Policy

SITHS

Certifikatspolicy för utgivande av certifikat inom vård och omsorg

Version 2003-03-01

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

Certifikatpolicy för utfärdande av certifikat inom vård och omsorg (HCC).

INNEHÅLLSFÖRTECKNING

Certifikatpolicy för utfärdande av certifikat inom vård och omsorg (HCC)

Detta dokument innehåller SITHS 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 [HCC] 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 1.2.

SEIS Certificate Policy SEIS – S10, [SEIS] och den svenska version som utgivits av Posten Sverige AB [Posten] har varit utgångspunkterna vid framtagandet av denna policy.

Denna certifikatpolicy kräver upprättande av ett separat CPS. Den förutsätter också att lokala ”Registration Authorities”, RA upprättas och att dessa arbetar enligt en särskild RA-policy [RA-policy].

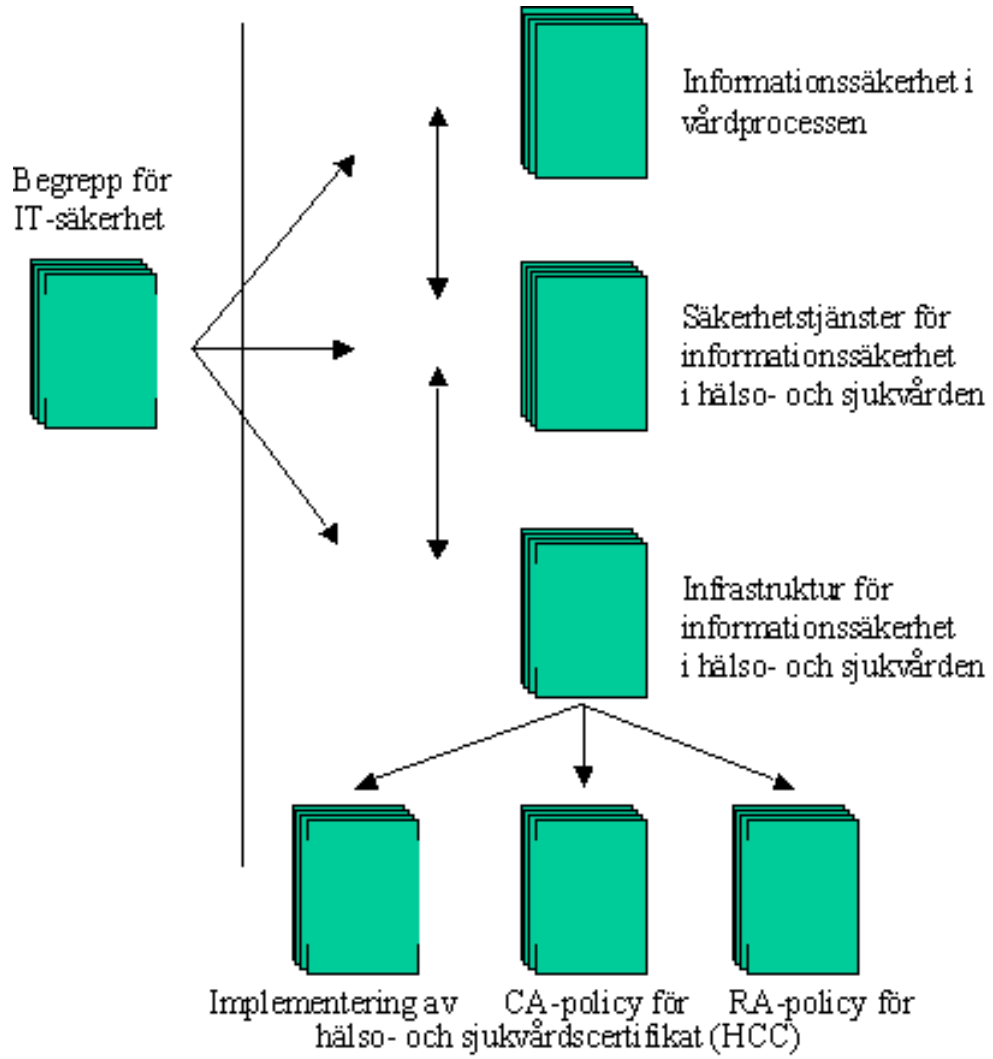
Detta dokument ägs och förvaltas av Carelink AB.

Revisionshistorik

Version	Status
2000-02-25	Första färdiga förslaget presenterat vid ett SITHS-seminarium 2000-03-15.
2000-05-15	Slutligt förslag från SITHS-projektet.
2000-05-15A	Carelinks utgåva av SITHS-projektets förslag. Denna utgåva innebär ingen förändrad säkerhetsgrad. Endast formella ändringar om identifiering av policyn, ägarskap och kontaktpersoner har gjorts enligt följande: 1.2 Policynamn och OID införda 1.4.1 Carelink AB infört 1.4.2 Kontaktuppgifter för Carelink införda 2.9 Kontaktuppgifter för Carelink införda 8.1 Carelink AB infört
2003-03-01	Carelinks andra utgåva av SITHS-policyn, fastställd av SITHS förvaltningsgrupp 18 februari 2003. Denna version innehåller två väsentliga förändringar: • tillämpligheten har vidgats (avsnitt 1.3.4) • spärrning har begränsats (avsnitten 3.4, 4.4.2 och 4.4.3) Slutligen så har genomgående begreppet ”hälso- och sjukvård” bytts ut mot det mer omfattande begreppet ”vård och omsorg” vilket även innefattar kommunal verksamhet.

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].

Applikation: IT-tjänst eller IT-tillämpning.

Asymmetrisk krypteringsalgoritm: En krypteringsteknik som utnyttjar två relaterade transformeringsalgoritmer, en publik transformering, med användande av en publik nyckel, och en privat transformering med användande av en privat nyckel. De två transformeringarna har den egenskapen att om man känner den publika transformeringen är det matematiskt omöjligt att ur denna härleda den privata transformeringen.

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.

Bascertifikat: Se primärcertifikat.

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.

Certification Authority: Se CA.

Certification Practice Statement: Se CPS.

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

Certifikatextensioner: Del av certifikatinnehåll specificerat av standarden X.509 version 3.

Certifikatskedja: Kedja med certifikat där delarna i kedjan är CA-certifikat för CA som korscertifierat varandra. Vid verifiering av ett certifikat, följs kedjan tills en betrodd CA hittats.

Certifikatsnivå: Det finns certifikat på två nivåer, primärcertifikat och sekundärcertifikat.

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

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 identitetskontroll: Identitetskontroll som kan göras utan att den, vars identitet kontrolleras, är personligen närvarande.

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

Förlitande part: En mottagare av ett certifikat som förlitar sig på detta certifikat vid autenticering, verifiering av digitala signaturer och/eller kryptering av information.

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.

Katalogtjänst: Databastjänst som i detta dokument avser en databas som struktureras enligt standarden X.500.

Korscertifiering: Processen där en CA utfärdar ett certifikat för en annan CA:s publika CA-nyckel.

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.

Kryptografisk modul: En enhet i vilken krypteringsnycklar lagras tillsammans med en processor som kan utföra kritiska kryptografiska algoritmer. Exempel på kryptografisk modul är EID-kort och diskett.

Lagringsmodul: I detta dokument avses kryptografisk modul.

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.

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.

Oavvislighetstjänster: Tjänster vars syfte är att binda en nyckelinnehavare vid ansvar för signerade meddelanden på ett sådant sätt att det kan verifieras av en tredje part vid senare tidpunkt.

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.

Operatör: Anställd hos CA.

Policy: I detta dokument synonymt med certifikatpolicy.

Primärcertifikat: Ett certifikat, som utfärdats på grundval av identifiering av nyckelinnehavaren på annat sätt än att denne företett ett annat certifikat. Identifieringen sker då vanligtvis genom att nyckelinnehavaren istället företer en identitetshandling.

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. Förkortning av Registration Authority.

RA-policy: En namngiven uppsättning regler för RA:s roll i framställning, utgivning och spärrning av certifikat och som reglerar tillämpligheten av certifikaten inom ett specifikt användningsområde.

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

Registration Authority: Se RA.

Registration Authority Practice Statement: Se RAPS.

RSA: Namn på en specifik asymmetrisk krypteringsalgoritm för kryptering med publika och privata nycklar, uppkallad efter matematikerna Rivest, Shamir och Adleman.

Sekundärcertifikat: Certifikat som utfärdas på grundval av ett annat certifikat, primärcertifikatet. Detta innebär att utfärdande CA litar på den CA som utgett primärcertifikatet, d.v.s. accepterar certifieringen av den publika nyckeln till nyckelinnehavaren, vilket i sin tur förutsätter tillit till att identifieringen av nyckelinnehavaren vid utfärdandet av primärcertifikatet är korrekt.

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.

Symmetrisk kryptering: Kryptosystem som kännetecknas av att både sändare och mottagare av krypterad information använder samma hemliga nyckel både för kryptering och dekryptering.

Tillförlitlig tredje part: Se TTP.

TTP: En part som två eller flera samverkande parter litar på. En TTP utför tjänster åt de samverkande parterna, såsom t ex tidsstämpling, certifikatsutgivning.

