Registration Authority Practice Statement RAPS

<Org.namn>

<Ange Org.nr>

INNEHÅLLSFÖRTECKNING

BILAGOR

FIGURER

Revisionshistorik

Version	Datum	Status
		RAPS MALL v4.8

1 Inledning

1.1 Översikt

Detta dokument är den Registration Authority Practice Statement (RAPS) som beskriver hur RA-organisationen är utformad för <Org.namn> för att uppfylla de krav som anges i SITHS CA:s RA-policy.
SITHS CA ger ut elektroniska certifikat, så kallade Health Care Certificate (HCC), för personer, organisationer och funktioner inom svensk vård och omsorg.
Denna RAPS beskriver de förutsättningar, ansvar, procedurer och rutiner som tillämpas vid beställning och spärrning av HCC inom RA-organisationen. Målgrupp för dokumentet är SITHS CA, RA, ORA, KRA, LRA och verksamhetsansvariga inom <Org.namn>.

1.2 Bilagor

Bilagor som följer med denna RAPS:

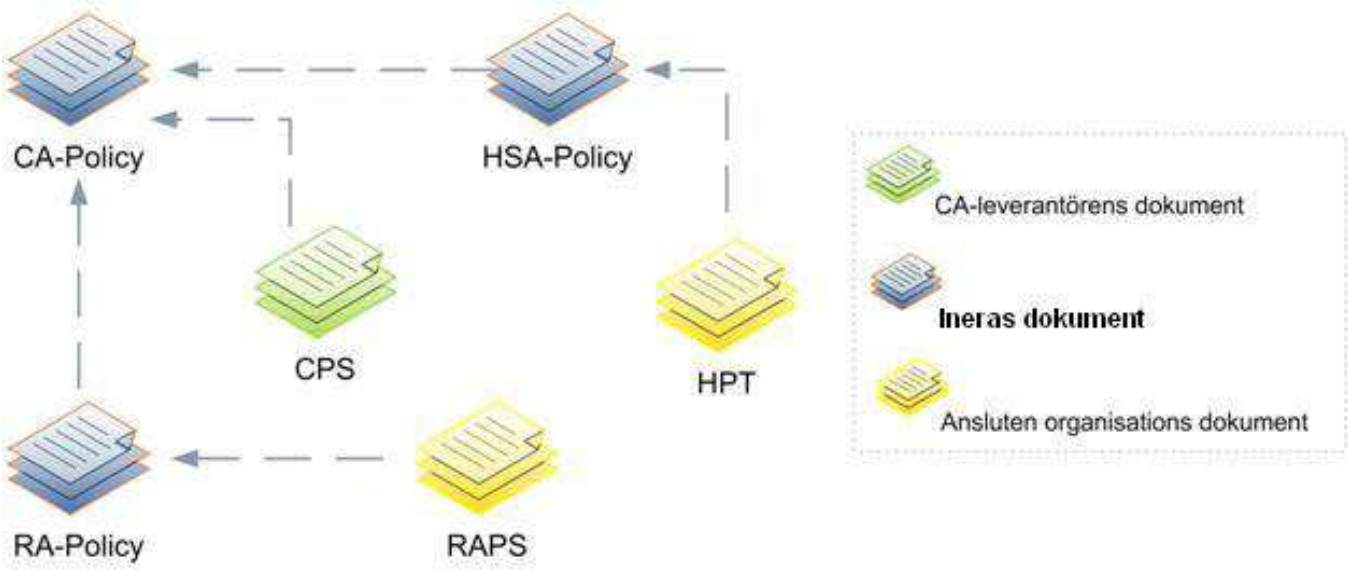
Underbilaga 1 Rutiner vid missbruk av certifikat
Underbilaga 2 Plan för genomförande av intern kontroll
Underbilaga 3 Kontinuitetsplan med rutiner för avbrottshantering
Underbilaga 4 Lista på organisationer som omfattas av denna RAPS
Underbilaga 5 Rutin för arkivering av privata nycklar
Underbilaga 6 Bemanning av roller för denna RAPS
Underbilaga 7 Rutiner för kort- och certifikatutgivning

1.3 Identifiering

De rutiner och åtaganden som följer av denna RAPS är endast tillämpliga i samband med sådana certifikat där nedanstående CA- och RA-policier åberopas.

Policynamn för CA-policy är	{SE-SITHS-CA-Policy-4}
Objektidentifierare (OID) för denna policy är:	{1.2.752.74.1.1.4}
RA-policynamn:	{SE-SITHS-RA-Policy-4}
Objektidentifierare (OID):	{1.2.752.74.1.2.4}
Namn på denna RAPS är:	{SE-SITHS-RAPS-<Ange Org.nr>}
Objektidentifierare (OID för denna RAPS är:	{1.2.752.74.1.3.4.}

1.4 Relation till övriga styrande dokument



Figur 1. RAPS relation till övriga styrande dokument

CA-policy publiceras av Inera AB och är det dokument som beskriver de övergripande kraven för procedurer och rutiner som ska tillämpas vid hantering av HCC.

Certification Practice Statement (CPS) publiceras av CA:s driftleverantör och beskriver rutiner och organisation för hur CA:s driftleverantör tillämpar Inera ABs CA-policy.

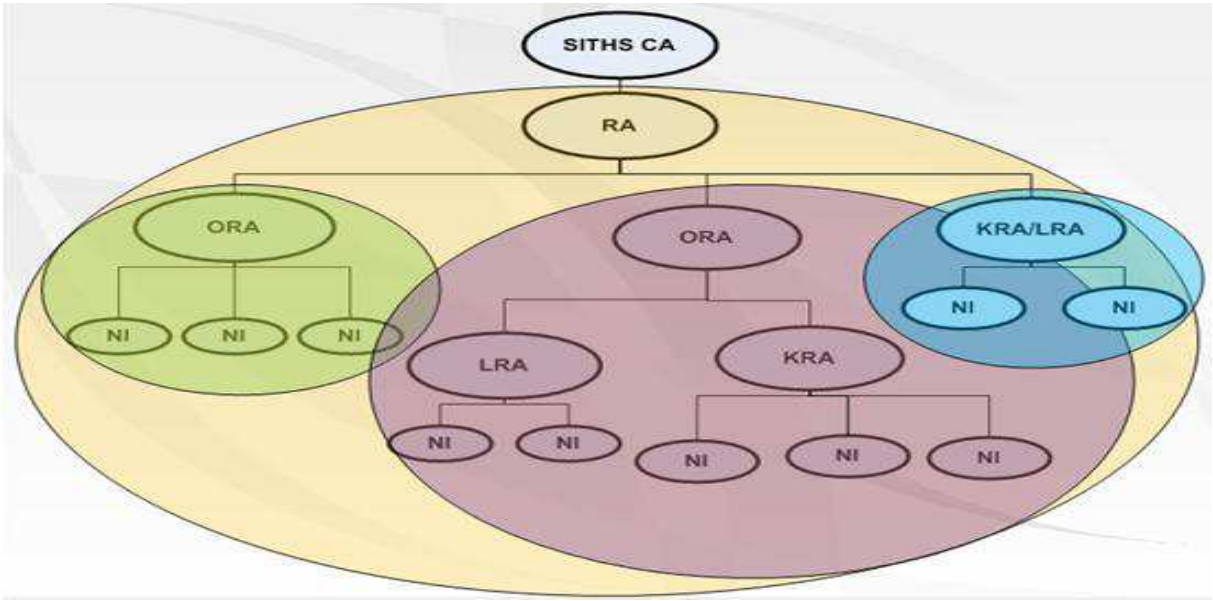
RA-policy publiceras av Inera AB och är det dokument som beskriver kraven på procedurer och rutiner som ska tillämpas i RA-organisationer vid hantering av HCC.

