MSB:s CPS för certifikatutfärdande under CA-Policy ver. 1

Detta dokument innehåller MSB:s CPS för utfärdande av certifikat.
Detta dokument har försetts med namn och objektidentifierare (OID). Dessa framgår av avsnitt 1.2.
MSB:s CA-policy version 1 har varit utgångspunkt vid framtagandet av denna CPS. Rubrikerna i CPS:en följer i möjligaste mån den struktur som finns i CA-policyn vilket innebär att även avsnitt som inte ingår i CA:s ansvar finns medtagna men med informationen att de inte är tillämpbara på CA:s åtaganden.
Detta dokument ägs och förvaltas av MSB.

1 Inledning

1.1 Översikt

Denna CPS beskriver de procedurer och rutiner som tillämpas vid utfärdande av certifikat för personer, funktioner och utrustning inom MSB samt för spärr och spärrkontroll av sådana certifikat.
CPS:en beskriver MSB:s tillämpning av de krav och regler som finns i MSB:s CA-policy version 1.

1.2 Identifiering

De rutiner och åtaganden som följer av denna CPS är endast tillämpliga i samband med sådana certifikat där CA-policyn åberopas.
Policynamnet för MSB:s CA-policy är {SE-Myndighet för samhällsskydd och beredskap-certifikatpolicy} och objektidentifieraren (OID) är {1.2.752.147.1.1}.
CPS-namn för denna CPS är {SE- Myndighet för samhällsskydd och beredskap -CPS-1} och objektidentifieraren är {1.2.752.147.1.1}.

1.3 Målgrupp och tillämplighet

1.3.1 Certifikatutgivare (CA)

MSB ansvarar för produktion av eget CA i enlighet denna CPS. MSB kommer att tillse att det finns tillräckliga resurser i form av egna medel och försäkringar för att kunna fullgöra sina åtaganden enligt denna CPS.

1.3.2 Cerifikatinnehavare

Slutanvändarcertifikat utfärdas till följande typer av nyckelinnehavare:

Typ av nyckelinnehavare	*Certifikatstyp*
Person	Person
System eller tjänst	Funktion

1.3.2.1 Personcertifikat

Personcertifikat 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 MSB eller som har personal som är involverad i säkert informationsutbyte med MSB.

Personcertifikat utfärdade under denna CPS 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.

1.3.2.2 Funktionscertifikat

Funktionscertifikat utfärdas endast till en namngiven funktion inom en organisation som kan vara t.ex. en tjänst eller tillämpning inom en organisation.

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

1.3.3 Tillämpning

Denna CPS 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 CPS är primärt avsedda för att understödja säker informationshantering inom MSB.

Certifikat utgivna enligt denna CPS 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

Myndigheten för samhällsskydd och beredskap
651 81 KARLSTAD
Telefonväxel: 0771-240 240
Faxnummer: 010-240 56 00
E-post: registrator@msb.se

1.4.1 Ansvarig på myndighet

Denna policy är registrerad på Myndigheten för samhällsskydd och beredskap. Utfärdare är ansvarig för denna CPS.

1.4.1.1 CPS

MSB:s Säkerhetschef ansvarar för granskning av att CPS utgiven av CA uppfyller alla krav ställda i denna policy.

2 Allmänna bestämmelser

2.1 Förpliktelser

2.1.1 Förpliktelser för MSB

MSB åtar sig att i enlighet med denna CPS:

a) i förekommande fall generera eller tillhandahålla tjänster för generering av nycklar för person- och funktionscertifikat.

b) publicera information till katalogtjänst, som tillhandahålls av MSB, 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 publicera spärrinformation i enlighet med kapitel 4

h) uppfylla alla allmänna bestämmelser i kapitel 2.

2.1.1.1 Skydd av CA:s privata nyckel

MSB förpliktigar sig att skydda privata CA-nycklar i enlighet med denna CPS.

2.1.1.2 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

Skydd av privat RA-nyckel sker enligt CPS.

2.1.2.3 Restriktioner gällande bruk av privata nycklar

Restriktioner gällande bruk av privata nycklar följer CPS.

