgifter röjs för obehörig.

5.2 PROCEDURORIENTERAD SÄKERHET

RA ansvarar i enlighet med 2.1.1 ovan (förpliktelser) för alla procedurer och förhållanden som definieras i detta avsnitt. Detta innefattar allt från beställning, utlämnande och spärrning samt därtill hörande administrativa funktioner

RA kan dock välja att dela upp ansvaret för ovan angivna förpliktelser genom att skapa en egen organisation.

RA-organisationen omfattar företrädare för organisationen avpassade efter RA:s arbetsuppgifter:

- RA
- LRA
- Informationssäkerhetsansvarig.

5.3 PERSONALORIENTERAD SÄKERHET

RA- och LRA-organisationen ska bemannas med ansvarsfulla personer som uppvisat lämplighet för en sådan befattning Dessa personer får inte inneha annan befattning som kan bedömas stå i konflikt med RA/LRA-uppdraget.

Alla företrädare för organisationen skall genomgå utbildning och erhållit den praktik som krävs för att på ett säkert sätt utföra sina arbetsuppgifter inom ramen för denna RA-policy och inom ramen för gällande informationssäkerhetspolicy. Utbildning ska genomföras kontinuerligt.

6 TEKNIKORIENTERAD SÄKERHET

6.1 GENERERING OCH INSTALLATION AV NYCKELPAR

Ej tillämpligt för RA.

6.2 UTLÄMNANDE AV PRIVAT NYCKEL TILL NYCKELINNEHAVARE VID ORGANISATION OCH FUNKTION HCC

Nycklar och eventuella koder utlämnas, enligt gällande avtal med CA, till nyckelinnehavare eller behörig representant för nyckelinnehavaren sedan denne identifierat sig i enlighet med 3.1.4.1 i CA-policy.

Mottagande av nycklar och koder kvitteras. Kvittens ska sparas enligt gällande arkiveringsregler.

6.3 SKYDD AV PRIVAT NYCKEL

Privata nycklar skall förvaras och distribueras på ett säkert och skyddat sätt så att de inte kan falla i orätta händer samt att de inte i något fall exponeras eller brukas på otillbörligt sätt, innan de nått rätt mottagare.

6.4 ARKIVERING AV PRIVATA NYCKLAR

Inga nycklar arkiveras.

6.5 SÄKERHET I DATORSYSTEM

Hela RA-systemet skall vara uppbyggt på ett sådant sätt att betrodda företrädare för RA-organisationen, enligt 5.2 ovan, kan isoleras och separeras i systemet.

Det accesskontrollsystem som används skall vara så konstruerat att varje företrädare för organisationen identifieras på individuell nivå.

För att åstadkomma isolering och separering av företrädare för organisationen vid åtgärder på OS-nivå används dubbelbemanning.

Anslutning av RA-klienter ska ske i enlighet med bestämmelserna i CA:s CPS.

6.6 SÄKERHET I SAMVERKAN MELLAN CA OCH RA/LRA

Se avsnitt om hur CA och RA kopplas samman i kapitel 6 av rapporten ”Implementering av hälso- och sjukvårdscertifikat” [HCC].

7 REFERERADE DOKUMENT

[CApolicy] * **SITHS. Certifikatpolicy för utfärdande utgivande av certifikat inom vård och omsorg.** Version 2003-03-01. Carelink.

[HCC1A] * **Certifikat för svensk vård och omsorg. HCC.** Version 1A. Carelink 2002-12-13.

[HSApolicy] * **Policy för elektronisk katalog inom svensk vård och omsorg.** Version 1. Carelink 2001-08-31.

[IMPL] * **Implementering av hälso- och sjukvårdscertifikat.** Version 1. SITHS-projektet mars 2000.

[INFRA] * **Infrastruktur för informationssäkerhet i hälso- och sjukvården.** Version 1. SITHS-projektet mars 2000.

[ITS6] Mats Ohlin: Terminologi för Informationssäkerhet Rapport ITS 6. Informationstekniska standardiseringen, mars 1994.

[NSVO] **Norstedts stora svenska ordbok.**

[Posten] **Tjänster för elektronisk Identifiering.** Posten Sverige AB. Statskontoret februari 1999. Ramavtal nr 6422/99.