Tillämpningsanvisning RAPS (detta dokument) beskriver RA-organisationen och rutiner för att uppfylla de krav och förpliktelser som anges i CA-policy, CPS och RA-policy. RAPS arkiveras av respektive RA-organisation och kopia överlämnas till Inera AB.

Policy för HSA publiceras av Inera AB och är det dokument som beskriver hur en lokal katalog för aktörer inom vård- och omsorg skall upprättas och underhållas för att kunna ingå i HSA.

HSA Katalogpolicytillämpning (HPT) beskriver <Org.namn>s rutiner och organisation för tillämpning av HSA-policyn. Vår organisation ansvarar för upprättande och publicering av HPT.

1.5 RA-organisation



Figur 2. Exempel på roller inom RA-organisationen

1.5.1 Organisationens roller

<Org.namn> tecknar avtal med SITHS CA (Inera AB) om rätt att utnyttja HCC (i SITHS CA). I avtalet åtar sig <Org.namn> att upprätta en organisation för beställning och återkallande av HCC, en RA-organisation. Ett exempel på en RA-organisation illustreras i figur 2.

RA har det övergripande ansvaret för RA-organisationen. För effektivare administration av RA-organisationen kan en eller flera RA personer etableras. Verksamhetsansvarig för vår organisation upprättar och bemannar RA och meddelar detta till SITHS CA. Förändringar av RA personal meddelas direkt till SITHS CA. RA upprättar och bemannar ORA (om så är tillämpbart), KRA samt LRA. ORA/KRA/LRA ansvarar för hanteringen av HCC inom sin del av RA-organisationen. Organisationen upprättar även en supportorganisation samt definierar behöriga beställare för kommunikation med driftleverantörens kundstöd.

Inom varje förvaltning (motsvarande) kan en ansvarig person, ORA, utses för certifikatshantering för en eller flera förvaltningar. Om ORA rollen ej tillämpas äger RA detta ansvar själv. Dennes uppgift är att bygga upp och bemanna en organisation av KRA-personer, benämns även korthandläggare, och LRA-personer inom sin del av RA-organisation. RA/ORA utfärdar HCC till nyckelinnehavare (NI), som kan vara personer, funktioner och organisationer. HCC för personer kan tilldelas anställda inom vår organisation eller till personer som utför uppdrag åt vår organisation.

KRA utfärdar HCC till nyckelinnehavare (NI) i samband med beställning av nytt kort. Beställning av nytt kort kan göras till personer som är anställda inom vår organisation eller till personer som utför uppdrag åt vår organisation.

LRA utfärdar HCC till nyckelinnehavare (NI) i samband med beställning av certifikat för personer och reservkort. HCC för personer kan tilldelas anställda inom vår organisation eller till personer som utför uppdrag åt vår organisation.

Säkerhetsansvarig ansvarar för uppföljning av verksamhetens efterlevnad av utgivningsprocesser av SITHS-kort och certifikat. Uppdraget innebär planering av säkerhetsrevisioner, mm. Person som innehar rollen som Säkerhetsansvarig får inte inneha någon annan roll i RA-organisationen, undantag LÄS.

Registeransvarig ansvarar för register över underskrivna kortkvittenser för utfärdade SITHS-kort.

Inom vår organisation har vi följande roller:

☒ Säkerhetsansvarig

☒ Registeransvarig

☒ RA

☐ ORA

☐ KRA

☐ LRA

1.6 Nyckelinnehavare och certifikatstyper

Tabellen nedan visar vilka typer av nyckelinnehavare och certifikatttyper som finns inom RA-organisationen.

Typ av nyckelinnehavare (NI)	Certifikattyp	Certifikatform
Person med giltig e-legitimation	HCC Person	Sekundärcertifikat
Person utan svenskt personnummer, t ex "Samordningsnummer"	HCC Person	Sekundärcertifikat
Person utan svenskt personnummer, t ex "Passnummer"	HCC Person	Sekundärcertifikat på reservkort
Organisation/Organisationsenhet	HCC Organisation	Primärcertifikat
Verksamhetsfunktion	HCC Funktion	Primärcertifikat
System eller tjänst	HCC Funktion	Primärcertifikat

Personer, funktioner och organisationer finns upplagda som objekt i HSA med den kvalitet som anges i HSA-policyn. Detta är en förutsättning för att kunna ge ut HCC för personer, funktioner och organisationer.

1.6.1 HCC Person

HCC Person utfärdas till fysisk person anställd inom vår organisation. HCC Person kan utfärdas till personer inom en organisation som har avtal med vår organisation och till personer som utför uppdrag åt vår organisation. HCC Person lagras i HSA och om så önskas på SITHS-kortet.

1.6.1.1 Tidsbegränsat HCC Person

Tidsbegränsat HCC Person kan utfärdas på reservkort till person som inte kan erhålla ordinarie kort. Giltighetstid för tidsbegränsat certifikat, på reservkort, sätts utifrån behov, dock till maximalt 180 dagar alternativt anställningens längd. Tidsbegränsat HCC Person lagras i HSA och om så önskas på reservkortet.

1.6.1.2 Tillfälligt HCC Person

Tillfälligt HCC Person kan utfärdas på reservkort till person anställd inom vår organisation, till person inom en organisation som har avtal med vår organisation eller till person som utför uppdrag åt vår organisation. Giltighetstid för tillfälligt certifikat, på reservkort, sätts utifrån verksamhetens behov, dock till maximalt 180 dagar. Tillfälligt HCC Person lagras i HSA och om så önskas på reservkortet.