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 omedelbart spärra certifikaten och i förekommande fall kortens primärcertifikat 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.

2.1.4 Förpliktelser för förlitande part

2.1.4.1 Användning av certifikat för avsedda ändamål

Förlitande part skall säkerställa att denne 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,

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

c) i sin riskbedömning ta med de ansvarsfriskrivningar som framgår av denna CPS.

Förlitande part skall särskilt beakta:

- vad som sägs i 1.3.4 om användningsområden,
- att:
  - Publika nycklar för Signering används till att verifiera Signaturer
  - Publika nycklar för identifiering till att verifiera identitet
  - Publika krypteringsnycklar till kryptering för insynsskydd samt att nyckeln för Signering inte får användas för andra säkerhetstjänster medan en och samma nyckel däremot får användas för verifiering av identitet och kryptering för insynsskydd,
- vad som sägs i 2.2 och 2.3 om ansvar.

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

MSB ansvarar beträffande de certifikat som utfärdats av MSB CA, genomför kontroller och verifikationer i enlighet med rutiner som framgår av denna CPS.

2.2.1.2 Friskrivningar

MSB ansvarar inte för skada på grund av att uppgifterna i ett certifikat eller i spärrinformation är felaktiga, såvida MSB inte gjort sig skyldig till grov vårdslöshet.

2.2.2 Ansvar för RA

I de fall där MSB agerar RA tar MSB fullt ansvar för RA-funktionen.

2.3 Finansiellt ansvar

2.3.1 Skadeersättning

CA tar inget finansiellt ansvar vid användandet av utfärdarcertifikat eller tillhörande privat nyckel

2.4 Tolkning och verkställighet

2.4.1 Tillämplig lag

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

2.4.2 Procedurer för konfliktlösning

Tvist med anledning av denna CPS ska avgöras enligt ICC:s regler för förlikning och skiljedomsförfarande. Förhandlingarna ska hållas på svenska.

2.5 Avgifter

2.5.1 Avgifter för utfärdande och certifikat

Inga avgifter för internt bruk

2.5.2 Avgifter för certifikatsåtkomst

Inga avgifter för internt bruk

2.5.3 Avgifter för åtkomst till spärrlistor

Inga avgifter för internt bruk

2.5.4 Avgifter för åtkomst till CPS

Inga avgifter för internt bruk

2.6 Publicering och förvaringsplats

2.6.1 Publicering av CA-information

Följande information ska vara tillgänglig:
a) Denna CPS
b) Spärrlistor med spärrade certifikat
c) Utfärdade CA-certifikat, självsignerade CA-certifikat och korscertifikat för korscertifierade CA.
Varje publicerad spärrlista (CRL) tillhandahåller vid publiceringstillfället all tillgänglig spärrinformation för samtliga spärrade certifikat som spärrlistan är avsedd att förmedla.

2.6.2 Leverans

Leveransen sker enligt rutin för de olika kategorierna av användare samt certifikatutgivare

2.6.3 Tillgänglighet

Enligt överenskommelse med beställaren samt underliggande CA

2.6.4 Källa

Denna CPS kan beställas hos MSB och är även tillgänglig på intranät/extern webbplats.

2.7 Granskning

2.7.1 Förekomst

MSB ska genomföra löpande internrevision av att MSB CA-policy version 1 och denna CPS efterlevs.

Vid revisionen ska speciellt följande undersökas:

a) CPS:ens lämplighet och överensstämmelse med gällande CA-policyn.

b) Jämförelse mellan CA:s interna rutiner, instruktioner, anvisningar och denna CPS

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 förändra tillämpade rutiner, instruktioner och anvisningar och/eller uppdatera denna CPS.

Om denna CPS uppdateras på sådant sätt att den nya CPS:en bedöms medföra en förändrad säkerhetsgrad så skall en ny CPS med en ny version upprättas.

2.8 Konfidentialitet

2.8.1 Typ av information som skall hållas konfidentiell

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

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 och spärrinformation

c) Villkor för nyckelinnehavare

d) Denna CPS

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

2.8.3 Utlämnande av uppgifter till rättsvårdande myndigheter

Utlämning av uppgifter skall följa Myndigheten för samhällsskydd och beredskaps standardregler och bestämmelser.