[RAPSmall] * **SITHS RAPS**

[SEIS] **SEIS –S10 98/98. SEIS Certificate Policy SeisS10-1:1.0 and related policies.** High assurance general ID-certificate with private key protected in an electronic ID-card. Approved 1998-06-16.

[SAOL] **Svenska Akademins Ordlista.**

[SÄKBRP] * **Begrepp för IT-säkerhet.** Version 1. SITHS-projektet november 1999.

[Vårdproc] * **Informationssäkerhet i vårdprocessen.** Krav beskrivna i generella användningsfall utifrån vårdscenarios. Rapport nr 1 från SITHS-projektet. Mars 2000.

* senaste version finns tillgänglig på Carelinks hemsida www.carelink.se.

Bilaga 1. PARTER VID UTGIVNING AV HCC

Denna bilaga är endast informativ och syftar till att klargöra relationerna mellan de parter som är inblandade vid utgivningen av HCC.

Vi har följande parter:

- **CA,** den organisation som utfärdar certifikat.
- **Nyckelinnehavare,** den som certifikatet utfärdats för, kan vara anställd inom vård och omsorg men kan även vara en organisationsenhet eller en funktion inom vård och omsorg.
- **Uppdragsgivare,** den vård och omsorgsorganisation (en juridisk person) som nyckelinnehavaren tillhör.
- **RA,** den funktion som registrerar och verifierar de uppgifter som ska ingå i certifikatet.
- **Lokal RA-funktion,** LRA, funktion som på uppdrag av RA författar certifikatsbegäran och kommunicerar med CA. LRA kan vara en del av RA eller vara en separat funktion/organisationsenhet.

Den part som ger ut certifikat kallas Certification Authority, CA, eller på svenska certifikatsutfärdare. Utgivningen av certifikat omfattar bl.a. följande moment:

a) Registrering och kontroll av de uppgifter som ska ingå i certifikatet. Detta omfattar främst uppgifter som säkert fastlägger identiteten på den som certifikatet avser, nyckelinnehavaren, samt två publika nycklar, en för autenticering/kryptering och en för signering (oavvislighet).
b) Generering av två nyckelpar; detta sker endast om det certifikat som ska utfärdas är ett primärt certifikat. I fallet med HCC gäller detta endast organisations HCC och funktions HCC.
c) Elektronisk signering av uppgifterna i certifikatet; detta görs med utfärdarens privata signeringsnyckel, s.k. CA-nyckel.
d) Publicering av certifikat i elektronisk katalog.
e) Distribution av certifikat (och eventuellt privata nycklar) till nyckelinnehavaren.
f) Mottagande av begäran om spärrning av certifikat samt publicering av spärrade certifikat i så kallade spärrlistor, eller Certificate Revocation List (CRL).

CA utfärdar certifikat enligt en särskild så kallad CA-policy. I certifikaten finns en unik identitet för den policy enligt vilken certifikatet utfärdats. För utgivning av HCC har SITHS-projektet utarbetat ett förslag till CA-policy [CApolicy]. Hur denna policy tillämpas ska beskrivas i särskild dokumentation. Den publika delen av denna dokumentation kallas Certification Practise Statement, CPS. (Vedertaget svenskt namn saknas).

Vissa delar av momenten a) till f) ovan kan ibland med fördel utföras av en särskild del av den utfärdande organisationen, denna del (och funktion) brukar kallas Registration Authority (RA).

Flera CA-policies anger specifikt att RA-funktionen kan utföras av annan organisation än CA, men på CA:s uppdrag och att CA i dessa fall bär samma ansvar som ifall RA-funktionen hade utförts av CA själv. I figur 1 nedan visas en konventionell CA med inbyggd RA-funktion.

HCC ska utfärdas för anställda inom vård och omsorg liksom för organisationsenheter och funktioner inom vård och omsorg. Detta gör att de funktioner som man normalt förknippar med RA (främst a), e) och delar av f) ovan)) lämpligast utförs inom den beställande organisationen, uppdragsgivaren.