1.6.2 HCC Organisation

HCC Organisation utfärdas till en organisationsenhet inom vår organisation eller till en organisation som har avtal med vår organisation.

1.6.3 HCC Funktion

HCC Funktion utfärdas till funktion inom vår organisation eller funktion inom organisation som har avtal med vår organisation. Funktionen kan vara en verksamhetsfunktion, en tjänst eller ett system.

1.7 Kontaktuppgifter

Frågor angående denna RAPS adresseras till:

RA Funktionen

Adress

E-post

2 Allmänna villkor

2.1 Förpliktelser och åtaganden

Möjlighet till ställföreträdande personer finns på alla nivåer i organisationen.

2.1.1 <Org.namn> - SITHS-CA

Vår organisation ansvarar för att upprätta avtal med SITHS CA och utse RA samt ställföreträdande RA. Då RA slutar sitt uppdrag meddelar vår organisation detta till SITHS CA inom skälig tid. Behörigheter för RA tas då bort och delas ut till efterträdare.

2.1.2 RA - SITHS-CA

RA har det övergripande ansvaret för vår organisations RA-organisation. RA ansvarar för att vår organisations RA-organisation, inklusive annan uppdragstagare som eventuellt ingår, följer CA-policy, RA-policy och denna RAPS. RA ansvarar för att RAPS tas fram samt uppdateras vid förändringar i CA-policy, RA-policy och i den egna organisationen. Enligt bestämmelser reglerade i SITHS CA:s CPS, utser RA behöriga ORA personer och tilldelar åtkomsträttigheter i SITHS CA:s behörighetssystem (SITHS Admin). RA kan även utse behöriga KRA/LRA personer och tilldela åtkomsträttigheter i SITHS CA:s behörighetssystem.

2.1.3 RA - ORA

RA utser, om tillämpbart, ORA i RA-organisationen, och ger behörighet samt ansvarar för att dessa personer utbildas i gällande rutiner. ORA utses i samråd med respektive verksamhetsansvarig och ansvarar, inom sitt ORA-område, för att RAPS tillämpas. RA har en förteckning över behöriga ORA personer i organisationen. Då en ORA slutar sitt uppdrag meddelar verksamhetsansvarig inom ORA-området detta till RA inom skälig tid och behörigheter för ORA tas bort.

2.1.4 RA/ORA - KRA

RA eller ORA utser KRA i RA-organisationen, och ger behörighet samt ansvarar för att dessa personer utbildas i gällande rutiner. KRA utses i samråd med respektive verksamhetsansvarig och säkerhetsansvarig för SITHS-korten och ansvarar, inom sitt KRA-område, för att RAPS och driftleverantörens policy för utgivande av e-legitimationer tillämpas samt i förekommande fall att SIS-reglementet följs. RA/ORA har en förteckning på behöriga KRA personer inom det egna ansvarsområdet, och KRA-områdena är klart definierade. Då en KRA slutar sitt uppdrag meddelar verksamhetsansvarig inom KRA-området detta till RA/ORA och DNV (om SIS-kort används) samt till kortleverantören inom skälig tid. Behörighet för KRA tas bort.

2.1.5 RA/ORA - LRA

RA eller ORA utser LRA i RA-organisationen, och ger behörighet samt ansvarar för att dessa personer utbildas i gällande rutiner. LRA utses i samråd med respektive verksamhetsansvarig och ansvarar, inom sitt LRA-området, för att RAPS tillämpas. RA/ORA har en förteckning på behöriga LRA personer inom det egna ansvarsområdet, och LRA-områdena är klart definierade. Då en LRA slutar sitt uppdrag meddelar verksamhetsansvarig inom LRA-området detta till RA/ORA inom skälig tid och behörigheter för LRA tas bort.

2.1.6 KRA/LRA - NI

KRA/LRA ansvarar för att beställa HCC och för att begära spärrning av HCC enligt denna RAPS. KRA/LRA tillser att relevant information, bland annat rutiner vid spärrning och felanmälan, ges till NI. Då en förändring sker, som påverkar certifikatsinnehållet, eller då NI slutar sitt uppdrag, ansvarar NI:s verksamhetsansvarig för att KRA/LRA meddelas snarast så att HCC kan spärras och eventuellt nytt HCC kan utfärdas.

Om NI inte har kontroll över SITHS-kortet, eller tillhörande PIN- och PUK-koder, kontaktas KRA/LRA. Motsvarande gäller för tilldelat reservkort.

2.1.7 RA/ORA - Behörig representant

RA/ORA ansvarar för att beställa HCC Organisation eller HCC Funktion och för att begära spärrning av dessa HCC enligt denna RAPS. RA/ORA tillser att relevant information, bl.a. rutiner vid spärrning och felanmälning, ges till den behöriga representanten. RA/ORA har en förteckning över alla behöriga representanter och dess ansvar inom det egna RA/ORA-området. Då en förändring sker, som påverkar certifikatsinnehållet, eller då den behöriga representanten slutar sitt uppdrag, ansvarar verksamhetsansvarig (med ansvar för den behöriga representanten) för att RA/ORA meddelas snarast så att HCC kan spärras och eventuellt nytt HCC kan utfärdas.

Om behörig representant inte har kontroll över PIN-koder eller då den privata nyckeln associerad med HCC Organisation eller HCC Funktion misstänks vara röjd, kontaktas RA/ORA

2.1.8 Missbruk av certifikat

Om missbruk av certifikat upptäcks ska detta hanteras i enlighet med underbilaga 1.

2.2 Friskrivning från ansvar

Vår organisation och personer inom vår organisations RA-organisation ansvarar inte för följder av:

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

2.3 Revision

2.3.1 Extern kontroll

SITHS CA har rätt att revidera ansluten RA-organisation och meddelar skriftligen RA-organisationen om detta.

2.3.2 Intern kontroll

Intern kontroll genomförs löpande för att tillse att denna RAPS och motsvarande RA-policy efterlevs inom vår organisation. Plan för genomförande av intern kontroll beskrivs i underbilaga 2.

2.4 Konfidentialitet

Frågor 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) samt Socialtjänstlagen (SoL).

För kontinuerlig kortredovisning, som sker från driftleverantören och innehåller viss integritetskänslig information som nyckelinnehavares personnummer, ställs krav på säker informationsöverföring, t ex genom krypterad informationsöverföring.

RAPS tillämpas så att gällande lag om konfidentialitet uppfylls.

