SITHS Anslutningsavtal

RA Policy

Innehållsförteckning

1 INLEDNING 5
1.1 ÖVERSIKT 5
1.2 IDENTIFIERING 5
1.3 MÅLGRUPPER OCH TILLÄMPLIGHET FÖR RA-POLICY 5
1.4 KONTAKTUPPGIFTER 6
2 ALLMÄNNA VILLKOR 7
2.1 FÖRPLIKTELSER 7
2.2 ANSVAR 8
2.3 FINANSIELLT ANSVAR 8
2.4 TOLKNING OCH VERKSTÄLLIGHET 8
2.6 ÅTKOMSTKONTROLL 9
2.7 REVISION 9
2.8 KONFIDENTIALITET 9
2.9 IMMATERIELLA RÄTTIGHETER 9
2.10 AVTAL/ÖVERENSKOMMELSER 9
3 IDENTIFIERING OCH AUTENTICERING 10
3.1 IDENTIFIERING VID REGISTRERING 10
3.2 BEGÄRAN OM SPÄRRNING AV CERTIFIKAT 11
4 OPERATIONELLA KRAV 11
4.1 BESTÄLLNING AV CERTIFIKAT 12
4.2 UTLÄMNANDE AV CERTIFIKAT 12
4.3 SPÄRRNING AV CERTIFIKAT 12
4.4 BESTÄLLNING AV SIHS KORT 12
4.5 PROCEDURER FÖR SÄKERHETSREVISION AV XRA-ARBETSPLATSER 13
4.6 ARKIVERING 13
4.7 PLANERING FÖR KATASTROF 13
4.8 UPPHÖRANDE AV RA-ORGANISATION 13
5 FYSISK, PROCEDURORIENTERAD OCH PERSONALORIENTERAD SÄKERHET 14
5.1 FYSISK SÄKERHET 14
5.2 PROCEDURORIENTERAD SÄKERHET 14

5.3 PERSONALORIENTERAD SÄKERHET 14
6 TEKNIKORIENTERAD SÄKERHET 15
6.1 GENERERING OCH INSTALLATION AV NYCKELPAR 15
6.2 UTLÄMNANDE AV PRIVAT NYCKEL TILL NYCKELINNEHAVARE VID HCC ORGANISATION OCH HCC FUNKTION 15
6.3 SKYDD AV PRIVAT NYCKEL 15
6.4 ARKIVERING AV PRIVATA NYCKLAR 15
6.5 SÄKERHET I DATORSYSTEM 15
7 REFERERADE DOKUMENT 16
BILAGA A - DEFINITIONER 16
BILAGA B - FÖRKORTNINGAR 20

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).

HCC finns specificerat i Certifikat för svensk vård och omsorg HCC [HCC].

Denna RA-policy kräver upprättande av ett separat dokument, RA-policy Practice Statement, RAPS. Mall för upprättande av RAPS finns framtagen av Inera AB och ska användas [RAPS mall].

Detta dokument ägs och förvaltas av Inera AB.

Revisionshistorik		
Datum	Författare	Kommentar
2000-05-15		Slutligt förslag från SITHS-projektet.
2003-06-16		Ny version med anledning av upprättande av RAPS-mall.
2006-04-26		Ny version med anledning av ny CA-policy, 2006-02-01 samt i samband med utarbetande av ny RAPS-mall. Fastställd av SITHS Förvaltningsgrupp.
2006-12-20		Ny version med anledning av framtagande av HCC 2.2 2008-03-03 Uppdatering av gällande version med anledning av övergång till Inera AB.
2008-06-24		Version 4 av SITHS RA-policy.
2011-01-17	Maria B.	Byte till Inera AB:s dokumentmall.

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 ska 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.

1.2 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-4}`
Objektidentifierare (OID) `{1.2.752.74.1.1.4}`

Denna RA-policy har namn och identifikation enligt nedan.

RA-policynamn `{SE-SITHS-RA-policy-4}`
Objektidentifierare (OID): `{1.2.752.74.1.2.4}`

1.3 MÅLGRUPPER OCH TILLÄMPLIGHET FÖR RA-POLICY

1.3.1 CERTIFICATION AUTHORITY (CA)

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

1.3.2 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 ska 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.

1.3.3 RA:S ÅTAGANDE

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

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

1.3.4 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 ORA
- Av RA eller ORA eventuellt utsedd LRA
- Av RA eller ORA eventuellt utsedd KRA
- Organisation som svarar för HSA och dess innehåll
- IT-infrastrukturorganisation (i förekommande fall)
- Arkiveringsorganisation (i förekommande fall)
- Nyckelinnehavare, NI

1.4 KONTAKTUPPGIFTER

1.4.1 ADMINISTRATIONSANSVARIG

Organisationen är ansvarig för förvaltning, administration och tillämpning av denna RA-policy.