Uppdragsgivare: Den organisation inom hälso- och sjukvården 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*
CAA	Certification Authority Administrator
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
HSA	Hälso- och sjukvårdens adressregister [HSA]
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PKIX	Public Key Infrastructure (x.509) (IETF Working Group)
RA	Registration Authority*
RAPS	Registration Authority Practice Statement*
RO	Registration Officer
RFC	Request For Comments
RSA	Rivest – Shamir – Adleman, asymmetrisk krypteringsalgoritm*
SA	System Administrator
SEIS	Säker Elektronisk Information i Samhället
SIS	Swedish Institute of Standards
SMTP	Simple Mail Transfer Protocol
SO	Security Officer
TF	Tjänsteförvaltare
TTP	Tillförlitlig tredje part eller Trusted Third Party*

*se också definitionerna ovan.

1 INTRODUKTION

1.1 ÖVERSIKT

Denna certifikatpolicy beskriver de procedurer och rutiner som tillämpas vid utfärdande av certifikat för personer, organisationer och funktioner inom vård och omsorg i Sverige, s.k. Healthcare Certificates (HCC). [HCC]

Beskrivning av rutiner och organisationer för tillämpning av denna certifikatspolicy skall finnas i en separat s.k. Certification Practice Statement (CPS), publicerad av den CA som tillämpar denna policy.

Om den CA som tillämpar denna policy väljer att kontraktera Registration Authority (RA) för identifiering av nyckelinnehavare och insamling av egenskaper hos nyckelinnehavaren, skall denna RA arbeta enligt RA-policy och en av RA publicerad Registration Authority Practice Statement (RAPS) som beskriver rutiner och organisation för tillämpning av RA-policyn.

1.2 IDENTIFIERING

De rutiner och åtaganden som följer av denna certifikatpolicy är endast tillämpliga i samband med sådana certifikat där nedanstående policy åberopas.

Policynamn för denna policy är `{SE-SITHS-CA-Policy-2}`.

Objektidentifierare (OID) för denna policy är `{1.2.752.74.1.1.2}`.

1.3 MÅLGRUPP OCH TILLÄMPLIGHET

1.3.1 CERTIFICATION AUTHORITY (CA)

CA skall publicera ett CPS som innehåller referens till denna certifikatpolicy.

Organisation som ger ut certifikat enligt denna policy (CA) skall ha giltigt avtal med de vård- och omsorgsorganisationer på vilkas uppdrag certifikat utfärdas. Detta avtal skall referera till den CPS som tillämpas för att följa denna CA-policy.

CA är skyldig att inneha tillräckliga resurser i form av egna medel och försäkringar för att kunna fullgöra sina åtaganden enligt denna certifikatpolicy.

1.3.2 REGISTRATION AUTHORITIES (RA)

Samtliga anlitade RA skall arbeta efter RA-policy [RApolicy] och en till denna policy knuten RAPS. RA skall garantera att man till fullo uppfyller samtliga berörda krav i denna certifikatpolicy.

1.3.3 NYCKELINNEHAVARE

Slutanvändarcertifikat utfärdas till följande typer av nyckelinnehavare:

Typ av nyckelinnehavare	*Certifikatstyp*	*Certifikatsnivå*
Person	Person HCC	Sekundärcertifikat
Organisation	Organisation HCC	Primärcertifikat
Organisationsenhet	Organisation HCC	Primärcertifikat
Verksamhetsfunktion	Funktion HCC	Primärcertifikat
System eller tjänst	Funktion HCC	Primärcertifikat

1.3.3.1 Person HCC

Person HCC utfärdas endast till fysisk person som:

a) kan styrka en omisskännlig identitet vars uppgifter kan kontrolleras och styrkas av en tillförlitlig tredje part (TTP)

b) är anställd vid eller genom avtal kopplad till en organisation som antingen är en organisation inom vård och omsorg eller som har personal som är involverad i säkert informationsutbyte med organisationer eller vårdgivare inom vård och omsorg.

Person HCC utfärdade under denna certifikatpolicy kan omfatta olika typer av certifikat som certifierar olika typer av identitetsuppgifter. Gemensamt för dessa är att de identitetsuppgifter som certifieras skall forma en omisskännlig identitet som unikt identifierar en specifik fysisk person (inom organisationen).

Oberoende av vilken typ av certifikat som utfärdas gäller vidare att alla certifierade uppgifter skall kunna kontrolleras och styrkas av en tillförlitlig tredje part.

Person HCC utfärdas som sekundärcertifikat, dvs. med ett primärcertifikat som grund. Detta primärcertifikat förutsätts ha utgetts av en betrodd CA som samtidigt har gett ut ett EID-kort, där den privata nyckeln förvaras. Detta innebär att inga nycklar genereras för Person HCC enligt denna policy.

Utmärkande för Person HCC är att dessa innefattar ett namn på en person som är starkt knuten till en organisation.

1.3.3.2 Organisations HCC

Organisations HCC utfärdas endast till en organisation eller en enhet inom en organisation där:

a) certifikatet inte är associerat samtidigt med en fysisk person,

b) organisationen eller enheten finns registrerad i det land som anges för organisationen i certifikatet samt att organisationens fullständiga registrerade namn certifieras i certifikatet.

I det fall certifikat utfärdas till enhet som inte är egen juridisk person, skall ansvarig juridisk person under vilken enheten underställs finnas representerad med fullständigt namn i den information som certifieras i certifikatet.

Den organisation eller enhet inom en organisation som ett certifikat utfärdas till benämns genomgående som nyckelinnehavare i denna policy.

I de fall där certifikat är utfärdade till enheter som inte är egen juridisk person, så anses nyckelinnehavare i juridiskt hänseende, vara den juridiska person under vilken enheten är underställd.

Organisations HCC ges ut som ett primärcertifikat. Innan detta sker genereras ett nyckelpar enligt avsnitt 6.1.

Utmärkande för kategorin Organisation HCC är att nyckelinnehavarens namn inte innefattar personnamn eller namn på funktion.

1.3.3.3 Funktion HCC

Funktion HCC utfärdas endast till en namngiven funktion inom en organisation som kan vara:

a) en verksamhets- eller en personalfunktion inom organisationen eller

b) en tjänst eller tillämpning inom en organisation

Ett Funktion HCC är aldrig utfärdat till en enskild fysisk person. En funktion eller verksamhetsfunktion i denna mening är vidare alltid underställd en organisation och ibland även en specifik enhet inom organisationen.

En utmärkande skillnad mellan Funktion HCC och Organisations HCC är att Funktion HCC innefattar ett namn på rollen/funktionen.

Funktionen, som ett certifikat utfärdas till, benämns genomgående som nyckelinnehavare i denna policy.

Nyckelinnehavare i juridiskt hänseende, är den juridiska person under vilken rollen/funktionen är underställd.

Funktion HCC ges ut som ett primärcertifikat. Innan detta sker genereras ett nyckelpar enligt avsnitt 6.1.

Utmärkande för kategorin Funktion HCC är att nyckelinnehavarens namn innefattar namn på funktion men saknar personnamn (namn på fysisk person).

1.3.4 TILLÄMPLIGHET

Denna certifikatpolicy är relevant för CA, av CA kontrakterade RA, leverantörer av systemkomponenter, revisorer, förlitande parter samt nyckelinnehavare certifierade i utfärdade certifikat.

Certifikat utfärdade i enlighet med denna certifikatpolicy är primärt avsedda för att understödja säker informationshantering inom vård och omsorg. HCC kan också användas inom verksamheter som tillhör en organisation som är aktör inom svensk vård och omsorg.

Certifikat utgivna enligt denna certifikatpolicy kan identifiera följande olika användningsområden för det certifierade nyckelparet i enlighet med konventioner stipulerade i 6.1.9.

1. Elektroniska signaturer för användning i oavvislighetstjänster

2. Identifiering och autenticering

3. Konfidentialitetskryptering

Det ligger utanför CA: s kontroll att förhindra att privata nycklar används för otillbörliga ändamål eller i strid med nyckelinnehavarens intentioner. Varje nyckelinnehavare måste uppmanas att endast använda privata nycklar i utrustning och applikationer som är trovärdiga och tillförlitliga i detta avseende samt att inte med den privata nyckeln signera data som inte i förväg granskats och godkänts av nyckelinnehavaren.

1.4 KONTAKTUPPGIFTER

Carelink AB är ansvarig för förvaltning och administration av denna certifikatpolicy enligt vad som sägs i avsnitt 2.6.1 och kapitel 8.

Frågor rörande denna certifikatpolicy skickas skriftligen 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 CA

2.1.1.1 Generella förpliktelser

Utfärdande CA åtar sig att i enlighet med denna certifikatpolicy:

a) generera nycklar för Organisation HCC och Funktion HCC

b) utfärda HCC

c) tillhandahålla katalogtjänst i enlighet med avsnitt 2.6

d) utöva tillsyn enligt kapitel 4, 5 och 6

e) utföra identifiering enligt kapitel 3

f) understödja nyckelinnehavare och förlitande parter vilka använder certifikatet i enlighet med tillämpliga lagar och regelverk

g) spärra certifikat och ge ut spärrlistor i enlighet med kapitel 4

h) uppfylla alla allmänna villkor i kapitel 2.