3 Rutiner för identifiering

3.1 HCC Person

3.1.1 Identifiering vid beställning av HCC Person

Inom RA-organisationen krävs, vid initial beställning av HCC Person och när man efter en kortförlust ska få ett nytt SITHS-kort med HCC Person, personlig närvaro av NI med giltig legitimation. Vid nästkommande beställning av HCC Person på befintligt SITHS -kort krävs inte personlig närvaro av NI som har/eller har haft ett giltigt HCC. Den elektroniska id-handlingen (e-legitimation) på befintligt kort räcker. Vid utlämning av reservkort måste den anställde personligen närvara hos ORA/LRA för identitetskontroll.

Då en nyckelinnehavare, NI, identifierar sig sker det enligt ett av följande alternativ:

1. Personlig närvaro av NI med giltig id-handling (SIS godkänd eller motsvarande).
2. Elektronisk identifiering av NI med giltig e-legitimation
3. Att annan känd person inom organisationen skriftligen går i god för NI:s identitet.

Sättet som NI identifieras på dokumenteras i systemet av xRA.

3.1.2 Identifiering vid spärrning av HCC Person

Då RA/ORA/KRA/LRA via CA begär spärrning av HCC Person identifierar sig RA/ORA/KRA/LRA elektroniskt med hjälp av sitt HCC mot SITHS CA.

Då en nyckelinnehavare, NI, begär spärrning, via RA/ORA/KRA/LRA, av sitt certifikat identifieras NI enligt ett av följande alternativ:

1. Av NI signerad elektronisk beställning, t ex genom signerad e-post.
2. Personlig närvaro av NI med giltig id-handling (SIS godkänd eller motsvarande).
3. Som reservrutin, om det misstänks föreligga risk för missbruk av en privat nyckel, associerad med ett certifikat, kan en förenklad form av identifiering göras. Detta görs genom motringning och/eller genom att ställa kontrollfrågor.

Verksamhetsansvarig kan begära spärrning via RA/ORA/KRA/LRA av annan persons certifikat och identifieras då enligt ett av följande alternativ:

1. Signerad elektronisk beställning av verksamhetsansvarig, t ex genom signerad e-post eller sin personliga e-legitimation.
2. Personlig närvaro av verksamhetsansvarig med giltig id-handling (SIS godkänd eller motsvarande).

Verksamhetsansvarig går här i god för NI:s identitet och att NI:s certifikat skall spärras.

3.1.3 Identifiering vid beställning av kort utan HCC

Inom RA-organisationen krävs, vid initial beställning av kort personlig närvaro av NI med giltig legitimation. Vid utlämning av reservkort måste den anställde inställa sig personligen hos RA/ORA/LRA för identitetskontroll.

Då en nyckelinnehavare, NI, identifierar sig sker det enligt ett av följande alternativ:

1. Personlig närvaro av NI med giltig id-handling (SIS godkänd eller motsvarande).
2. Att annan känd person inom organisationen skriftligen går i god för NI:s identitet (intygsgivning).

3.2 HCC Organisation och HCC Funktion

3.2.1 Identifiering vid beställning av HCC Organisation och HCC Funktion

Vid utfärdande av HCC Organisation och HCC Funktion sker alltid identifiering av behörig representant genom en giltigt id-handling eller giltigt HCC person enligt någon av punkterna i avsnittet 3.1.1 Identifiering vid beställning av HCC person.

3.2.2 Identifiering vid spärrning av HCC Organisation och HCC Funktion

Vid spärrning av HCC Organisation och HCC Funktion sker identifiering av behörig representant enligt någon av punkterna i avsnittet 3.1.2 Identifiering vid spärrning av HCC person.

4 Rutiner för certifikatshantering

4.1 Beslut om beställning av HCC

Verksamhetsansvariga inom respektive RA/ORA/KRA/LRA-område beslutar om beställning av HCC inom sitt ansvarsområde.

4.2 Beställning av HCC

4.2.1 HCC Person till nytt SITHS-kort

1. NI:s verksamhetsansvarige kontaktar sin RA/KRA. KRA förvissar sig om att NI har uppdrag inom det egna ansvarsområdet samt att uppgifterna som ska ingå i HCC Person är korrekta.
2. RA/KRA gör en beställning av HCC-underlag i systemet. Denna beställning kan göras innan personen anländer.
3. Personen identifieras enligt 3.1.1 och identifieringssättet skrivs in i systemet.
4. Beställningen av underlaget för HCC till nytt SITHS-kort fullgörs och signeras av RA/KRA.
5. Kortet levereras till organisationens kontor efter ca fem arbetsdagar.
6. Efter ca sju arbetsdagar får personen ett PIN-brev till sin folkbokföringsadress och kan sedan hämta ut sitt SITHS kort med HCC Person hos RA/KRA.
7. Personen identifieras enligt 3.1.1 och identifieringssättet skrivs in i systemet. Mottagandet av kortet kvitteras enligt 6.1 Utlämnande av privat nyckel.

4.2.2 HCC Person till befintligt SITHS-kort

1. NI kontaktar sin RA/ORA/KRA/LRA som förvissar sig om att NI har uppdrag inom det egna RA/ORA/KRA/LRA-området samt att uppgifterna som ska ingå i HCC är korrekta.
2. Personen identifieras enligt 3.1.1.
3. RA/ORA/KRA/LRA gör en beställning av HCC-underlag i systemet. Giltighetstiden sätts till anställningens slut eller maximalt till primärcertifikatets giltighetstid.
4. Beställningen av HCC Person signeras av RA/ORA/KRA/LRA och därefter kan NI hämta sitt HCC Person i SITHS Självadministration som samtidigt lagrar HCC Person i HSA.

4.2.3 HCC Person till SITHS reservkort

1. NI:s verksamhetsansvarige eller NI personligen kontaktar sin RA/ORA/LRA som förvissar sig om att NI har uppdrag inom det egna RA/ORA/LRA-området samt att uppgifterna som ska ingå i HCC är korrekta.
2. RA/ORA/LRA gör en beställning och signerar HCC-underlaget i systemet. Giltighetstiden för HCC Person på reservkort ska sättas utifrån behov i varje enskilt fall, maximalt 180 dagar.
3. Personen identifierar sig enligt 3.1.1 och identifieringssättet skrivs in i systemet när NI hämtar reservkortet hos RA/ORA/LRA. Mottagandet av kortet kvitteras enligt 6.1 Utlämnande av privat nyckel.
4. NI hämtar sitt HCC Person i SITHS Självadministration som samtidigt lagrar HCC Person i HSA.