1.4.2 KONTAKTPERSON

Frågor, synpunkter och förslag rörande denna RA-policy skickas till:
Organisation: Inera AB
Adress: Box 17703
Postnummer: 118 93
Ort: Stockholm
Telefon: 08-452 71 60
E-post: kundservice@inera.se
Webbplats: www.inera.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 avsnitt 4.6 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 HCC Organisation och HCC Funktion)
- att specifikationer av certifikatsinnehåll är giltiga med avseende på certifikatstyp, enligt kapitel 1 ovan och avseende uppgifter om nyckelinnehavare, enligt kapitel 3 nedan
- att följa operationella krav enligt kapitel 4.

2.1.2 FÖRPLIKTELSER AVSEENDE XRA

RA har följande förpliktelser avseende sina xRA:

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

2.1.3 FÖRPLIKTELSE FÖR NYCKELINNEHAVARE

Nyckelinnehavare som tilldelas HCC förpliktigar sig att:

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

2.1.4 REGLER OCH RUTINER SOM SKA 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 [HSA-policy].

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 xRA-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 4.

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 FINANSIELLT ANSVAR

Ej tillämpligt för RA-policyn.

2.4 TOLKNING OCH VERKSTÄLLIGHET

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

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

2.5 AVGIFTER

Ej tillämpligt för RA-policyn.

2.6 ÅTKOMSTKONTROLL

Certifikat och spärrlistor ska publiceras i enlighet med vård och omsorgsorganisationens bestämmelser vilket bl.a. regleras i gällande HSA-policy.

2.7 REVISION

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

Vid upptäckt av brister eller behov av förändringar ska 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.

2.8 KONFIDENTIALITET

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

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

2.9 IMMATERIELLA RÄTTIGHETER

Ej tillämpligt för RA-policyn.

2.10 AVTAL/ÖVERENSKOMMELSER

2.10.1 AVTAL MED CA

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

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

2.10.2 ÖVERENSKOMMELSE MED DEN ORGANISATION SOM RA OCH XRA TILLHÖR

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

- överenskommelse/beslut avseende krav och skyldigheter för RA
- överenskommelse/beslut avseende krav och skyldigheter för ORA (i förekommande fall)
- överenskommelse/beslut avseende krav och skyldigheter för LRA
- överenskommelse/beslut avseende krav och skyldigheter för KRA
- överenskommelse/beslut med xRA: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 ska RA följa CA-policy, avsnitt 3.1. Initial beställning av organisation med dess rätt till domännamn, rätt till certifikat, rätt att beställa och mottaga certifikat ska alltid verifieras av oberoende källor. Resultat och verifieringens tillvägagångssätt ska dokumenteras och arkiveras.

3.1.2 IDENTIFIERINGSPROCEDUR GENOMFÖRD AV RA/ORA/LRA/KRA

RA/ORA 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/ORA/LRA ska upprätta underlag för certifikatsbeställning verifierade mot adekvat ansökan beslutad av verksamhetsansvarig. KRA ska upprätta underlag för kortbeställning verifierade mot adekvat ansökan
beslutad av verksamhetsansvarig.

Vid certifikatsbeställning görs identitetskontroll enligt någon av nedanstående procedurer:

- vid HCC person 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 HCC Organisation och HCC Funktion genom personlig närvaro av behörig representant som uppvisar godkänd och giltig legitimationshandling vid första tillfället; vid efterföljande certifikatsbeställningar behövs ej någon personlig identifiering eftersom personen är elektroniskt känd.

3.1.3 KRAV PÅ PERSONLIG NÄRVARO

RA/ORA utlämnar privata nycklar samt tillämpliga lösenord eller PIN-koder vid HCC Organisation och HCC Funktion. Utlämnandet sker personligen till behörig representant mot uppvisande av godkänd och giltig legitimation eller via e-post med användande av S/MIME. Behörig representant måste ha ett giltigt HCC Person. Dessa rutiner beskrivs närmare i RAPS.

3.1.4 AUTENTICERING AV ORGANISATION OCH FUNKTION INOM EN ORGANISATION

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

Initial beställning av organisation med dess rätt till domännamn, rätt till certifikat, rätt att beställa och mottaga certifikat ska alltid verifieras av oberoende källor. Resultat och verifieringens tillvägagångssätt ska dokumenteras och arkiveras. Dessa rutiner beskrivs närmare i RAPS.