MSB kommer att lämna ut konfidentiell information om domstol eller någon annan rättslig instans som lyder under svensk lag så beslutar. Privata nycklar kopplade till utfärdade certifikat kan inte tillhandahållas då dessa inte finns sparade.

2.9 Immateriella rättigheter

Tillstånd gäller dock generellt för att reproducera och sprida denna CPS i sin helhet under förutsättning att det sker utan avgift och att ingen information i dokumentet läggs till, tas bort eller förändras.

3 Identifiering och autentisering

3.1 Inledande registrering

Certifikatinnehavaren/Nycklelinnehavaren registreras med kontaktuppgifter samt identitetsuppgifter.

3.1.1 Certifikatuppgifter

Följande uppgifter är obligatoriska för certifikatinnehavare och ska ingå i certifikatet:

Attribut	Innehåll
Land	Landskod, två tecken (SE)
	Underliggande CA:s namn
Organisation	Organisationsnamn MSB
Serienummer	Organisationsnummer

3.1.2 Krav på korrekta uppgifter

Uppgifterna skall verifieras att de är officiella namn för certifikatsinnehavaren.

3.1.3 Regler för namngivning

Uppgifter skall på ett tydligt sätt redovisa den underliggande objekts identitet.

3.1.4 Unika identifierare

Certifikatets namn skall vara unikt inom namndomänen ”Myndigheten för samhällsskydd och beredskap ”och CA. Den unika identifieraren kan vara av annat slag än svensk personnummer.

3.1.5 Konflikter vid namngivning

Inga bestämmelser.

3.1.6 Autentisering av organisationstillhörighet

Certifikatinnehavarens organisationstillhörighet auktoriseras av respektive organisations ansvarige för certifikatutfärdning.

3.1.7 Autentisering av personers identitet

3.1.7.1 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.

c) Nyckelinnehavaren är känd av minst två anställda vid RA

Identitetskontroll enligt a) utförs i normalfallet av RA och det är RA:s åtagande att utföra identifieringen i enlighet med MSB:s RA-Policy.

3.1.7.2 Procedur för autentisering

Innan certifikat skapas så kontrolleras samtliga nyckelinnehavarens identitetsuppgifter, som inte undantags nedan, mot personallistan eller lämplig katalogtjänst.

3.1.7.3 Krav på personlig närvaro

I normalfallet utförs identitetskontroll som kräver personlig närvaro.

3.1.8 Metod att bevisa innehav av privat nickel

Certifikatbegäran ska utföras enligt standardprotokoll som medger verifiering av innehav av privat nyckel.

3.1.9 Funktionscertifikat

Vid beställning av certifikat av typen funktionscertifikat, samt vid distribution av privata nycklar och koder kopplade till dessa, infordras en skriftlig beställning från en funktion/resursägaren. Denna beställning kan avse en eller flera nyckelinnehavare.

3.1.9.1 Autentisering av behörig representant

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

3.1.9.2 Krav på personlig närvaro

Identitetskontroll vid utlämning av privata nycklar och koder kräver personlig närvaro av behörig representant vid utlämningstillfället eller likvärdigt.

3.1.10 Identifiering av underliggande CA-administratörer

Administratörer ska identifieras vid inpassering till utrymme samt med stark autentisering vid åtkomst till systemet för certifikatutgivning.

3.2 Förnyat certifikat

Utgivning av nytt certifikat sker efter samma rutiner som nybeställning för underliggande CA.
Livslängd enligt MSB CP för rootcertifikat.

3.3 Förnyat certifikat efter spärrning

Utgivning av nytt certifikat efter spärrning sker efter samma rutiner som nybeställning för underliggande CA.

3.4 Begäran om spärrning av certifikat

En certifikatsinnehavare ska kunna begära spärrning av sitt personliga certifikat.
MSB:s säkerhetschef kan i samråd med IT-säkerhetsansvarig begära spärrning av CA certifikat.

CA kan på eget initiativ spärra underliggande CA vid behov.