4.2.4 HCC Organisation och HCC Funktion (PKCS#12)

1. Behörig representant kontaktar sin RA/ORA.
2. Personen identifieras enligt 3.2.1.
3. RA/ORA kontrollerar att representanten är behörig beställare av HCC Organisation eller HCC Funktion enligt överenskommelse med verksamhetsansvarig samt att behörig representant och aktuell organisation/funktion finns upplagd i HSA på rätt nivå och med rätt uppgifter.
4. RA/ORA beställer HCC Organisation eller HCC Funktion och anger behörig representant. Behörig representant måste ha ett giltigt HCC Person, vilket fungerar som elektronisk id handling och kommer att användas vid signering och kryptering vid försändelser via S/MIME krypterad e-post.
5. CA genererar HCC och nyckelpar. RA/ORA sparar ner PKCS#12 filer med HCC.
6. CA skickar lösenord för PKCS#12 filer och PIN-koder via krypterat e-post till behörig representants e-postadress.
7. Om behörig representant saknar HCC Person kan HCC Funktion och HCC Organisation levereras med e-post om och endast om PIN-koder sänds via annan media, t ex ett oberoende SMS-textmeddelande. RA/ORA ansvarar här för att PIN-koder, via krypterad e-post, först sänds till medarbetare hos RA/ORA med giltigt HCC Person med slutgiltig leverans till behörig representant.
8. Behörig representant kvitterar mottagandet för PKCS#12 filer och RA/ORA arkiverar kvittens om utlämnande av HCC.

Mottagande av koder och nycklar sker enligt 6.1.3 Utlämnande av privat nyckel i samband med utfärdande av HCC Organisation och HCC Funktion (PKCS#10 och PKCS#12).

4.2.5 HCC Funktion (PKCS#10)

1. Behörig representant kontaktar sin RA/ORA.
2. Personen identifieras enligt 3.2.1.
3. RA/ORA kontrollerar att representanten är behörig beställare av HCC Funktion enligt överenskommelse med verksamhetsansvarig samt att behörig representant och aktuell funktion finns upplagd i HSA på rätt nivå och med rätt uppgifter.
4. Behörig representant överlämnar certifikatbegäran (CSR) till RA/ORA, t ex genom signerad e-post.
5. RA/ORA beställer HCC Funktion med hjälp av en CSR och anger behörig representant. Saknas behörig representant i HSA anges medarbetare hos RA/ORA.
6. CA genererar HCC. Därefter skickar CA PKCS#10 objekt med HCC till RA/ORA. RA/ORA sparar ner PKCS#10 objektet med HCC på en fil och överlämnar detta till behörig representant, t ex genom signerad e-post.
7. Behörig representant kvitterar mottagandet av HCC Funktion för PKCS#10 och RA/ORA arkiverar uppgifter om utlämnandet av HCC Funktion.

Mottagande av koder och nycklar sker enligt 6.1.3 Utlämnande av privat nyckel i samband med utfärdande av HCC Organisation och HCC Funktion (PKCS#10 och PKCS#12).

4.3 Spärrning av HCC

4.3.1 Godkända anledningar till att begära spärr av HCC

HCC spärras om något av följande har inträffat:

- förhållanden som påverkar certifikatsinnehållet har ändrats,
- någon uppgift i HCC är eller misstänks vara felaktig,
- NI har tappat kontrollen över kortet eller koderna,
- NI:s e-legitimation har blivit spärrad
- NI:s e-legitimation inte är tillgängligt för NI (kortförlust),
- den privata nyckeln har röjts eller
- SITHS-/reservkortet återlämnas.

4.3.2 Undantag

Om NI inte har tillgång till sitt kort, men säger sig komma att få tillgång till detta snart igen, samtidigt som NI garanterar att ingen obehörig kan använda de på kortet lagrade privata nycklarna, kan RA/ORA/KRA/LRA välja att inte spärra HCC.

4.3.3 Spärrbegäran

Följande roller kan begära spärrning av HCC:

- NI kan av RA/ORA/KRA/LRA begära spärrning av sitt eget HCC,
- verksamhetsansvarig kan av RA/ORA/KRA/LRA begära spärrning av HCC inom egen organisation,
- behörig representant kan av RA/ORA begära spärrning av det HCC Organisation eller HCC Funktion eller
- RA/ORA/KRA/LRA kan begära spärrning av HCC inom det egna ansvarsområdet.

4.3.4 Spärrning

Följande roller kan utföra spärr av HCC via CA:

- NI kan själv via "SITHS Självadministration" spärra sitt eget HCC,
- RA kan spärra HCC hos CA inom eget RA-område,
- ORA kan spärra HCC hos CA inom eget ORA-område,
- KRA kan spärra HCC Person hos CA inom eget KRA-område eller
- LRA kan spärra HCC Person hos CA inom eget LRA-område.

4.4 Arkivering

4.4.1 RA

RA ansvarar för att följande arkiveras:

- RA-organisationens avtal med SITHS CA,
- RA-organisationens godkända RAPS,
- RA-organisationens förteckning av utsedda RA och dess ställföreträdande, inklusive historik,
- RA-organisationens förteckning av utsedda ORA personer och ställföreträdande samt deras områden, inklusive historik,
- där ORA personer inte förekommer ansvarar RA för förteckning av RA-organisationens utsedda KRA/LRA personer, behöriga representanter och dess ställföreträdande samt deras områden, inklusive historik,
- RA-organisationens förteckning över avtal med andra parter, t ex driftleverantörer, SIS/DNV eller andra ingående organisationer, inklusive historik och
- uppgifter vid utfärdande av HCC Organisation och HCC Funktion, t ex kvittens, identitet på behörig representant och datum för utlämnandet av HCC.

4.4.2 ORA

ORA ansvarar för att följande arkiveras:

- ORA-områdets förteckning av utsedda KRA och LRA personer och ställföreträdande samt deras områden, inklusive historik,
- ORA-områdets förteckning av utsedda behöriga representanter och deras ansvarsområden, inklusive historik och
- uppgifter vid utfärdande av HCC Organisation och HCC Funktion, t ex kvittens, identitet på behörig representant och datum för utlämnandet av HCC.

4.4.3 KRA/LRA

KRA/LRA ansvarar för att följande inom KRA/LRA-området arkiveras:

- uppgifter om kortbeställningar och kortkvittenser,
- uppgifter om utlämnade SITHS-kort,
- uppgifter om återlämnade SITHS-kort,
- uppgifter om utlämnade och återlämnade reservkort samt åtgärder som vidtas efter att ett använt reservkort har återlämnats,
- uppgifter om utlämnade HCC och
- uppgifter om spärrade HCC.

4.5 Avbrottshantering och avveckling

4.5.1 Rutiner för avbrottshantering

I händelse av att man inte kan lita på HCC, ge ut HCC eller inte komma åt spärrlistor för HCC följs en kontinuitetsplan med rutiner för avbrottshantering. Kontinuitetsplan med rutiner för avbrottshantering för vår organisation finns i underbilaga 3.