3.2 BEGÄRAN OM SPÄRRNING AV CERTIFIKAT

Spärrning av certifikat kan initieras av:

- organisationen genom initiativ från RA/ORA/LRA/NI eller Nyckelinnehavares verksamhetsansvarige (t.ex. då anställning upphör; organisation förändras)
- RA/ORA 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 och
- beställning av kort.

Dessa uppgifter för RA och xRA ska beskrivas mer detaljerat i RAPS.

Denna policy definierar de operationella krav som rör:

- CA,
- Organisationen,
- RA-organisationen inklusive xRA,
- katalogorganisationen,
- organisationen som ansvarar för IT-infrastruktur och
- 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 beställning kontrolleras av RA/ORA/LRA genom att nyckelinnehavarens lämnade personuppgifter verifieras mot HSA-katalogen. RA/ORA/LRA beställer certifikat hos CA.
- beställningshandlingar arkiveras enligt RAPS.

4.2 UTLÄMNANDE AV CERTIFIKAT

Utfärdandet av ett certifikat representerar CA:s acceptans av RA/ORA:s beställning.
Vid utlämnande av HCC Organisation och HCC Funktion fullföljs följande moment:

- RA/ORA mottar certifikat samt privata nycklar
- Koder/lösenord skickas från CA till nyckelinnehavare i krypterad form
- RA/ORA ansvarar för att utlämnandet av certifikat och privata nycklar sker till nyckelinnehavare och att denne identifieras enligt CA-policy kapitel 3.1.

4.3 SPÄRRNING AV CERTIFIKAT

- Spärrning av HCC kan beslutas av verksamhetsansvarig eller Nyckelinnehavaren själv.
- RA/ORA/LRA ombesörjer och ansvarar för att spärrningsbegäran skickas till CA.
- Orsaker till spärrning regleras och beskrivs i CA-policy och RAPS.
- RA/ORA/LRA ansvarar för att verksamhetsansvarig och nyckelinnehavare informeras om spärrning av HCC i enlighet med CA-policy.
- Spärrningsbegäran från RA/ORA/LRA ska ske enligt CA-policy 4.4.3.

4.4 BESTÄLLNING AV SIHS KORT

Rutiner för detta ska framgå av RAPS.

4.5 PROCEDURER FÖR SÄKERHETSREVISION AV XRA-ARBETSPLATSER

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

4.6 ARKIVERING

- Den information som lagras hos CA arkiveras enligt CA-policyn kapitel 4.6.
- xRA 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 arkivering inom vård och omsorg.

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

4.7 PLANERING FÖR KATASTROF

Katastrofplan ska finnas framtagen i enlighet med organisationens övriga krav på katastrofberedskap. RAPS ska innehålla referens till katastrofplanen för RA och xRA.
Vid kompromettering av CA-nyckel ska RA informera sin organisation enligt CA-policy.

4.8 UPPHÖRANDE AV RA-ORGANISATION

Vid upphörande av RA-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 och
- 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 och xRA ska 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 ska 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,
- ORA (i förekommande fall),
- LRA,
- KRA och
- Informationssäkerhetsansvarig.

5.3 PERSONALORIENTERAD SÄKERHET

RA-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 uppdraget.

Alla företrädare för organisationen ska genomgå utbildning och erhålla 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 HCC ORGANISATION OCH HCC FUNKTION

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.

6.3 SKYDD AV PRIVAT NYCKEL

Privata nycklar ska 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.

Det är RA-organisationen som ansvara för att tillfredsställande säkerhet uppnås i användarnas lokala miljöer. Om en privat nyckel nyttjas av programvara på en server, så kan skyddet anses vara fullgott om den lokala infrastrukturen skyddar certifikatet med hjälp av digitala åtkomsträttigheter på filsystemet.

6.4 ARKIVERING AV PRIVATA NYCKLAR

Inga privata nycklar tillhörande Person HCC arkiveras inom RA-organisationen. Privata nycklar tillhörande HCC Organisation eller HCC Funktion får endast arkiveras för backupändamål. Om sådan arkivering sker ska den dokumenteras enligt rutin i RAPS.

6.5 SÄKERHET I DATORSYSTEM

Hela RA-systemet ska 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 ska 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 operativsystemnivå används dubbelbemanning.

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

7 REFERERADE DOKUMENT

SITHS Anslutningsavtal
* senaste version finns tillgänglig på Ineras webbplats www.inera.se.

BILAGA A - DEFINITIONER

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 hälsooch 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 ska 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 ska 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.

BILAGA B - 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*
SITHS	Säker IT i Hälso- och sjukvård
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.