4 Operationella krav

4.1 Ansökan om certifikat

Vid ansökan fullföljs följande procedurer:
a) Uppdragsgivaren (behörig representant eller RA) fyller i ansökan och undertecknar denna via digital signatur varvid alla villkor för nyttjande av tjänsten accepteras. I denna process uppger nyckelinnehavaren samtliga relevanta personliga uppgifter enligt 3.1.1.
b) Nyckelinnehavaren identifieras enligt 3.1.7.
c) Ansökningshandlingar arkiveras enligt 4.6.

4.2 Utfärdande av certifikat

Hantering av elektronisk registrering hos av aktuell organisation 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 RA personligen konstaterat att angivna beställningsrutiner och kontrollrutiner fullföljts.
Varje signerad beställning från behörig operatör hos RA kan spåras individuellt till den operatör som signerat beställningen.
Vid utfärdande av underliggande CA gäller även att säkerhetsenheten verifierar att CP och CPS är godkända och administratören behörig för uppgiften.

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 som t.ex. signerad epost.
2. Genom att den privata nyckeln genereras av CA samt säkert skyddas och distribueras till ansvarig nyckelinnehavare
3. Då nyckelinnehavaren redan innehar certifikat som korresponderar mot aktuell privat nyckel, kan innehav av korrekt privat nyckel styrkas genom uppvisande av detta certifikat. Förutsättningen är dock att detta certifikat påvisar en säkerhetsnivå som minst korresponderar mot denna CPS.

4.3 Utlämning av certifikat

CA ska meddela den underliggande CA att certifikatet är färdig och hur det kan levereras. 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

MSB tillhandahåller en tjänst för spärrning av certifikat. MSB skapar löpande signerade listor över spärrade certifikat (CRL:er), varav den senaste lagras internt tillgänglig. Aktuell spärrlista omfattar information om spärrning för de certifikat som är associerade med spärrlistan, i enlighet med innehållet i CRL enligt X.509, version 3. Denna innefattar information om alla spärrade certifikat vars giltighetstid inte löpt ut.
Spärrkontroll genom on-line kontroll av ett certifikats giltighet kan också göras mot en tjänst som MSB tillhandahåller. Aktualiteten i denna tjänst är densamma som spärrlistan.
Vid spärrning av certifikat informeras nyckelinnehavaren i enlighet med gällande villkor.

4.4.1 Orsaker till spärrning

MSB genomför spärr av 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 kort eller motsvarande lagringsmodul som innehåller korresponderande privat nyckel inte längre innehas/kontrolleras eller inte längre kan brukas av rätt nyckelinnehavare.
e) Vid 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 MSB beslutar upphöra med sin CA-verksamhet enligt 4.8.

4.4.2 Vem kan begära spärrning hos CA

Spärrningsbegäran kan begäras av RA, behörig representant för RA eller nyckelinnehavaren.
MSB 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 stycket ovan.

4.4.3 Procedurer för spärrningsbegäran

En till CA:n 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 CPS uppdateras och publiceras så snart spärrbegäran inkommit och beslut om spärrning fattats, dock minst en gång per dygn.
Funktionen att uppdatera och publicera spärrlistor kan vid service och systemfel vara otillgänglig under en begränsad tid.

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.

Spärrlistor publiceras kontinuerligt till katalogen. Sökvägen till spärrlistorna i denna framgår av informationen i extensionen CDP (CRL Distribution Points) som ingår i samtliga certifikat.
Sökvägen till denna tjänst framgår av informationen i extensionen AIA (Authority Information Access) som ingår i samtliga certifikat.

4.5 Procedurer för säkerhetsrevision av CA-systemet /Uppföljning

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 Händelser som ska registreras

Som minst följande händelser ska loggas i de av CA berörda system:
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 Kontroll av loggar

Loggarna ska analyseras för upptäckt av obehöriga aktiviteter

4.5.3 Bevarande av loggar

Loggarna bevaras enligt nedan:

- MSB personal CA:loggar sparas i minst 2 år
- CA: loggar sparas i 6 år

4.5.4 Skydd av loggar

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.