Vi får då en mera komplicerad struktur där RA-funktionen dels ska arbeta på uppdrag av CA på ett sådant sätt att CA kan ta fullt ansvar för RA:s arbete samtidigt som RA är en del av uppdragsgivarens organisation och måste följa de interna regler och anvisningar som finns i denna organisation. Avtalet mellan uppdragsgivaren och CA blir därför centralt. Detta avtal måste reglera åtagande och förpliktelser för de båda parterna. I detta regleras t.ex. hur uppdragsgivarens RA-organisation ser ut med avseende på antal LRA etc., hur denna organisation kan förändras och hur detta ska meddelas CA. Bilagor till ett sådant avtal kan bl.a. vara:

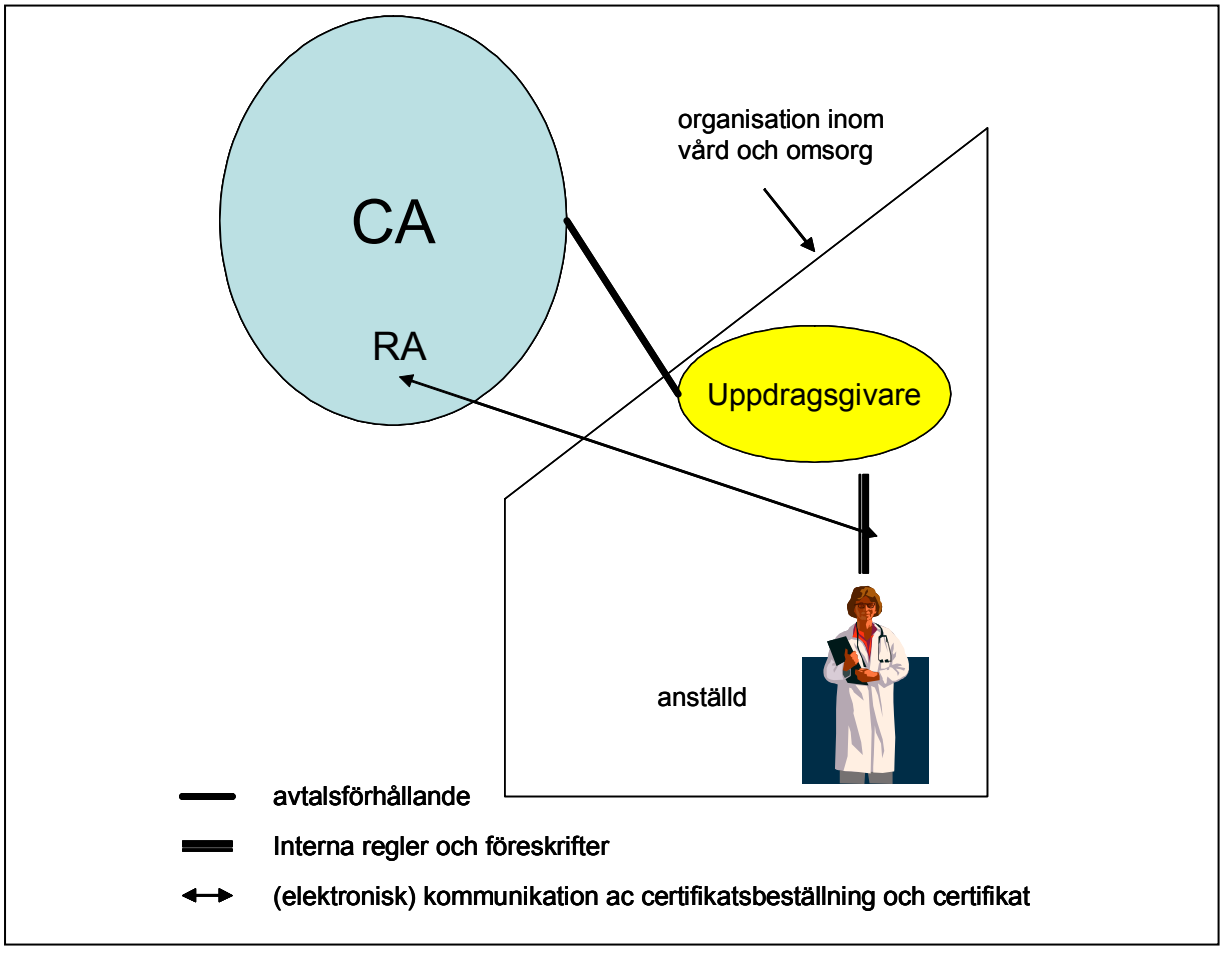
- CA-policy
  (Detta givetvis är den av SITHS föreslagna policyn [CA-policy]).