Åtagandet gäller den organisation som i certifikaten identifieras så som utfärdare, oavsett om det är denna organisation eller annan, som på uppdrag åt denna organisation, utför tjänsterna.

2.1.1.2 Skydd av CA:s privata nyckel

Utfärdande CA förpliktar sig att skydda sina privata CA-nycklar i enlighet med denna certifikatpolicy.

2.1.1.3 Restriktioner gällande bruk av privat CA-nyckel

CA:s privata nycklar används enbart för att signera data enligt följande:

a) Signering av certifikat

b) Signering av spärrlistor

c) Signering av interna loggar och annan information som är relevant i samband med drift av CA-systemet

d) Signering av annan information som är intimt förknippat med CA:s roll som TTP, t ex vid tidsstämpling.

2.1.2 FÖRPLIKTELSER FÖR RA

2.1.2.1 Generella förpliktelser

Åtagandet i 2.1.1.1 från utfärdande CA:s sida gäller oavsett om det är CA organisationen eller annan, som på uppdrag av CA organisationen, utför tjänsterna.

2.1.2.2 Skydd av privat RA-nyckel

Åtagandet i 2.1.1 från utfärdande CA:s sida gäller oavsett om det är CA organisationen eller annan, som på uppdrag av CA organisationen, hanterar RA:s nycklar.

2.1.2.3 Restriktioner gällande bruk av privata nycklar

Åtagandet i 2.1.1 från utfärdande CA:s sida gäller oavsett om det är CA organisationen eller annan, som på uppdrag av CA organisationen, utför tjänsterna.

RA anlitad av utfärdande CA förbinder sig, genom avtal med CA, att privata nycklar som används i samband med realisering av processer enligt denna certifikatpolicy inte används för något annat syfte.

2.1.3 FÖRPLIKTELSER FÖR NYCKELINNEHAVARE

2.1.3.1 Generella förpliktelser

Förpliktelser för nyckelinnehavare anges i de avtalsvillkor som nyckelinnehavaren måste acceptera innan certifikat utfärdas. De förpliktelser som anges nedan finns med i de allmänna villkor som nyckelinnehavaren måste godkänna.

Vid ansökan om certifikat måste nyckelinnehavaren uppfylla sin del i de registrerings- och identifieringsprocesser som stipuleras i avsnitt 3 och 4.

2.1.3.2 Skydd av nyckelinnehavarens privata nyckel

Nyckelinnehavare förpliktar sig att skydda sin privata nyckel i enlighet med villkor accepterade av nyckelinnehavaren vid erhållandet av primärcertifikatet.

Det åligger nyckelinnehavare att informera CA så fort minsta misstanke uppstår om att den privata nyckeln har blivit komprometterad.

2.1.3.3 Restriktioner gällande bruk av nyckelinnehavarens privata nyckel

Nyckelinnehavare ansvarar för att privata nycklar endast används i sådana sammanhang och utrustningar att man med fog inte kan förvänta sig att de privata nycklarna kan missbrukas.

I detta avseende skall applikationer vara av de typer som anges i 1.3.4.1.

2.1.4 FÖRPLIKTELSER FÖR FÖRLITANDE PART

2.1.4.1 Användning av certifikat för avsedda ändamål

Förlitande part skall säkerställa att han förlitar sig på uppgifterna i ett certifikat i den utsträckning som är lämpligt med hänsyn till transaktionens karaktär. Därvid skall förlitande part

a) noga beakta de restriktioner i användningsområde som framgår av certifikatet eller av avtal mellan utfärdande CA och förlitande part,

b) bedöma om den allmänna säkerhetsnivå som framgår av denna certifikatpolicy är erforderlig med hänsyn till riskerna som är förknippade med den aktuella transaktionen samt

c) i sin riskbedömning ta med de ansvarsfriskrivningar som framgår av denna certifikatpolicy eller avtal.

Förlitande part erinras särskilt om sitt ansvar för att i eget intresse försäkra sig om att privata nycklar associerade med utfärdade certifikat används i typer av applikationer enligt 1.3.4.1 samt att beakta eventuella konsekvenser av att detta inte efterlevs.

2.1.4.2 Verifieringsansvar

Det är förlitande parts eget ansvar att verifiera certifikat i enlighet med en lämplig certifieringskedja som utgår från en av den förlitande parten betrodd CA-nyckel.

2.1.4.3 Ansvar att kontrollera spärrning och suspendering av certifikat

Det är förlitande parts eget ansvar att kontrollera ett certifikats giltighet i enlighet med 4.4.6 innan certifikatet används.

2.2 ANSVAR

2.2.1 ANSVAR FÖR CA

2.2.1.1 Garantier och ansvarsbegränsningar

Utfärdande CA ansvarar inför alla som har rimlig anledning att förlita sig på uppgifterna i ett utfärdat certifikat, att denne i enlighet med denna certifikatpolicy kontrollerat att uppgifterna i utfärdade certifikat är korrekta.

2.2.1.2 Friskrivningar

Utfärdande CA ansvarar inte för skada på grund av att uppgifterna i ett certifikat eller en spärrlista är felaktiga, såvida utfärdande CA inte gjort sig skyldig till grov vårdslöshet.

2.2.2 ANSVAR FÖR RA

Utfärdande CA ansvarar för de tjänster som RA utför på CA:s uppdrag. Det åligger CA att i avtalet med RA återspegla det ansvar som CA har enligt denna policy.

2.3 FINANSIELLT ANSVAR

2.3.1 FULLMAKTSFÖRHÅLLANDEN

CA, eller av CA anlitad RA, är fristående i förhållande till transaktionen mellan förlitande part och nyckelinnehavare. CA representerar således inte någon av parterna i deras transaktion.

2.4 TOLKNING OCH VERKSTÄLLIGHET

2.4.1 TILLÄMPLIG LAG

Vid tolkning av denna certifikatpolicy och vid bedömning av CA:s agerande i samband med utfärdande av certifikat enligt denna certifikatpolicy skall svensk lag tillämpas.

2.4.2 PROCEDURER FÖR KONFLIKTLÖSNING

Tvist i anledning av detta avtal skall slutligt avgöras i svensk domstol.

2.5 AVGIFTER

2.5.1 AVGIFTER FÖR UTFÄRDANDE OCH CERTIFIKAT

Inga föreskrifter.

2.5.2 AVGIFTER FÖR CERTIFIKATSÅTKOMST

Inga föreskrifter.

2.5.3 AVGIFTER FÖR ÅTKOMST TILL SPÄRRLISTOR

Inga föreskrifter.

2.5.4 AVGIFTER FÖR ÅTKOMST TILL POLICY OCH CPS

CA får ej ta ut avgifter som överstiger självkostnaden för att reproducera och distribuera kopior av denna policy eller den CPS som refererar till denna policy.

2.6 PUBLICERING OCH FÖRVARINGSPLATS

2.6.1 PUBLICERING AV CA-INFORMATION

Det åligger utfärdande att CA att göra följande information publikt tillgänglig

a) CPS som refererar till denna policy

b) Spärrlistor med spärrade certifikat

c) Utfärdade CA-certifikat, egensignerade CA-certifikat och korscertifikat för korscertifierade CA.

Utfärdande CA kan komma att publicera och tillhandahålla certifikatinformation i enlighet med tillämplig lag samt enligt överenskommelse med berörd vård och omsorgsorganisation.

Varje publicerad spärrlista (CRL) tillhandahåller vid publiceringstillfället all tillgänglig spärrinformation för samtliga spärrade certifikat som spärrlistan är avsedd att förmedla.

Utfärdande CA tillhandahåller CA certifikat för samtliga publika CA-nycklar så länge dessa kan användas för verifiering av giltiga certifikat.

2.6.2 ÅTKOMSTKONTROLL

Information som enligt denna certifikatpolicy publiceras via katalogtjänst inom vård och omsorg (HSA eller motsvarande) tillhandahålls i enlighet med respektive organisations bestämmelser.

2.7 REVISION

Utfärdande CA ska genomföra löpande intern revision av att denna policy efterlevs.

Vid revisionen ska speciellt följande undersökas:

a) CPS:ens lämplighet och överensstämmelse med denna policy

b) Jämförelse mellan CA:s interna rutiner och handböcker och denna policy

c) Avtal och annat som rör samverkan med RA.

Vid upptäckt av brister eller behov av förändringar skall CA vidta lämpliga åtgärder i form av att:

1. förändra tillämpade rutiner, och/eller;
2. uppdatera denna policy.

Om policy uppdateras på sådant sätt att den nya policyn bedöms medföra en förändrad säkerhetsgrad så skall en ny policy med en ny identitet upprättas (se 1.2).

2.8 KONFIDENTIALITET

2.8.1 TYP AV INFORMATION SOM SKALL HÅLLAS KONFIDENTIELL

Information som inte undantages i 2.8.2 eller på annat sätt definieras som publik i denna certifikatpolicy eller i tillämpad policy, behandlas som konfidentiell och lämnas inte ut utan samtycke från berörda avtalsparter och nyckelinnehavare.