4.5.2 Avveckling av RA-organisation

Vid avveckling av RA-organisation åligger det vår organisation att avveckla RA-organisationen enligt följande procedur:

- informera alla NI och alla parter som vår organisation har avtal eller överenskommelser med,
- avsluta åtagande och behörigheter för RA-organisationen och
- tillse att alla arkiv och loggar bevaras/överlämnas enligt med gällande anvisningar inom vår organisation.

Vid upphörande av ett ORA/KRA/LRA-område åligger det RA/ORA att avveckla berörd del av organisationen enligt följande procedur:

- informera alla NI och alla parter som RA/ORA har avtal och/eller överenskommelser med,
- avsluta åtagande och behörigheter för ORA/KRA/LRA-organisationen och
- tillse att alla arkiv och loggar bevaras/överlämnas enligt gällande anvisningar inom vår organisation.

5 Fysisk och personalorienterad säkerhet

5.1 Fysisk säkerhet

Vid utlämnande av nycklar och koder beaktas den fysiska säkerheten.

RA/ORA/KRA/LRA-arbetsplatsen skall finnas i låsbart utrymme med låsbara skåp för förvaring av arkivmaterial enligt avsnitt 4.4.

Då RA/ORA/KRA/LRA lämnar arbetsplatsen lämnas inte SITHS-kort obevakat.

PIN- och PUK-koder förvaras så att inte obehörig får tillgång till dessa. NI uppmanas att förvara koder och kort på fysiskt åtskilda ställen.

Arkivmaterial och reservkort med PIN- och PUK-koder samt SITHS kort som inte lämnats ut förvaras inlåst i skåp. Papperskvittens förvaras i brandsäkert skåp.

RA/ORA ansvarar för att RA-organisationen har säkra rutiner för beställning, distribution och förvaring av reservkort med tillhörande PIN- och PUK-koder.

5.2 Personalorienterad säkerhet

RA/ORA/KRA och LRA-personer utses enligt avsnitt 2.1 Förpliktelser och åtaganden. Dessa personer har inte annat uppdrag som kan bedömas stå i konflikt med uppdraget samt att de kan anses dugliga och ej innebära riskfaktorer i uppdraget.

Alla RA/ORA/KRA och LRA-personer har genomfått utbildning för att fullgöra sina arbetsuppgifter på ett säkert sätt.

Utbildning och uppföljning av utbildning av RA/ORA/KRA och LRA-personer genomförs regelbundet inom RA-organisationen.

6 Teknikorienterad säkerhet

6.1 Utlämnande av privat nyckel

6.1.1 Utlämnande av privat nyckel vid utlämnande av SITHS-kort

Nycklar och koder arkiveras ej i systemet. PIN- och PUK-kodsbrev sänds med post till NI:s folkbokföringsadress (eller via skatteverkets förmedlingskontor för NI med skyddad identitet).

6.1.2 Utlämnande av privat nyckel vid utlämnande av reservkort

Nycklar och koder utlämnas av RA/ORA/LRA till NI sedan denne identifierat sig, se kapitel 3. Mottagande av nycklar och koder kvitteras av NI. Kvittens ska sparas enligt gällande arkiveringsregler enligt avsnitt 4.4 Arkivering.

6.1.3 Utlämnande av privat nyckel i samband med utfärdande av HCC Organisation och HCC Funktion (PKCS#10 och PKCS#12)

Nycklar och koder utlämnas av RA/ORA till behörig representant, sedan denne identifierat sig, se kapitel 3. Mottagande av nycklar och koder kvitteras av den behöriga representanten. Kvittens ska sparas enligt gällande arkiveringsregler enligt avsnitt 4.4 Arkivering. Den behöriga representanten ska förvara nycklar och koder på fysiskt åtskilda platser.

6.2 Skydd av privat nyckel

För privata nycklar tillhörande HCC Funktion eller HCC Organisation gäller att de förvaras och distribueras på ett säkert och skyddat sätt så att de inte faller i orätta händer samt att de inte i något fall exponeras eller brukas på otillbörligt sätt, innan de nått rätt mottagare. NI skall skydda sin e-legitimation så att ingen obehörig får tillgång till den. Därför skall NI skydda sin dator och/eller sitt kort och annan utrustning där e-legitimation förvaras eller används. NI skall därför:

- välja säkerhetskoder som inte är lätta att lista ut,
- hålla säkerhetskoderna hemliga och
- inte anteckna säkerhetskoderna på ett sätt eller en plats som gör att de kan kopplas till NI:s e-legitimation.

6.3 Arkivering av privata nycklar

Inga privata nycklar tillhörande HCC Person arkiveras inom RA-organisationen.

Privata nycklar tillhörande HCC Organisation eller HCC Funktion får endast arkiveras för back-up ändamål. Om sådan lagras skall den hanteras enligt redovisad rutin i underbilaga 5.

6.3.1 Hantering av PIN- och PUK-koder

NI uppmanas att förvara den PIN- och PUK-kodshandling som erhölls från kortleverantören eller korthandläggaren (reservkort) som en värdehandling.