4.5.5 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 revisionsunderlag

System för insamling av loggar enligt detta avsnitt hanterar enbart intern logginformation skapad i det centrala systemet för certifikatproduktion och utgör underlag för revisionsens granskning.

4.6 Arkivering

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

4.6.1 Uppgifter som ska arkiveras

Följande information arkiveras löpande:

a) Alla program och filer tillhörande CA-systemet.
b) Transaktioner innehållande signerad begäran om certifikatproduktion och spärrning av certifikat från behörig operatör.
c) Ansökningshandlingar undertecknade av ansökande uppdragsgivare samt av personer ansvariga för att ta emot och acceptera ansökan.
d) Undertecknade mottagningskvittenser vid utlämning av nycklar och koder.
e) Utgivna certifikat samt därtill relaterade uppdateringar av katalog.
f) Historik rörande tidigare CA-nycklar, nyckelidentifierare samt korscertifikat mellan olika generationer av CA-nycklar.
g) Begäran om spärrning samt därtill relaterade uppgifter inkomna till spärrtjänsten.
h) Utgivna spärrlistor samt därtill relaterade uppdateringar av CA:s katalog.
i) Resultat av revision av CA:s uppfyllelse av denna CPS.
j) Gällande villkor och kontrakt (i alla tillämpade versioner).
k) Denna CPS samt alla tidigare tillämpade versioner av denna CPS.

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 Arkiveringstid

All arkiverad information bevaras i minst 1 år efter det aktuella certifikatet gått ut.

4.6.3 Procedurer för att nå och verifiera arkivmaterial

Arkiverat material som är klassat som konfidentiellt 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 2 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 MSB:s kostnader.

4.7 Byte av CA-nyckel

4.7.1 Förnyelse av CA-nyckel

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

Vid byte av CA-nyckel sker följande:

a) nytt självsignerat 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 publiceras i relevant katalog.

4.7.2 Planering för kompromettering och katastrof

Vid misstanke om att MSB inte längre äger fullständig och exklusiv kontroll över den privata CA-nyckeln, vidtas 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 MSB har en relation med, att CA-nyckeln är komprometterad och hur nytt CA-certifikat kan hämtas.

c) I det fall MSB har korscertifierat den komprometterade CA-nyckeln med en annan operativ CA-nyckel, spärra sådana korscertifikat och se till att spärrinformation finns tillgänglig för certifikatet fram till dess att de spärrade certifikatens giltighetstid löpt ut.

4.7.3 Nyckelinnehavare

Nyckelinnehavare informeras om att omedelbart upphöra med användning av privata nycklar som är associerade med certifikatutfärdade med den komprometterade CA-nyckeln.

Nyckelinnehavarna informeras om processen 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.

4.7.4 Förlitande part

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

Förlitande part agerar utanför MSB:s inflytande. Dessa erhåller genom MSB:s hantering av spärrinformation den information som krävs för att de skall kunna agera på ett korrekt sätt.

4.8 Upphörande av CA

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

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

b) Öppet informera om att verksamheten upphör minst en månad 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:ns namn.

e) Se till att alla arkiv och loggar bevaras under angiven bevaringstid.

5 Säkerhetsskydd

5.1 Fysisk säkerhet

5.1.1 Krav på lokaler

Anläggningen som rymmer centrala CA-funktioner är fysiskt placerad i en starkt skyddad datorhall. CA-systemet skall vara skyddat från obehörig access. CA:s privata nycklar skall förvaras på ett sådant sätt att de ej kan exponeras eller manipuleras.

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. Frånsett datorhall enligt 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.

5.1.3 Fysisk säkerhet för RA

Några RA-funktioner som innefattar roller enligt ansvar och roller stycket nedan kan förekomma utanför den skyddade centrala fysiska miljön. 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.

Punkter 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.

5.1.4 Miljökrav

Lokaler avsedda för CA -systemet skall vara utrustade med elförsörjning och luftkonditionering så att en säker driftmiljö kan erhållas samt att gällande brandskyddskrav kan uppfyllas. Datorer avsedda för generering av privata nycklar och certifikat skall vara försedda med avbrottsfri kraft.