2.8.2 TYP AV INFORMATION SOM INTE ANSES VARA KONFIDENTIELL

Följande informationsobjekt anses inte vara konfidentiella:

a) Utfärdade certifikat inklusive publika nycklar

b) Spärrlistor

c) Villkor för nyckelinnehavare

d) Certification Practice Statement, CPS

Undantag kan gälla för information relaterat till nyckelinnehavare om detta finns föreskrivet i särskild överenskommelse med nyckelinnehavarens organisation.

2.8.3 TILLHANDAHÅLLANDE AV INFORMATION VID DOMSTOLSBESLUT

Utfärdande CA tillhandahåller certifikatinformation i enlighet med tillämplig lag.

Privata nycklar kopplade till utfärdade certifikat kan inte tillhandahållas då dessa inte får finnas sparade hos utfärdande CA eller hos någon av dess underleverantörer.

2.9 IMMATERIELLA RÄTTIGHETER

Ansökan om tillstånd att på annat sätt reproducera och sprida delar av detta dokument kan göras hos:

Organisation: Carelink AB
Namn: Programområdesansvarig, informationssäkerhet och katalog
Adress: Box 12713
Postnummer: 112 94
Ort: Stockholm
Telefon: 08/650 26 13
Fax: 08/650 26 42
E-post: carelink@carelink.se
Web: www.carelink.se

2.10 AVTAL

CA utfärdar HCC på uppdrag av organisationer inom svensk vård och omsorg.

Mellan CA och sådan organisation skall avtal tecknas. I detta avtal skall framgå arbetsgivares ansvar att lämna korrekta uppgifter samt skyldighet att rapportera förändringar i omständigheter som innebär eller kan påverka beslut om spärrning av certifikat.

Utfärdande CA skall ha avtal med samtliga underleverantörer som reglerar parternas rättigheter och skyldigheter. Begreppet underleverantör omfattar RA. Genom dessa avtal försäkrar sig CA om att valda underleverantörer lever upp till CA:s åtaganden i denna certifikatpolicy.

Innan produktion av certifikat kan ske, krävs att nyckelinnehavaren accepterar avtal som reglerar relationen mellan utfärdande CA och nyckelinnehavaren.

3 IDENTIFIERING OCH AUTENTICERING

3.1 INITIAL REGISTRERING

3.1.1 NAMNTYPER

Nyckelinnehavare registreras med kontaktuppgifter samt identitetsuppgifter.

De uppgifter om nyckelinnehavaren som publiceras i utfärdade certifikat utgör ett urval av nedanstående attribut:

- Land
- Region
- Organisation
- Organisationsenhet
- Förnamn
- Efternamn
- Fullständigt namn i enlighet med nyckelinnehavarens normalt använda presentationsform
- Unik identifieringskod
- Tjänstetitel
- Rollbeteckning
- Namn på tjänst/funktion
- e-postadress (SMTP eller X.400)
- EDI-adress

3.1.1.1 Person HCC

Av ovanstående attribut kan följande förekomma i ett Person HCC:

- Land
- Region
- Organisation
- Organisationsenhet
- Förnamn
- Efternamn
- Fullständigt namn i enlighet med nyckelinnehavarens normalt använda presentationsform
- Unik identifieringskod
- Funktionsbeteckning
- e-postadress (SMTP eller X.400)
- EDI-adress

3.1.1.2 Organisations HCC

Av ovanstående attribut kan följande förekomma i ett Organisations HCC:

- Land
- Region
- Organisation
- Organisationsenhet
- Unik identifieringskod
- e-postadress (SMTP eller X.400)
- EDI-adress

3.1.1.3 Funktion HCC

Av ovanstående attribut kan följande förekomma i ett Funktion HCC:

- Land
- Region
- Organisation
- Organisationsenhet
- Unik identifieringskod
- Funktionsbeteckning
- e-postadress (SMTP eller X.400)
- EDI-adress

3.1.2 KRAV PÅ NAMNS MENINGSFULLHET

Om attributet Land förekommer så specificerar detta det land inom vilket betydelsen av övriga attribut är definierad och ska kunna tolkas. Detta innebär då att alla förekommande attribut måste vara definierade och kunna tolkas inom samma land.

E-postadress kan utgöra såväl X.400-adress som SMTP-adress (RFC 822 namn).

Unik identifierare utgör en allmän identifierare som bör vara av annat slag än svenskt personnummer. Dess primära syfte är att tillhandahålla en fungerande unik identitet för informationssystem som inte kan tillämpa identiteter sammansatta av flera attribut, men det skall även säkerställa att två nyckelinnehavare inte certifieras med samma identitet.

Organisationsnamn utgör organisationens officiellt registrerade namn inom det specificerade landet. För organisationsnamn registrerade inom Sverige gäller att organisationsnamnet skall vara registrerat hos Svenska Patent- och Registreringsverket.

Organisationsenhet utgör godtycklig benämning på enhet eller gren av organisationen. Namn på organisationsenhet specificeras godtyckligt av ansvarig organisation som även ansvarar för att namnet är unikt inom organisationen för det specificerade landet.

Nyckelinnehavarens identitet kan specificeras av en godtycklig kombination av attributen i 3.1.1 så länge kombinationen innefattar obligatoriska attribut samt tillhandahåller en omisskännlig identitet. En omisskännlig identitet definieras här som 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 (som vid användning av e-postadress).

3.1.3 AUTENTICERING AV ORGANISATIONSTILLHÖRIGHET

Nyckelinnehavares organisationstillhörighet måste vara styrkt (auktoriserad) av en behörig representant för den aktuella organisationen. En auktorisation kan representera en eller flera nyckelinnehavare.

Behöriga representanter specificeras i det avtal som enligt 2.9 tecknas med aktuell organisation. I avtalet framgår att organisationen är skyldig att rapportera relevanta förändringar i omständigheter av betydelse för beslut om spärrning av certifikat. Behörig representant kan vara RA, som arbetar enligt RA-policy. [RApolicy]

3.1.4 AUTENTICERING AV PERSONERS IDENTITET

Nyckelinnehavare för vilken behörig representant (arbetsgivare etc.) ansöker om certifikat identifieras vid beställningstillfället enligt 3.1.4.1 nedan.

Tjänsteman alternativt utsedd kontaktperson som godkänner ansökan gör en kontroll av att den ansökande uppfyller kraven för att kunna erhålla den typ av certifikat som ansökan avser. Godkännande av ansökan kan ske vid ansökningstillfället varvid kontrollanten anger hur beställaren identifieras och skriver under att identitetskontroll skett.

Godkännande kan även ske före själva ansökningstillfället varvid identitetskontroll loggas separat då den utförs.

3.1.4.1 Krav på identitetskontroll

Identitetskontroll görs enligt någon av nedanstående procedurer.

a) Nyckelinnehavaren uppvisar godkänd och giltig legitimationshandling.

b) Nyckelinnehavaren legitimerar sig och signerar beställningen elektroniskt med hjälp av elektronisk ID-handling som minst motsvarar säkerhetsnivån i denna certifikatpolicy.

3.1.4.2 Procedur för autenticering

Innan certifikat skapas så kontrolleras samtliga nyckelinnehavarens identitetsuppgifter, som inte undantags nedan, mot tillförlitliga register. Följande förhållanden kontrolleras i mån av tillämplighet:

a) att registrerad identitet finns registrerad i specificerat land

b) att stavning av namn är korrekt

c) att organisationsnamn representeras av namn som är registrerat hos svenska Patent- och Registreringsverket (om Sverige anges som land) av den organisation på vilkens uppdrag nyckelinnehavaren arbetar eller där nyckelinnehavaren är anställd.

Som undantag för kontroll mot tillförlitligt register gäller:

a) E-postadress accepteras efter skriftlig försäkran från nyckelinnehavaren att angiven e-postadress är korrekt samt efter det att kontrollmeddelande till angiven e-postadress besvarats korrekt med acceptans av att denna adress förknippas med nyckelinnehavarens identitet i det utfärdade certifikatet.

b) Organisationsrelaterad information så som association med organisation, organisationsenhet, organisationsadress, EDI-adress accepteras efter skriftligt medgivande från behörig representant för den aktuella organisationen. Dock kontrolleras organisationsnamnets stavning enligt ovan.

c) Fullständigt namn i enlighet med nyckelinnehavarens normalt använda presentationsform accepteras efter nyckelinnehavarens skriftliga intyg att detta är den namnform denne normalt använder vid namnpresentation.

3.1.4.3 Krav på personlig närvaro

Elektronisk identitetskontroll vid beställning av certifikat kräver inte personlig närvaro av nyckelinnehavaren.

Övrig identitetskontroll vid beställning kräver personlig närvaro.

3.1.5 AUTENTICERING AV ORGANISATIONER OCH FUNKTIONER INOM ORGANISATIONER

Vid beställning av certifikat av typerna Organisation HCC och Funktion HCC, samt vid distribution av privata nycklar och koder kopplade till dessa, infordras en skriftlig beställning från en behörig representant för den aktuella organisationen. Denna beställning kan avse en eller flera nyckelinnehavare.

Behöriga representanter specificeras i det avtal som enligt 2.10 tecknas med aktuell organisation. I avtalet framgår i vilket avseende specificerade representanter har rätt att företräda organisationen.

3.1.5.1 Autenticering av behörig representant

Vid utlämning av privata nycklar och koder sker identitetskontroll av behörig representant.