- CPS
  Denna utformas av CA. En central del i detta sammanhang är CA:s krav på hur RA/LRA ska fungera, t.ex. i fråga om autenticering av RA, upphörande etc.
- RA-policy
  Föreliggande dokument som framläggs av CA.
- RAPS
  Beskriver hur organisationen tillämpar RApolicyn och därmed möter de krav som ställs av CA i CA-policy och CPS. RAPS utformas av uppdragsgivaren. Här specificeras hur RA-organisationen med LRA är uppbyggd hos uppdragsgivaren. Undertecknat avtal mellan parterna betyder att CA accepterar RAPS och kan ta ansvar för RA-funktionen enligt CA-policyn.

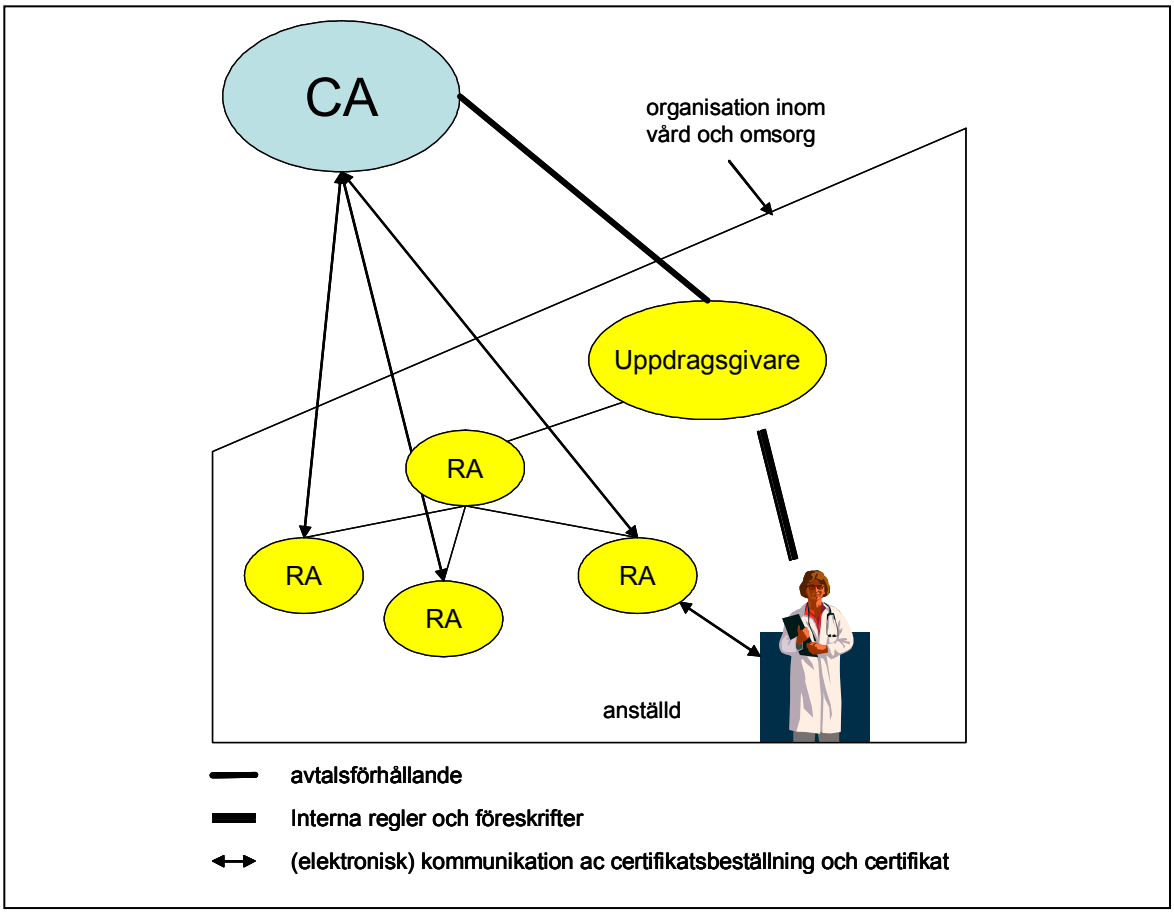
Eftersom RAPS är unik för varje uppdragsgivare har SITHS-projektet inte utarbetat något förslag till utformning och innehåll för detta dokument.

Avtal mellan den anställde och uppdragsgivaren måste, när den anställde får ett HCC, kompletteras med avtal (”nyckelinnehavareavtal”) som reglerar den anställdes förpliktelser i samband med HCC. Mall för detta avtal ska vara en del av innehållet i RAPS.