5.1.5 Kylning av systemet

Enligt driftleverantörens standard rutiner

5.1.6 Rutin för brandskydd

Enligt driftleverantörens standard rutiner

5.1.7 Rutin för lagring av media

Enligt driftleverantörens standard rutiner

5.1.8 Avveckling av hårdvara

Hårdvara som kan innehålla känslig information skall förstöras enligt gällande för informationsklassen rutiner

5.1.9 Backup på annan plats

Backup av CA förvaras i lokal/er med samma nivå av säkerhet som huvuddriftstället.

5.2 Procedurorienterad säkerhet

MSB 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 Roller och ansvar inom CA

Roller definierade för drift och underhåll av MSB:s CA är minst:

Roll	***Förklaring***	***Uppgifter***
Certification Authority Administrator (CAA)	Administrativ produktions-/driftspersonal för CA:n	• Skapa CA-certifikat • Personalisera kort • Generera nycklar • Generera spärrlista •Kontroll av certifikatutfärdarloggen
Systemadministratör (SA)	Teknisk produktions-/driftspersonal för CA:n	• Installationer • Systemunderhåll • Byte av media med säkerhetskopior
Säkerhetschef	Övergripande	

	säkerhetsansvarig för CA-plattformen	
IT-säkerhetsansvarig	Kan ha ett visst delegerat säkerhetsansvar 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.	
Systemövervakning/IT-beredskap	Personal ej direkt involverade i den centrala CA-driften som övervakar och agerar på larm genom att kontakta ovanstående roller.	

5.2.1.2 Betrodda roller inom RA

Enligt RA:s arbetsuppgifter.

5.2.2 Bemanning

Rollerna tillsätts av minst en person vardera. Person som innehar roll som IT-säkerhetsansvarig eller Systemadministratör innehar inte samtidigt någon annan av de andra rollerna.

Initiering av CA-systemet samt generering och initiering av CA-nycklar kräver närvaro av minst två personer som innehar någon av säkerhetsrollera ovan.

5.2.3 Identifiering och autentisering av varje roll

Identifiering av rollen systemadministratör sker i operativsystemet i CA-systemets enheter.

Identifiering av rollen CAA sker i CA-systemets applikationer och baseras på stark autentisering med hjälp av personliga operatörskort.

5.3 Personalorienterad säkerhet

5.3.1 Bakgrund, kvalifikationer, erfarenhet och tillståndskrav

Rollerna 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 Säkerhetsklassning

Administratörer samt operatörer av CA ska vara säkerhetsklassade enligt MSB:s regelverk.

5.3.3 Utbildningskrav

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 CPS och inom ramen för gällande säkerhetspolicy.

5.3.4 Krav på återkommande utbildning

Alla innehavare av rollerna som arbetar med CA-systemet ska fortlöpande utbildas i systemet.

5.3.5 Påföljd för obehörig handling

Enligt standard rutiner.

5.3.6 Krav på kontraktering av personal.

Enligt standard rutiner.

5.3.7 Dokumentation till personal

Säkerhetsinstruktion ska utgå från säkerhetschef samt information om säkerhets på arbetsplats

5.3.8 Personalorienterad säkerhet för RA

Ansvarig personal för RA-funktion utses inom den organisation som är utsedd att utföra tilldelade arbetsuppgifter.

Om sådan roll utförs av underleverantör 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.

Nyckelgenereringsprocessen innebär 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

Vid generering av utfärdarnycklar krävs flera personers närvaro.

6.1.1.2 Leverans av centralt genererade privata nycklar till nyckelinnehavare

Efter produktion levereras nycklar med säker transport till godkänd handläggare för utlämning till slutanvändare(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 denna CPS. Mottagande av nycklar och koder kvitteras. Kvittensen arkiveras i minst 5 år av RA.

6.1.1.3 Leverans av publik nyckel till CA.

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 CPS, som intygar nyckelinnehavarens association med nyckeln.