3.1.5.2 Krav på personlig närvaro

Beställning av certifikat sker genom skriftligt avrop från ingångna avtal vilket inte kräver personlig närvaro av beställaren. Identitetskontroll vid utlämning av privata nycklar och koder kräver personlig närvaro av behörig representant vid utlämningstillfället.

3.2 FÖRNYAD REGISTRERING VID FÖRNYELSE AV NYCKLAR

Begäran om förnyade nyckelpar och motsvarande certifikat för Organisation HCC och Funktion HCC skall ske enligt föreskrifterna i 3.1.

3.3 FÖRNYAD REGISTRERING VID FÖRNYELSE AV NYCKLAR EFTER SPÄRRNING

Begäran om förnyade nyckelpar och motsvarande certifikat efter spärrning av certifikat för Organisation HCC och Funktion HCC skall ske enligt föreskrifterna i 3.1.

3.4 SPÄRRNINGSBEGÄRAN

De normala rutinerna för hur autenticering ska gå till skall specificeras i CPS:en.

En spärrningsbegäran kan autenticeras med en digital signatur där det certifikat som ska spärras används.

Vid begäran om spärrning kan den som begär spärrning identifieras enligt följande:

Spärrning från	*Metod för spärrning*	*Identifieringsmetod*
RA eller annan behörig representant för RA	Elektroniskt meddelande	Spärrningsbegäran skickas som digitalt signerat meddelande.
Behörig representant för CA	Elektroniskt meddelande	Spärrningsbegäran skickas som digitalt signerat meddelande.

Spärrning från behörig CA-representant får endast göras då RA eller annan behörig representant är förhindrad att begära spärrning.

Om det misstänks föreligga risk för missbruk av en privat nyckel som är associerad med ett certifikat, så spärras certifikatet enligt begäran, även om ovanstående identifieringskrav ej fullt ut kan tillgodoses.

Metoden för autenticering av spärrningsbegäran ska loggas, liksom skälen till en förenkling av autenticeringsproceduren enligt ovan.

4 OPERATIONELLA KRAV

4.1 ANSÖKAN OM CERTIFIKAT

Vid ansökan fullföljs följande procedurer:

a) Uppdragsgivaren (behörig representant eller RA) fyller i ansökningshandlingar och undertecknar ansökan varvid alla villkor enligt 2.10 accepteras. I denna process uppger nyckelinnehavaren samtliga relevanta personliga uppgifter enligt 3.1.1.

b) Nyckelinnehavaren identifieras enligt 3.1.4.

c) Ansökningshandlingar arkiveras enligt 4.6.

4.2 UTFÄRDANDE AV CERTIFIKAT

Utfärdandet av ett certifikat innebär CA:s acceptans av nyckelinnehavarens ansökan samt av de uppgifter som nyckelinnehavaren lämnat.

Hantering av elektronisk registrering hos av CA utsedd RA sker i ett system och i en miljö som är väl integritetsskyddad samt följer rutiner som är avsedda att förhindra felaktig sammanblandning av identitetsuppgifter och nycklar.

Certifikat produceras efter det att ansvarig operatör hos CA eller RA personligen konstaterat att angivna beställningsrutiner och kontrollrutiner fullföljts.

Varje signerad beställning från behörig operatör hos CA eller RA, kan spåras individuellt till den operatör som signerat beställningen.

4.2.1 METOD FÖR ATT BEVISA INNEHAV AV PRIVAT NYCKEL

Nyckelinnehavarens innehav av korrekt privat nyckel säkras genom någon av följande metoder:

1. Nyckelinnehavaren styrker innehavet genom att korrekt använda nyckeln i ett för syftet lämpligt kontrollförfarande (vid utfärdande av Person HCC).
2. Genom att den privata nyckeln genereras av CA samt säkert skyddas och distribueras till ansvarig nyckelinnehavare (vid utfärdande av Organisations HCC och Person HCC).
3. Då nyckelinnehavaren redan innehar certifikat som korresponderar mot aktuell privat nyckel, kan innehav av korrekt privat nyckel styrkas mot uppvisande av detta certifikat. Förutsättningen är dock att detta certifikat påvisar en säkerhetsnivå som minst korresponderar mot denna policy samt att de användningsrestriktioner som identifieras i certifikatet korresponderar mot de användningsrestriktioner som skall gälla för det nya certifikatet (vid utfärdande av Person HCC).

4.3 ACCEPTERANDE AV CERTIFIKAT

Procedurer för nyckelinnehavarens accepterande av det utfärdade certifikatet ska framgå av den RA-policy och den RAPS som tillämpas vid den organisation som nyckelinnehavaren tillhör.

4.4 SPÄRRNING AV CERTIFIKAT

CA tillhandahåller en tjänst för spärrning av certifikat. Spärrtjänsten är öppen dygnet runt.

CA skapar löpande signerade listor över spärrade certifikat (CRL), varav den senaste lagras publikt tillgänglig i CA:s katalog. Spärrlistorna ska vara tillgängliga i en sådan omfattning att det är möjligt för en förlitande part att på ett säkert och effektivt sätt kontrollera ett certifikats giltighet. Aktuell spärrlista omfattar information om spärrning för de certifikat som är associerade med spärrlistan, i enlighet med innehållet i CRL enligt X.509, version 2. Denna innefattar information om alla spärrade certifikat vars giltighetstid inte löpt ut.

Vid spärrning av certifikat informeras nyckelinnehavaren i enlighet med gällande villkor.

4.4.1 ANLEDNING TILL SPÄRRNING

CA spärrar utfärdade certifikat i följande fall:

a) Vid ändring av någon av de uppgifter eller förhållande som certifieras i det utfärdade certifikatet t ex ändring av namn eller anställningsförhållande.

b) Efter mottagande av spärrningsbegäran enligt 4.4.3.

c) Vid misstanke om att den privata nyckeln används av annan än dess rättmätige nyckelinnehavare eller på något annat sätt misstänks vara komprometterad.

d) Vid misstanke om att det EID-kort eller motsvarande lagringsmodul som innehåller korresponderande privat nyckel inte längre innehas/kontrolleras eller inte längre kan brukas av rätt nyckelinnehavare.

e) Vid skälig misstanke om att nyckelinnehavaren bryter mot villkor enligt 2.10 eller att nyckelinnehavaren i sitt nyttjande av certifikat och privata nycklar bryter mot gällande rätt.

f) Om tillämpad CA-nyckel på något sätt misstänks vara komprometterad.

g) Om CA beslutar upphöra med sin CA-verksamhet enligt 4.9.

Om CA spärrar certifikat tillföljd av a–e ovan på felaktiga grunder gäller begränsningar i ansvar för CA enligt gällande villkor.

4.4.2 VEM KAN BEGÄRA SPÄRRNING HOS CA

Spärrningsbegäran enligt 3.4 kan begäras av RA eller av behörig representant för RA.

CA kan dock besluta om spärrning som ett resultat av uppgifter som lämnats av annan part om detta utgör skälig grund för att misstänka att något av fallen enligt 4.4.1 föreligger.

4.4.3 PROCEDURER FÖR SPÄRRNINGSBEGÄRAN

En till CA kopplad tjänst tar emot begäran om spärrning. Spärrningsbegäran ska vara signerad av RA eller av behörig representant för RA.

Samtliga mottagna spärrningsbegäran arkiveras tillsammans med information om:

a) hur begäran inkom

b) när begäran inkom

c) anledning för spärrning

d) hur den som begärde spärrning identifierats

e) resultat av begäran (spärrning eller ej spärrning)

f) tidpunkt för publicering i spärrlista

g) loggnummer

4.4.4 Behandlingstid vid spärrningsbegäran

Relevant information om spärrning publiceras i spärrlistan senast en timme efter beslut om spärrning av ett certifikat.

Beslut om spärrning fattas normalt i direkt anslutning till mottagandet av spärrningsbegäran. Vid tveksamma fall kan dock beslut dröja tills spärrtjänsten sökt särskild bekräftelse av grund för spärrning. Det finns ingen maximal tid för sådant agerande.

4.4.5 Utgivningsfrekvens för spärrlista

Alla spärrlistor utgivna inom ramen för denna certifikatpolicy uppdateras och publiceras så snart spärrbegäran inkommit och beslut om spärrning fattats, dock alltid en gång varje timme dygnet runt.

Funktionen att uppdatera och publicera spärrlistor kan vid service och systemfel vara otillgänglig under en begränsad tid i enlighet med 2.6.1.

4.4.6 Krav på kontroll mot spärrlista

Det är förlitande parts eget ansvar att kontrollera verifierade certifikat mot senast utgivna spärrlista.

Vid kontroll av spärrlista skall förlitande part försäkra sig om att:

a) certifikat kontrolleras mot en spärrlista som representerar den senaste aktuella spärrinformationen för certifikatet i fråga

b) spärrlistan fortfarande är giltig, dvs. att dess giltighetstid inte löpt ut

c) spärrlistans signatur är giltig

4.4.7 Möjlighet till kontroll av spärrlistor och certifikatsstatus

Som ett alternativ till spärrlistor kan on-line transaktioner för kontroll av ett certifikats giltighet och status användas. Beskrivning av procedurer för detta skall framgå av CPS:en.