Vid utgivning av organisations HCC och funktions HCC ersätts nyckelinnehavareavtalet ovan med ett internt reglemente som reglerar organisationens/funktionens förpliktelser i samband med erhållande av HCC. Mall för detta reglemente ska vara en del av innehållet i RAPS.

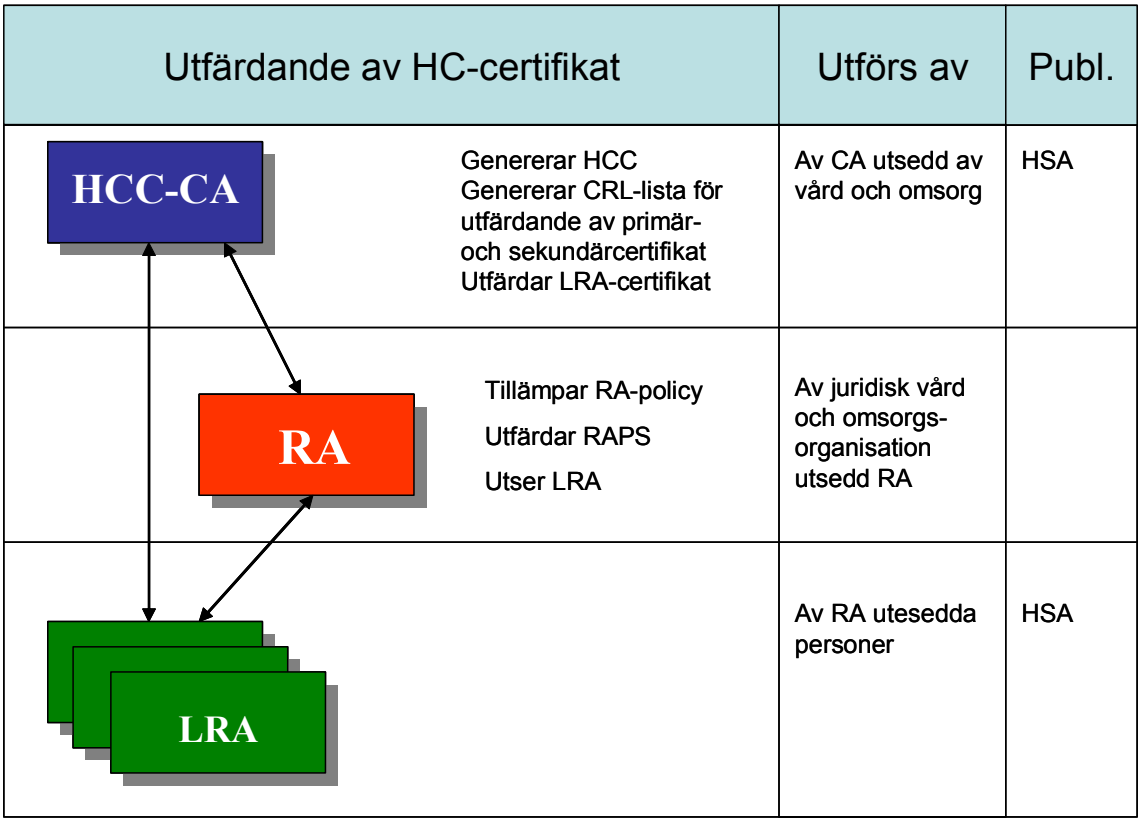


Figur 1. ”Konventionell” CA med inbyggs RA-funktion.



Figur 2. CA/RA-organisation föt utgivning av HCC.

Bilaga 2. GENERELL MODELL FÖR CERTIFIKAT OCH POLICY



Figur 3. Utfärdande av HCC.

Carelink ska öka samverkan samt sätta igång och stödja utvecklingsinsatser på IT-området inom vård och omsorg. Carelink Intresseförening och Carelink AB bildades I slutet av år 2000 av Landstingsförbundet, Svenska Kommunförbundet, Privatvårdens Arbetsgivarförbund och Apoteket AB.

care link
Carelink – Svenskt Nätverk för Kommunikation I Vården
BOX 12 713· 112 94 Stockholm · BESÖKSADRESS Hantverkargatan 7
TEL +46 8 452 71 40
www.carelink.se · E-POST Carelink@carelink.se