6.1.1.4 Leverans av CA:s publika nycklar till nyckelinnehavare och förlitandeparter

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

6.1.2 Nyckelstorlekar

Rootcertifikat 4096 bitar

Underordnad CA 2048 bitar

Utgivna certifikat minst 1024 bitar men rekommenderat 2048 bitar

6.1.3 Generering av publika nyckelparametrar

Nyckelinnehavares nycklar som i certifikaten markeras med användningsområdena kryptering och autentisering 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.
MSB kommer att ansvara för att kontinuerlig bevaka teknikutvecklingen inom kryptoteknikområdet och anpassning av kryptoalgoritmer i enlighet de senaste rönen på ett kostnadseffektivt sätt.

6.1.4 Kontroll av nyckelparametrar

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

Certifikat utgivna i enlighet med denna CPS kan omfatta följande användningsområden.

a) Identifiering och Autentisering (Key Usage digitalSignature (0))

b) Kryptering (Key Usage keyEncipherment (2) och/eller keyAgreement (4) och/eller dataEncipherment (3))

c) Verifiering av digitala signaturer i samband med oavvislighetstjänster (Key Usage nonRepudiation (1))

6.1.5 Generering av nycklar i hårdvara/mjukvara

CA:s utfärdarnycklar genereras och förvaras i för detta ändamål avsedd kryptografisk system/modul. Motsvarande gäller för de fall nycklar genereras lokalt i kortet.

6.2 Skydd av privat nyckel

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.

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 CPS.

2. Mjukvaruskyddade privata nycklar som genererats av CA enligt denna CPS.

Mjukvaruskyddade nycklar skall lagras i krypterad form med sådan 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.

6.2.1 Lagringsmedia för privat nyckel

CA:s privata nyckel som används för signering av certifikat och spärrlistor skall lagras på ett sätt som omöjliggör läsning/export.

6.2.2 Åtkomst till privat nyckel

För fullständig tillgång till CA-anläggningen med CA:s privata nyckel krävs minst två behöriga personer. Säkerhetschef samt behörig administratör.

6.2.3 Nyckeldeponering

Ingen nyckeldeponering utförs.

6.2.4 Säkerhetskopiering av privata nycklar

Det skall finnas minst två kopior av CA:s privata nyckel för händelse av hårdvarufel. Dessa skall lagras i enlighet med anvisning från säkerhetschef. Klassas som Hemlig information i enlighet med anvisning från säkerhetschef.

Säkerhetskopia av den underliggande CA:s privata nyckel får under inga omständigheter göras av CA, detta är den underliggande CA:s eget ansvar.

6.2.5 Arkivering av privata nycklar

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

6.2.6 Aktivering av privat nyckel

Aktivering av CA:s privata nyckel ska kräva att två personer deltar i processen eller aktivering genom validering av inmatade data.

6.2.7 Avaktivering av privat nyckel

Enligt säkerhetschefensbeslut för CA. Användning av kryptografiska moduler som har aktiverats ska inte lämnas obevakade utan avaktiveras via t.ex. utloggningsprocess.

6.2.8 Förstöring 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 Övriga 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.

6.3.1 Arkivering av publik nyckel

Publika nycklar arkiveras av CA som en del av certifikatarkiveringen.

6.3.2 Giltighetstid för publika och privata nycklar

Certifikat för nyproducerade nycklar ges maximalt en giltighetstid på 5 år.

Certifikat för existerande nycklar ges maximalt en giltighetstid fram till dess att ursprungscertifikatets giltighetstid löper ut, dock max 5 år. Certifikat som används av personal vid drift av CA-systemet ges maximalt en giltighetstid på 18 månader.

Privata CA-nycklar används maximalt 5 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 och spärrlistor.

Korscertifikat mellan olika generationer av CA nycklar ges maximalt en giltighetstid på 5 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 PIN-koder

6.4.1 Generering av PIN-koder

Användande av privat nyckel för CA skall skyddas av en PIN-kod bestående av minst 5 siffror.
PUK-kodshantering styrs av hanteringen för de olika tokens som används, förvaringen kontrolleras av säkerhetschef eller motsvarande.
Genereringsprocessen ska vara utformad så att ingen information om aktiveringsdata hanteras utanför systemet för generering annat än genom säker överföring till avsedd plats.