4.5 Procedurer för säkerhetsrevision av CA-systemet

I detta avsnitt specificeras procedurer för loggning av händelser samt därtill relaterad revision av säkerhet i CA-systemet på systemnivå och operativsystemnivå.

4.5.1 Typ av loggade händelser

I och runt CA-systemet loggas minst följande händelser:

a) Skapande av användarkonton

b) Initiering av operationer på operativsystemsnivå av systemanvändare med uppgift om vem som begärde operationen, typ av operation, samt indikering av resultat av initieringen

c) Installation och uppdatering av mjukvara

d) Relevant information om säkerhetskopior

e) Start och avstängning av systemet

f) Tid och datum för alla hårdvaruuppgraderingar

g) Tid och datum för säkerhetskopiering och tömning av loggar

h) Tid och datum för säkerhetskopiering och tömning av arkivdata (enligt 4.6)

4.5.2 Frekvens för bearbetning av logg

Loggarna analyseras dagligen för upptäckt av obehöriga aktiviteter.

4.5.3 Bevaringstid för logg

Loggar enligt 4.5.1 bevaras i minst 10 år.

4.5.4 Skydd av logg

Loggar skyddas mot otillbörlig förändring dels genom de logiska skyddsmekanismerna i operativsystemet samt dels genom att systemet i sig inte är fysiskt och logiskt åtkomligt annat än för behörig personal.

Alla loggposter är individuellt tidsstämplade.

Loggarna verifieras och konsolideras minst en gång per månad under överinseende av minst två personer i SA befattning alternativt ISSO befattning (se 5.2.1.1).

4.5.5 Procedurer för säkerhetskopiering av logg

Två kopior av den konsoliderade loggen, signerad med CA:s privata nyckel, lagras i fysiskt säkrade utrymmen på fysiskt skilda platser.

Loggarna lagras på sådant sätt att de vid allvarlig misstanke om oegentligheter kan tas fram och göras läsbara för granskning under den angivna lagringstiden.

4.5.6 System för insamling av revisionsinformation

System för insamling av loggar enligt detta avsnitt hanterar enbart intern logginformation skapad i det centrala systemet för certifikatproduktion.

4.6 Arkivering

CA arkiverar relevant material som berör drift av CA-tjänsten. Procedurer och förutsättningar för denna arkivering specificeras i följande underavsnitt.

4.6.1 Typ av arkiverad information

Följande information arkiveras löpande:

a) Transaktioner innehållande signerad begäran om certifikatproduktion och spärrning av certifikat från behörig operatör.

b) Ansökningshandlingar undertecknade av ansökande uppdragsgivare samt av personer ansvariga för att ta emot och acceptera ansökan.

c) Undertecknade mottagningskvittenser vid utlämning av nycklar och koder.

d) Utgivna certifikat samt därtill relaterade uppdateringar av katalog.

e) Historik rörande tidigare CA-nycklar, nyckelidentifierare samt korscertifikat mellan olika generationer av CA-nycklar.

f) Begäran om spärrning samt därtill relaterade uppgifter inkomna till spärrtjänsten.

g) Utgivna spärrlistor samt därtill relaterade uppdateringar av CA:s katalog.

h) Resultat av revision av CA:s uppfyllelse av denna certifikatpolicy.

i) Gällande villkor och kontrakt (i alla tillämpade versioner).

j) Denna certifikatpolicy samt alla tidigare tillämpade versioner av denna certifikatpolicy.

I de fall den arkiverade informationen utgörs av en digitalt signerad informationsmängd så arkiveras även nödvändig information som krävs för verifiering av signaturen under angiven arkiveringstid.

4.6.2 BEVARINGSTID FÖR ARKIV

All arkiverad information enligt 4.6.1 bevaras i minst 15 år.

4.6.3 PROCEDURER FÖR ATT NÅ OCH VERIFIERA ARKIVMATERIAL

Arkiverat material som är klassat som konfidentiellt enligt 2.8.1 är inte tillgängligt för externa parter i sin helhet annat än vad som krävs genom lag och beslut i domstol.

Utlämning av enstaka uppgifter rörande en specifik nyckelinnehavare eller transaktion kan göras efter individuell prövning.

Arkiven lagras under sådana förhållanden att de förblir läsbara för granskning under den angivna lagringstiden. Parter görs dock uppmärksamma på att teknik för lagring av arkivmaterial kan komma att ändras och att CA i sådant fall inte är ålagd att bibehålla funktionell utrustning för tolkning av gammalt arkivmaterial om detta är äldre än 5 år. I dessa fall är dock CA istället ålagd att ha beredskap för att sätta upp nödvändig utrustning mot uttagande av en avgift som svarar mot CA:s kostnader.

Av den händelse att procedurer för tillgång till arkivmaterial förändras förorsakat av att CA upphör med sin verksamhet, så kommer information om procedur för fortsatt tillgång till arkivmaterial att tillhandahållas av CA genom underrättelseprocedurer enligt 4.9.

4.7 BYTE AV CA-NYCKEL

Ny CA-nyckel skapas minst tre månader före den tidpunkt då tidigare CA-nyckel upphör att användas för utfärdande av nya certifikat.

Vid byte av CA-nyckel sker följande:

a) nytt egensignerat certifikat utfärdas för den nya publika CA-nyckeln,

b) korscertifikat utfärdas där den gamla CA-nyckeln signeras med den nya CA-nyckeln,

c) korscertifikat utfärdas där den nya CA-nyckeln signeras med den gamla CA-nyckeln och

d) certifikaten enligt a–c publiceras i relevant katalog.

4.8 PLANERING FÖR KOMPROMETTERING OCH KATASTROF

CA åtar sig att, vid misstanke om att CA inte längre äger fullständig och exklusiv kontroll över den privata CA-nyckeln, vidta följande åtgärder:

a) Upphöra med alla spärrkontrolltjänster rörande certifikat utgivna med den komprometterade nyckeln samt alla spärrkontrolltjänster som signeras med den komprometterade nyckeln eller av nyckel som certifierats med den komprometterade nyckeln. Detta innebär att alla associerade spärrlistor plockas bort från sina anvisade platser.

b) Informera alla nyckelinnehavare, och alla parter som CA har en relation med, att CA-nyckeln är komprometterad och hur nytt CA-certifikat kan hämtas.

c) I det fall CA har korscertifierat den komprometterade CA-nyckeln med en annan operativ CA-nyckel, spärra sådana korscertifikat.

d) Sörja för att spärrinformation finns tillgänglig för certifikat enligt c) fram tills dess att de spärrade certifikatens giltighetstid löpt ut.

4.8.1.1 Nyckelinnehavare

Nyckelinnehavare informeras om att omedelbart upphöra med användning av privata nycklar som är associerat med certifikat utfärdade med den komprometterade CA-nyckeln.

Nyckelinnehavarna informeras om hur dessa skall förfara för att erhålla ersättningscertifikat och eventuellt även nya privata nycklar, samt under vilka förutsättningar gamla privata nycklar kan användas i samband med andra certifikat som inte är utfärdade med den komprometterade CA-nyckeln.

4.8.1.2 Förlitande part och korscertifierande CA

Information kommer att göras tillgänglig för förlitande parter och för korscertifierande CA som klart informerar att berörda certifikat samt CA:ns utfärdarnyckel är spärrade från användning.

Förlitande part och andra korscertifierande CA agerar utanför CA:s inflytande. Dessa erhåller genom CA:s hantering av spärrlistor den information som krävs för att de skall kunna agera på ett korrekt sätt.

4.9 UPPHÖRANDE AV CA

I den händelse CA:s verksamhet upphör så förbinder sig CA att fullfölja följande procedurer:

a) Specifikt informera alla nyckelinnehavare och alla parter som CA har en relation med, minst sex månader innan verksamheten upphör.

b) Öppet informera om att verksamheten upphör minst tre månader i förväg.

c) Upphöra med alla spärrkontrolltjänster rörande certifikat utgivna med upphörande utfärdarnycklar. Detta innebär att alla associerade spärrlistor plockas bort från sina anvisade platser och att inga nya spärrlistor utfärdas som ersättning för de som plockats bort.

d) Avsluta alla rättigheter för underleverantörer att agera i den upphörande CA:s namn.

e) Sörja för att alla arkiv och loggar bevaras under angiven bevaringstid samt i enlighet med angivna föreskrifter.

Det åligger CA att inneha garantier för medel som täcker kostnaderna för åtgärderna a–e under föreskriven tid.

5 FYSISK, PROCEDURORIENTERAD OCH PERSONALORIENTERAD SÄKERHET

5.1 FYSISK SÄKERHET

5.1.1 ANLÄGGNINGENS LÄGE OCH KONSTRUKTION

Anläggningen som rymmer centrala CA-funktioner är fysiskt placerad i en starkt skyddad datorhall. I denna datorhall är viktiga komponenter inlåsta i separata och fristående säkerhetsskåp.

Datorhallen som är låst och larmad befinner sig i en byggnad som även den är låst och larmad. Dessa skyddas gemensamt genom aktiv bevakning.

5.1.2 FYSISKT TILLTRÄDE

Detaljerad information av säkerhetsprocedurer för fysiskt tillträde är av säkerhetsskäl inte publikt tillgänglig.