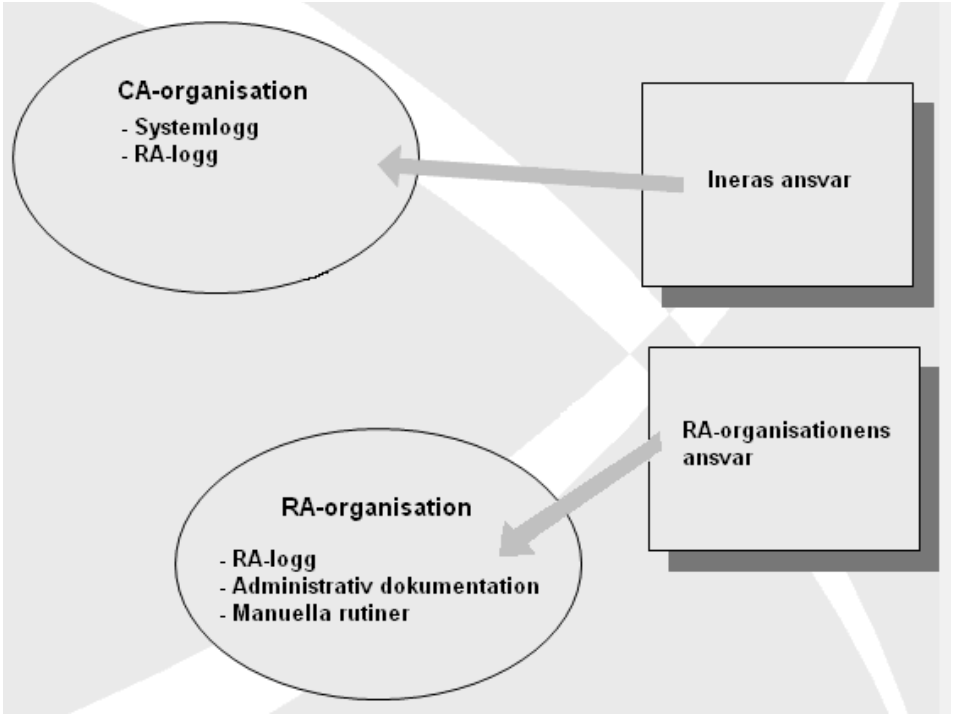
6.4 Processer för säkerhetsrevision

6.4.1 Loggning

Loggning av CA-aktiviteter sker hos SITHS CA:s leverantör av CA-tjänster. CA-leverantörens loggar är av två slag, systemloggar och loggar över RA-operationer. Systemloggar beskrivs närmare i driftleverantörens CPS. Loggar över RA händelser sker så att spårbarhet i processerna rörande utgivning och återkallande av HCC uppnås. Spårbarhet finns, t ex av vem som utfärdat/beställt ett certifikat, med vilka uppgifter och när.

Loggning sker också lokalt inom RA-organisationen. Loggar över egna RA händelser, administrativ dokumentation eller särskilda manuella rutiner, se Figur 3.

Alla RA/ORA/LRA har tillgång till sin egen del av loggen över RA-operationer. Denna sparas i systemet och bör regelbundet analyseras av RA-organisationen samt göras tillgänglig för revision.



Figur 3. Loggar för säkerhetsrevision

6.4.2 Analys av logg

Verksamhetsansvarig eller annan utsedd person som inte utfärdar HCC (oberoende part) skall regelbundet analysera logg som genererats inom RA-organisationen. Rutin för logganalys redovisas enligt underbilaga 2.

6.4.3 Bevarandetid för logg

Loggar bevaras i CA-system i minst 10 år.

7 Refererande dokument

CA Policy	**Certifikatspolicy för utgivande av certifikat inom vård och omsorg.** SE-SITHS-CA-Policy-4.pdf
CPS	**Certification Practice Statement.** Telia_SITHS_CPS_v2.0.pdf
RA policy	**RA-policy för utfärdande utgivande av certifiikat inom vård och omsorg.** SE-SITHS-RA-Policy-4.pdf
HCC	**Certifikat för svensk vård och omsorg. HCC.** HCC Version 2.35.pdf
HSA Policy	**Policy för elektronisk katalog inom svensk vård och omsorg.** HSA_Policy_Version_3.3_2008-12-03.pdf
HPT	**HSA Policy Tillämpning version 3.1** HPT-mall version 3.3.1 2009-06-15.doc
	<Org.namn>s HPT är inlämnad och godkänd

Definitioner

Arkivmaterial: Dokument som används för att nedteckna beställningar av HCC, signerade elektroniska beställningar, kvittenser vid mottagande av SITHS kort samt utförda verifieringskontroller av beställare.

Asymmetrisk kryptering: Kryptosystem som kännetecknas av att både sändare och mottagare av krypterad information använder olika nycklar för kryptering och dekryptering.

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

Behörig representant: Anställd hos uppdragsgivare eller med avtalade uppdrag åt denna, som har befogenhet att beställa, ta emot och spärra HCC Organisation och HCC Funktion hos administratör.

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.

Certification Authority: Se CA.

Certification Practice Statement: Se CPS.

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

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

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

CRL: Se spärrlista.

CSR: Underlag innehållande bland annat publik nyckel och uppgifter ifrån t ex en webbserver. CSR används vid skapandet av ett certifikat till en aktuell server. Förkortning av Certificate Signing Request.

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 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 (smart card) innehållande certifikat och nycklar samtidigt som kortets framsida kan utgöra en visuell ID-handling. Ett eID kort är en kryptografisk modul.

E-legitimation: Identitetshandling som vid elektronisk kommunikation används för legitimering eller underskrift.

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

Handläggare: Handläggare är den person som handhar beställningar av SITHS kort. Handläggare ansvarar också för att utlämnande av SITHS kort sker till den person som kortet är utställt till samt att underskrivna kortkvittenser hanteras till Registeransvarig för arkivering.

HCC: Tjänstecertifikat för de som arbetar inom svensk vård och omsorg. Förkortning av Health Care

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

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

Förkortningar

CA	Certification Authority
CRL	Certification Revocation List
CPS	Certification Practice Statement
CSR	Certificate Signing Request
DNV	Det Norske Veritas
HCC	Healthcare Certificate, certifikat för svensk vård och omsorg
HPT	HSA Policy Tillämpning
HSA	Namn för katalogtjänst för svensk vård och omsorg
IDC	Identity Certificate, identitetscertifikat
ISO	International Standardization for Organization
KRA	Kort RA, benämns även “Handläggare”
KUR	KRA med utökade rättigheter
LRA	Lokal RA
NI	Nyckelinnehavare
OID	Object Identifier
ORA	OmrådesRA
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RA	Registration Authority
RAPS	Registration Authority Practice Statement
SIS	Swedish Institute of Standards
SITHS	Säker IT i Hälso- och sjukvården
SoL	Socialtjänstlagen
xRA	samlingsnamn för ORA, KRA och LRA

Underbilaga 1. Rutiner vid missbruk av certifikat

Detta är "exempeltext" som skall anpassas helt eller delvis för att visa på hur er organisation avser att arbeta med eventuellt missbruk av certifikat inom SITHS.

Då missbruk av certifikat misstänks (t ex utlåning av kort eller åtkomst till PIN-koder) eller uppdagas skall xRA samt aktuell verksamhetsansvarig omedelbart informeras och vidta lämpliga åtgärder för att stoppa missbruket, till exempel genom att begära spärrning av aktuella certifikat och/eller behörigheter i CA-systemet.
Vid konstaterat missbruk av certifikat skall RA och Säkerhetsansvarig/Verksamhetschef meddelas. Dessa skall sedan tillsammans med aktuell xRA utreda missbrukets omfattning, informera berörd personal om aktuell händelse samt vilka åtgärder som vidtagits för att förhindra missbruket.
Erfarenheter av utredningar i samband med missbruk av certifikat skall återkopplas till verksamheten. Dessa baseras på de incidentrapporter (enligt organisationens interna rutiner för avvikelsehantering) som alltid skall upprättas över händelsen. Rapporterna arkiveras på ett betryggande sätt hos RA.
I allvarliga fall av missbruk av certifikat skall SITHS CA underrättas.

Underbilaga 2. Plan för genomförande av intern kontroll

Detta är "exempeltext" som skall anpassas helt eller delvis för att visa på hur er organisation avser att arbeta med kontinuerligt revisionsarbete.