6.4.2 Hantering av PIN-koder

PIN-koden ska hanteras som konfidentiell och strikt personlig uppgift och får ej delges någon annan.

6.4.3 Andra aspekter på aktiveringsdata

Aktiveringsdata ska distribueras till användaren på ett sådant sätt att ingen annan får kontroll över aktiveringsdata utan att detta upptäcks.
Aktiveringsdata skickas normalt ut via PIN-brev eller genom system speciellt anskaffat för ändamålet.

6.5 Säkerhet i datorsystem

Installation av operativsystem och system för certfikatutgivning sker i direkt anslutning till formatering av diskar och med leverantörens original programvara. Vid installation, nyckelceremoni samt registrering av initiala behörigheter i systemet ska minst två personer delta. Hela CA-systemet skall vara uppbyggt på ett sådant sätt att individuella roller kan separeras.
Separering av roller på OS-nivå skall säkras.

De accesskontrollsystem som används skall vara så konstruerade att varje operatör identifieras på individuell nivå. 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.

6.6 Säkerhet vid utveckling och underhåll

6.6.1 Kontroller under systemutveckling

CA-systemets mjukvara utvecklas av tillverkare som använder en kontrollerad utvecklingsmiljö med ett väl dokumenterat kvalitetssäkringssystem. Alla ingående komponenter skall vara verifierade och säkerhetsgranskade före driftsättning. Säkerhetskopia på all ingående programvara skall finnas tillgänglig.
Dokumentation skall finnas till alla program som ingår i CA-systemet.
Ingen systemutveckling ska ske i drift/produktionsmiljö.
Det skall finnas dedikerad reservutrustning för alla ingående komponenter för att säkerställa att certifikatutgivningstjänsten kan upprätthållas.
Undantag standardkomponenter som snabbt kan ersättas.

6.6.2 Kontroll av säkerhetsadministration

De roller som definierats ska införas i driftorganisationer och befintligt säkerhetsregelverk ska följas.
Riskanalys ska alltid föregå förändringar av systemet för certifikatutgivning.

6.7 Nätverkssäkerhet

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

Viktig informationsutväxling mellan RA och CA är krypterad och transaktioner som påverkar användningen av CA:s privata utfärdarnycklar är individuellt signerade. Alla kommunikationsportar i CA-systemet som inte behövs är avaktiverade och tillhörande mjukvarurutiner som inte används är blockerade. Datamedia som innehåller uppgifter som läses in i CA-systemet skall dess ursprung säkerhetsställas och kontrolleras innan inläsning.

6.8 Komponenter med kryptologisk funktionalitet

Komponenter med kryptologisk funktionalitet som avser specifik hårdvara för lagring av kryptologiska nycklar, t ex CA:s privata nyckel får användas endast efter godkännande av Myndigheten för samhällsskydd och beredskap:s säkerhetschef.

7 Specifikationsadministration

7.1 Procedurer för specifikationsförändringar

7.1.1 Ändringar som kan ske utan underrättelse

De enda förändringar som kan företas i denna CPS utan underrättelse är språkliga justeringar och omdispositioner som inte påverkar säkerhetsnivån i beskrivna procedurer och regelverk.

7.1.2 Ändringar som skall ske med underrättelse

Små förändringar som är av mindre vikt och som endast berör en mindre del av alla nyckelinnehavare eller förlitande parter kan göras 30 dagar efter underrättelse.

Underrättelse om förändringar i denna CPS publiceras på mellan parterna överenskommen plats. För att kunna beaktas bör kommentarer inkomma senast 15 dagar efter publicering av underrättelse.

Myndigheten för samhällsskydd och beredskap avgör vilka åtgärder som vidtas med anledning av inkomna kommentarer. Om inkomna kommentarer innebär förändringar i det ursprungliga förändringsförslaget, som inte täcks av den ursprungliga underrättelsen, kan dessa förändringar träda i kraft tidigast 30/xxx dagar efter publiceringen av en ny modifierad underrättelse. Alla förändringar i denna CPS skall vara konsistenta med den eller de certifikatpolicy(-ies) som identifieras.