Lokalernas externa skydd så som lås och larmanordningar kontrolleras löpande av tjänstgörande vaktpersonal varje dygn.

5.1.3 LAGRING AV MEDIA

Frånsett datorhall enligt 5.1.1 finns en annan, fristående skyddad, lokal för lagring av säkerhetskopior och viktiga handlingar. I denna lokal finns särskilda individuellt låsbara skåp för förvaring av olika typer av loggar och arkiv.

5.1.4 FYSISK SÄKERHET FÖR RA

Några RA funktioner som innefattar roller enligt 5.2.1 kan förekomma utanför den skyddade centrala fysiska miljön enligt 5.1.1. De är:

1. Identifiering av nyckelinnehavare vid ansökan med personlig närvaro.
2. Utlämning av nycklar och koder.
3. Identifiering av nyckelinnehavare samt innehav av rätt privat nyckel vid elektronisk ansökan.
4. Elektronisk registrering av nyckelinnehavare.
5. Spärrtjänst för spärrning av certifikat.

Funktion enligt punkt 1 och 2 innebär ingen access till CA-systemet. Denna miljö har därför inga särskilda säkerhetsföreskrifter vad avser fysisk säkerhet.

Funktioner enligt punkt 3–5 utförs i låsbart utrymme i kontorsmiljö. Inga nycklar eller koder lämnas utan tillsyn. Operatörskort som ger access till operativa roller i CA-systemet är personliga och lämnas inte kvar då operatören lämnar lokalen. Lokalen innefattar även låsbara skåp för förvaring av arkivmaterial.

5.2 PROCEDURORIENTERAD SÄKERHET

CA ansvarar i enlighet med 2.1.1. för alla procedurer och förhållanden som definieras i detta avsnitt. Detta innefattar allt från produktion och logistik till administration av hela processen.

5.2.1 BETRODDA ROLLER

5.2.1.1 Betrodda roller inom CA

Roller definierade för drift och underhåll av CA-tjänsten skall vara:

Roll	*Förklaring/Uppgifter*
Certification Authority Administrator (CAA)	Administrativ produktions-/driftspersonal för CA:n. Typiska uppgifter som kan administreras av CAA är: • Skapa certifikat • Personalisera kort • Generera nycklar • Generera spärrlista • Kontroll av certifikatutfärdarloggen
System Administrator (SA)	Teknisk produktions-/driftspersonal för CA:n. Typiska uppgifter som kan administreras av SA är: • Installationer • Systemunderhåll • Byte av media med säkerhetskopior
Information Systems Security Officer (ISSO)	Säkerhetsansvarig för CA-tjänsten. ISSO är inte själva direkt involverad i processen att generera certifikat, kort och spärrlistor, men ansvarar för att alla operativa roller agerar inom ramen för sina befogenheter.

CA kan dock välja att dela upp ansvaret för ovan angivna roller i ytterligare delroller för att öka säkerheten.

5.2.1.2 Betrodda roller inom RA

Operatörer inom en RA besitter enbart roller avpassade efter RA:s arbetsuppgifter.

5.2.2 KRAV PÅ ANTAL PERSONER PER UPPGIFT

Rollerna enligt 5.2.1.1 tillsätts av minst en person vardera. Person som innehar roll som ISSO eller SO innehar inte samtidigt någon annan av dessa roller.

Initiering av CA-systemet samt generering och initiering av CA-nycklar kräver närvaro av minst tre personer som innehar ISSO eller CAA roll.

Övriga krav på närvaro av personer vid utförande av olika arbetsuppgifter redovisas under berörda avsnitt.

5.2.3 IDENTIFIERING OCH AUTENTICERING AV VARJE ROLL

Identifiering av roller i CA-systemet sker enligt följande:

Identifiering av rollerna SA sker i operativsystemet i CA-systemets enheter.

Identifiering av rollerna CAA (där så är tillämpligt) sker i CA-systemets applikationer och baseras på stark autenticering med hjälp av personliga operatörskort av typ som definieras enligt 6.2.1.

5.3 PERSONALORIENTERAD SÄKERHET

5.3.1 BAKGRUND, KVALIFIKATIONER, ERFARENHET OCH TILLSTÅNDSKRAV

Roller enligt 5.2.1.1 tilldelas endast särskilt utvalda och pålitliga personer som uppvisat lämplighet för en sådan befattning.

Dessa personer får inte inneha annan roll som kan bedömas stå i konflikt med den tilldelade rollen.

5.3.2 KRAV PÅ UTBILDNING

Alla innehavare av rollerna har genomgått den utbildning och träning som krävs för att på ett säkert sätt utföra sina arbetsuppgifter inom ramen för denna certifikatpolicy och inom ramen för gällande säkerhets-policy.

5.3.3 PERSONALORIENTERAD SÄKERHET FÖR RA

Ansvarig personal hos RA utses inom den organisation som är utsedd att utföra tilldelade arbetsuppgifter. Om sådan roll utses av underleverantör till CA så ansvarar denna även för att lämplig personalkontroll utförs.

RA personal som tilldelats roll i CA-systemet uppfyller samma krav som för motsvarande CA-personal vad avser lämplighet och utbildning.

6 TEKNIKORIENTERAD SÄKERHET

6.1 GENERERING OCH INSTALLATION AV NYCKELPAR

6.1.1 GENERERING AV NYCKELPAR

Nedan angivna krav för generering av nycklar avser endast de nycklar som skapas av CA.

Nycklar som skapas av CA genereras utifrån ett slumptal. Processen att generera slumptal, som bas för nyckelgenerering, är slumpmässig på så sätt att det är beräkningsmässigt ogörligt att återskapa ett genererat slumptal, oavsett mängden kunskap om genereringsprocessens beskaffenhet eller vid vilken tidpunkt eller med hjälp av vilken utrustning slumptalet skapades.

Nyckelgenereringsprocessen är så beskaffad att ingen information om nycklarna hanteras utanför nyckelgeneringssystemet annat än genom säker överföring till avsedd förvaringsplats.

Nycklarnas unicitet uppnås genom att nycklarna är slumpmässigt genererade och av sådan längd att sannolikheten för att två identiska nycklar genereras är försumbar.

6.1.1.1 Specifika krav rörande CA:s utfärdarnycklar

Generering av CA:s privata utfärdarnycklar sker i den datorenhet där nycklarna sedan används. Denna datorenhet skyddas fysiskt enligt avsnitt 5.1 vilket bl. a. innebär att tillträde till denna enhet kräver samtidig närvaro av två behöriga operatörer.

6.1.1.2 Specifika krav rörande privata nycklar för nyckelinnehavare

Centralt genererade RSA-nycklar genereras i en fristående arbetsstation och lagras på lämplig lagringsmodul och raderas därefter från arbetsstationens arbetsminne.

Lagringsmodul skall minst motsvara den skyddsgrad som tillhandahålls av s.k. smarta kort enligt 6.2.1.

6.1.2 LEVERANS AV CENTRALT GENERERADE PRIVATA NYCKLAR TILL NYCKELINNEHAVARE

Efter produktion levereras nycklar med säker transport till mottagaren (motsvarande Postens REK/ASS). Eftersändning är inte tillåten.

Färdiga nyckelmoduler som inte hinner packas och eller skickas inom samma dag, låses in i valv till nästföljande arbetsdag.

Nycklar och eventuella koder skickas enligt gällande avtal.

Nycklar till organisationer lämnas endast ut till behörig representant för nyckelinnehavaren sedan denne identifierat sig i enlighet med 3.1.4.1.

Mottagande av nycklar och koder kvitteras. Kvittensen arkiveras i minst 15 år.

6.1.3 LEVERANS AV PUBLIK NYCKEL TILL CA

Överföring av publika nycklar från nyckelinnehavare till CA sker endast vid begäran om sekundärcertifikat, dvs. då ett Person HCC ska utfärdas. Den publika nyckeln verifieras oberoende av hur den levereras genom ett för ändamålet särskilt protokoll, eller mot uppvisandet av ett certifikat som minst motsvarar säkerhetsnivån enligt denna policy, som intygar nyckelinnehavarens association med nyckeln.

6.1.4 LEVERANS AV CA:S PUBLIKA NYCKLAR TILL NYCKELINNEHAVARE OCH FÖRLITANDE PARTER

Förlitande part ansvarar för att hämta korrekta och gällande versioner av CA:s publika nycklar. CA-certifikat kan hämtas från CA:s katalog.

6.1.5 NYCKELSTORLEKAR

CA:s utfärdarnycklar genereras som RSA nycklar med 1024 bitars längd.

Nyckelinnehavares och operatörers RSA nycklar genereras med 1024 bitars längd.

6.1.6 GENERERING AV PUBLIKA NYCKELPARAMETRAR

Nyckelinnehavares nycklar som i certifikaten markeras med användningsområdena kryptering och autenticering ges publika exponenter som förhindrar kända attacker.

Nyckelinnehavares nycklar som i certifikaten markeras med användningsområdet avsett för verifiering av oavvisliga digitala dokument ges publika exponenter som förhindrar kända attacker.

CA:s utfärdarnycklar ges publika exponenter som förhindrar kända attacker.

Det förutsätts att CA håller sig ajour med teknikutvecklingen inom kryptoteknikområdet och anpassar sina kryptoalgoritmer i enlighet de senaste rönen.