Riskanalys av RA-organisationen och dess ansvarsområden skall genomföras vart tredje år eller då säkerhetspåverkande förändringar sker. Vid behov, dock minst med 12 månaders mellanrum, genomför Säkerhetsansvarig revision av rutiner och dokument samt rapporterar resultatet till RA. I övrigt kommer riskanalys avseende vår organisations RA-organisation att ligga till grund för vår organisations plan för genomförade av intern kontroll.

Loggar i CA-systemet kommer att analyseras minst 2 gånger per år för att upptäcka eventuella felaktigheter eller missbruk. Vår organisation arbetar med utgångspunkt från CA:s rekommendationer, se dokumentation "SITHS rutiner för Revisionsprocesser.doc".

För att kontrollera det manuella arbetet inom vår organisations RA-organisation kommer återkommande, interna stickprovsundersökningar att göras bland xRA-personal för att tillse att fastställda rutiner och regler följs. Denna interna kontroll av efterlevnad innefattar granskning av säkerhetsrutiner, arkivering och dokumentering. Vid upptäckt av brister i det manuella arbetet kommer åtgärder att vidtas för att korrigera dessa, till exempel genom utökad utbildning av xRA-personer, förändring av rutiner eller utbyte av xRA-personer.

Underbilaga 3. Kontinuitetsplan med rutiner för avbrottshantering

Detta är "exempeltext" som skall anpassas helt eller delvis för att visa på hur er organisation avser att arbeta med riskanalys och nödvändigt kontinuitetsarbete.

Vår organisation använder SITHS till att a) utföra kortbeställningar och dess administration, b) administrativa behörigheter till domäninloggning, c) inloggning till system som kräver "stark identifiering". Riskanalyser omfattar våra strategier och handlingsprogram vid händelser som om tillit till certifikatet inte kan uppnås eller dess tillgänglighet ej uppfylls (t ex spärrlista kan ej nås). Vår organisations riskanalysarbeten pekar på ett antal fokuseringsområden för att bibehålla vår tillit till certifikatets trovärdighet och tillgänglighet till dess beroenden.

I händelse av att beställning, spärrning samt andra funktioner för administration av kort och certifikat inte kan genomföras skall vår organisations Kundstöd omedelbart informeras. Vår organisations Kundstöd förmedlar informationen vidare till RA (eller utsedd kundstöd för SITHS-hanteringen). Denne ska undersöka felets omfattning och reproducerbarhet för att därefter anmäla felet till Kundstöd för SITHS CA. Baserat på information från SITHS CA och egna undersökningar bedömer RA avbrottets omfattning och eventuell tidpunkt för när det beräknas vara åtgärdat. RA (eller utsedd Kundstöd för SITHS) förmedlar sedan all information om driftstörningen till samtliga xRA via Intranätet/e-post.

Under avbrottet skall xRA manuellt registrera inkommande spärrbeställningar och vid särskilt kritiska fall tillse att behörigheter kopplade till dessa kort/certifikat tillfälligt dras in. När full administration av kort/certifikat åter är möjlig skall RA (eller utsedd Kundstöd för SITHS) informeras om detta samt orsak till avbrottet. Informationen vidareförmedlas av RA (eller utsedd Kundstöd för SITHS) till vår organisations Kundstöd och samtliga xRA.

Då avbrott som påverkar ovanstående inträffar i CA-systemet eller i HSA-katalogens toppnod är det CA som ansvarar för att informera RA via vår organisations RA-funktionsbrevlåda. I akuta fall även på telefon. Om avbrottet varar under mer än ett dygn skall alternativa inloggnings- och signeringsmetoder i drabbade applikationer användas i enlighet med de möjligheter som respektive berörd applikation medger. Meddelande om detta förfarande ska då skickas ut av RA (eller utsedd Kundstöd för SITHS) till berörda Systemägare och Systemförvaltare.

Under avbrott då man inte har åtkomst till den senaste spärrlistan och/eller onlinetjänsten för certifikatverifiering (OCSP-tjänsten) för att verifiera att ett certifikat är giltigt kan tidigare lokalt sparad version av spärrlista användas. Respektive systemägare får dock besluta om lämpligheten i detta, beroende på systemets klassning vad gäller sekretess, konfidentialitet och integritet. Detta ställningstagande dokumenteras och arkiveras inom respektive IT tjänst förvaltning.

Följande IT system är idag kopplade till spärrhanteringen:
...

...

I händelse av att man inte längre kan lita på kort/certifikat skall hela vår organisations RA-organisation informeras. Applikationer som använder kort/certifikat för inloggning och/eller signering skall ha en funktionalitet som möjliggör att andra förenklade inloggnings- och signeringsmöjligheter kan tillämpas tills kort/certifikat åter är tillgängligt.

Då avbrott som påverkar ovanstående inträffar i CA-systemet eller i HSA-katalogens toppnod är det CA som ansvarar för att informera vår organisations RA via vår organisations RA-funktionsbrevlåda. I akuta fall även på telefon.

Kontinuitetsplanens olika handlingsprogram med rutiner för eventuella avbrott, mm, testas årligen och erfarenheter av sådana tester skall återkopplas till verksamheten.
RA/Kundstöd för SITHS nås via:
Vardagar Beredskap 17-07, tfn xxx
Lördagar Beredskap 00-24, tfn yyy
Övrig tid Beredskap 00-24, tfn zzz

Underbilaga 4. Lista på organisationer som omfattas av denna RAPS

Organisation _____ Org.nr _____

Underbilaga 5. Rutin för arkivering av privata nycklar

Detta är "exempeltext" som skall anpassas helt eller delvis för att visa på hur er organisation avser att arbeta med arkivering av nycklar.

Ingen arkivering av privata nycklar skall ske.

SITHS CA hanterar inte arkivering av privata nycklar till personer, dvs kort. Dessa kan alltså inte arkiveras för att t ex i ett senare läge dekryptera information som tidigare lagrats krypterat. Vår organisation hanterar därför kryptering av dokument eller e-post med hänsyn till detta. Krypterad e-post används därför endast som skydd vid kommunikationen och inte för arkivering.

Privata nycklar till SITHS funktionscertifikat kan arkiveras för att säkerställa Back-up hantering. Vår organisation hanterar detta enligt...

Underbilaga 6. Bemanning av roller för denna RAPS

Roll	Namn	HSA-ID	E-post	Mobilnummer/Telefon
Säkerhetsansvarig				
Registeransvarig				
RA				
RA				

Underbilaga 7. Rutiner för kort- och certifikatutgivning

EXEMPELTEXT…

Särskild dokumentation finns upprättad, se "Rutiner för kort och certifikatutgiving".