6.1.7 KONTROLL AV KVALITET PÅ NYCKELPARAMETRAR

Nycklarnas kvalitet säkras dels genom krav på slumptalsgenerering enligt 6.1.1 samt dels genom att de genererade primtalsfaktorerna passerar statistiska primtalstester.

6.1.8 GENERERING AV NYCKLAR I HÅRDVARA/MJUKVARA

Nycklar genereras med mjukvara.

6.1.9 ANVÄNDNINGSOMRÅDE FÖR NYCKLAR

Utgivna certifikat innehåller information som definierar tillämpligt användningsområde för certifikatet och dess associerade nycklar. Markering av användningsområde sker i enlighet med X.509 version 3 och avsnitt 7.

Certifikat utgivna i enlighet med denna certifikatpolicy kan omfatta följande användningsområden:

a) Identifiering och Autenticering

b) Konfidentialitetskryptering

c) Verifiering av elektroniska signaturer i samband med oavvislighetstjänster

Användningsområde a) och b) representeras av samma certifikat. Användningsområde c) representeras av ett särskilt certifikat som inte kan användas för a) eller b).

Om användningsområdet c) finns markerat i ett certifikat så har detta innebörden att certifikatet och dess associerade nycklar endast får användas i oavvislighetstjänster.

6.2 SKYDD AV PRIVAT NYCKEL

Procedurerna enligt denna certifikatpolicy vad avser generering, förvaring och distribution av privata nycklar har som syfte att till största möjliga grad borga för att privata nycklar skyddas på ett sådant sätt att de inte kan falla i orätta händer samt, vad avser nyckelinnehavares privata nycklar, att de inte i något fall exponeras eller brukas på otillbörligt sätt, innan de nått rätt mottagare.

6.2.1 STANDARD FÖR KRYPTOGRAFISK MODUL

CA:s signeringsnyckel används och skyddas i en särskild datorenhet som är inlåst i ett säkerhetsskåp som i sin tur förvaras inom det skalskyddade område som definieras i 5.1.

Nyckelinnehavares privata nycklar kan inneslutas och skyddas på två olika sätt.

1. Hårdvaruskyddade nycklar som nyckelinnehavaren erhållit i samband med ansökan om andra certifikat som minst motsvarar säkerhetsnivån i denna policy.
2. Mjukvaruskyddade privata nycklar som genererats av CA enligt denna policy.

Mjukvaruskyddade nycklar skall lagras i krypterad form med säkerhetsnivå som gör det beräkningsmässigt ogörligt att forcera kryptoskyddet genom logiska attacker. Nycklar för dekryptering av skyddade privata nycklar skall skyddas mot obehörig åtkomst på ett sätt som skapar ett skydd mot missbruk som motsvarar hårdvaruskyddade nycklar. Nyckelinnehavare skall för detta ändamål använda av CA godkända metoder och verktyg. Dock gäller för lokalt genererade mjukvaruskyddade nycklar att det är nyckelinnehavaren (samt dennes organisation) som helt på egen hand ansvarar för att tillfredsställande säkerhet uppnås i användarens lokala miljö.

Privata operatörsnycklar som används för att signera beställning av certifikat och spärrlistor samt därtill relaterade funktioner, skyddas minst lika säkert som lagring på aktivt kort.

6.2.2 Säkerhetskopiering av privata nycklar

Säkerhetskopia skall tas av CA:s privata nyckel. Hantering av säkerhetskopian omgärdas av motsvarande regler för åtkomstskydd som gäller för originalet.

6.2.3 Arkivering av privata nycklar

Inga centralt genererade nycklar för nyckelinnehavare eller för RA får arkiveras av CA.

6.2.4 Metod för förstörande av privat nyckel

CA:s privata utfärdarnycklar förstörs då deras användningstid löpt ut.

Säkerhetskopior förstörs genom att använt lagringsmedium förstörs permanent.

För operativa nycklar som lagras i utfärdarsystemets hårddisk i krypterad form, gäller följande:

1. Om utrustningen skall användas vidare i samma skyddade miljö sker överskrivning på sådant sätt att dessa nycklar ej kan återvinnas.
2. Om utrustningen skall användas utanför den skyddade zonen eller säljas förstörs hårddisken eller hårddiskarna eller monteras ur efter radering enligt 1 och lagras i säkerhetsskåp.

6.3 Andra aspekter på hantering av nyckelpar

Inga privata nycklar eller annan konfidentiell information inom CA och RA får lämna sin föreskrivna skyddsmiljö. Vid service och liknande situationer då föreskrivna skyddsmetoder inte kan upprätthållas avlägsnas alternativt förstörs alla lagringsmedia som innehåller känslig information eller känsliga privata utfärdarnycklar enligt 6.2.4.

6.3.1 Användningsperiod för publika och privata nycklar

Certifikat utfärdade enligt denna certifikatpolicy utfärdas dels för nya nycklar och dels för befintliga nycklar som certifierats tidigare i samband med att nycklarna genererades.

Certifikat för nyproducerade nycklar ges maximalt en giltighetstid på två år.

Certifikat för existerande nycklar ges maximalt en giltighetstid fram till dess att ursprungscertifikatets giltighetstid löper ut, dock max två år.

Certifikat som används av personal vid drift av CA-systemet ges maximalt en giltighetstid på två år.

Privata CA-nycklar används maximalt två år för att utfärda certifikat.

Självsignerade CA-certifikat ges en giltighetstid som maximalt täcker tiden från genereringstillfället fram till och med den tidpunkt som associerad privat nyckel upphör att användas för signering av certifikat.

Korscertifikat mellan olika generationer av CA nycklar ges maximalt en giltighetstid på två år plus en överlappningstid på maximalt sex månader (Den tid innan nyckelbytet som den nya nyckeln samt korscertifikat för gamla nyckeln finns tillgänglig för uppdatering).

6.4 SÄKERHET I DATORSYSTEM

Hela CA-systemet skall vara uppbyggt på ett sådant sätt att individuella roller enligt 5.2 kan separeras. Separering av roller på OS-nivå skall säkras genom dubbelbemanning.

De accesskontrollsystem som används skall vara så konstruerade att varje operatör identifieras på individuell nivå. Separering av roller på OS-nivå skall säkras genom dubbelbemanning.

Ovanstående skall gälla oavsett om en operatör agerar direkt inne ifrån CA:s centrala anläggning eller om operatören befinner sig i en utflyttad RA-funktion.

6.5 SÄKRING AV LEVNADSCYKEL

6.5.1 SÄKRING AV SYSTEMUTVECKLING

CA-systemets mjukvara skall utvecklas av tillverkare som använder en kontrollerad utvecklingsmiljö med ett väl dokumenterat kvalitetssäkringssystem.

6.5.2 SÄKRING AV SÄKERHETSADMINISTRATION

Driftsdokumentation som i detalj dokumenterar hur roller och behörigheter skall tillämpas och vidmakthållas, skall finnas.

6.6 SÄKRING AV NÄTVERK

Brandvägg som strikt avgränsar all typ av informationsutväxling som definierats som otillåten skall finnas implementerad. Endast den typ av informationsutväxling som strikt behövs för CA-tjänsten skall vara tillåten.

Informationsutväxling mellan RA och CA skall vara krypterad och transaktioner som påverkar användningen av CA:s privata utfärdarnycklar skall vara individuellt signerade.

Alla kommunikationsportar i CA-systemet som inte behövs skall vara deaktiverade och tillhörande mjukvarurutiner som inte används skall vara blockerade.

7 CERTIFIKAT OCH CRL-PROFILER

7.1 FORMATVERSIONER OCH PROFILER FÖR CERTIFIKAT

HCC certifikat utformas i enlighet med separat standard för HCC som upprättas av vård och omsorg i Sverige. [HCC, HCC1A]

7.2 CRL-PROFIL

Spärrlistor (CRL) utformas i enlighet med separat standard för HCC som upprättas av vård och omsorg i Sverige. [HCC, HCC1A]

8 SPECIFIKATIONSADMINISTRATION

8.1 PROCEDURER FÖR SPECIFIKATIONSFÖRÄNDRING

Carelink AB kan ändra i denna publikation under iakttagande av följande grundprinciper.

Förändring som bedöms innebära en märkbar försämring av säkerhetsnivå skall resultera i en ny publikation som ges en ny identitet (Policyobjektidentifierare enligt 1.2). På så vis kan certifikat utfärdade efter nya regler särskiljas från certifikat utfärdade efter tidigare gällande regler.

Uppdaterad policy publiceras publikt på www.carelink.se innan de nya reglerna tillämpas.

9 REFERERADE DOKUMENT

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

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

[HCC1A] Certifikat för svensk vård och omsorg HCC, Version 1A. Carelink 2003-02-01.

[HSA] Hälso- och sjukvårdens adressregister över enheter och personal för kommunikationstjänster. HSA-X.500, modell, struktur, krav, innehåll samt egna objekt och attribut. HSA-specifikation. Slutlig utgåva. Version 1.3, 1999-04-15.

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

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

[RApolicy] RA-policy för hälso- och sjukvårdscertifikat. Version 1. SITHS-projektet mars 2000.

[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.

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

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.

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