Certificate Authority Policy

1 Inledning

1.1 Översikt

Denna policy anger en uppsättning regler för ett certifikats tillämpbarhet gällande en specifik sammanslutning och/eller ett tillämpningsområde med likartade säkerhetskrav. Syftet med en certifikatpolicy är att skapa tillit till de certifikat som är utgivna enligt säkerhetskraven i policyn.

De krav på hantering och lagring av privata nycklar som beskrivs i denna policy avser privata nycklar som ges ut av MSB Root CA samt underliggande certifikatsinstanser om inte annat anges.

1.2 Identifiering

Denna certifikatpolicy är registrerad och tilldelad en unik objektidentifierare som finns angiven i en utvidgning av certifikat enligt X.509 v3

Objektidentifierare (OID)	{iso(1) member-body(2) se(752) Myndigheten för samhällsskydd och beredskap(147) certifikatpolicy(1) version (1)}

1.3 Målgrupp och tillämpning

Detta avsnitt beskriver till vilka denna policy är riktad samt aktuella användningsområden för utgivna certifikat.

1.3.1 Certifikatutgivare

Denna certifikatutgivare (CA) för Myndigheten för samhällsskydd och beredskap, ställer ut certifikat till underliggande CA under följande förutsättningar:

- CA förbinder sig att följa denna policy.
- CA förbinder sig att publicera en utfärdardeklaration (Certification Practice Statement - CPS) som beskriver hur åtagandena i denna policy uppfylls.

1.3.2 Certifikatinnehavare

Underordnad certifikatsinstans som erhållit certifikat enligt denna policy är intern MSB personal samt om möjligt externa användare. De olika kategorier av användare delas på olika underliggande certifikatutgivare.

1.3.3 Tillämpning

Denna policy är relevant för utgivande CA och för underliggande certifikatinnehavare samt övriga förlitande parter.

Certifikat som är utgivna enligt denna policy är avsedda för:
- Certifikatsutgivning för underliggande CA:s
- Signering av spärrlistor (CRL)

1.4 Kontaktuppgifter

Här anges ansvarig parts kontaktuppgifter

1.4.1 Ansvarig myndighet

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

1.4.1.1 Adress

Myndigheten för Samhällsskydd och Beredskap

Säkerhetschef

651 81 Karlstad

Telefon: 0771-240 240

E-post: registrator@msbmyndigheten.se

1.4.1.2 CPS

MSBs 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 CA:s förpliktelser

En CA som ger ut certifikat enligt denna policy skall förpliktiga sig att:

- Utföra regelbundna kontroller för att säkerställa att CP och CPS följs.
- Stödja berörda parter i överensstämmelse med berörda lagar och förordningar.
- Tillhandahålla lista (underlag för katalogtjänst) över utgivna certifikat.
- Spärra certifikat och publicera spärrinformation.
- Skydda sin privata nyckel enligt CP och CPS.
- Använda privat nyckel endast för ändamål beskrivna enligt denna CP.

2.1.2 Underliggande CA:s förpliktelser

En underliggande CA som tilldelats certifikat i enlighet med denna policy ska:

- Hantera sitt certifikat och tillhörande privata nyckel enligt CP och CPS för CA.
- Underliggande CA ska ha en av MSB godkänd CP och CPS.

2.1.3 Förlitande parts förpliktelser

En förlitande part som hanterar certifikat utfärdade i enlighet med denna policy skall:

- Tillse att certifikat och privata nycklar används i enlighet med denna policy.
- Verifiera certifikatens giltighet.

2.2 Ansvar

2.2.1 CA:s ansvar

CA ansvarar för att ett certifikat utfärdas i enlighet med beställningsuppgifter från underliggande CA samt enligt fastställd utgivningsprocess för CA..
CA ansvarar för att ge ut certifikat som kan uppfylla svensk lag för digitala signaturer.

2.2.1.1 Garantier och ansvarsbegränsningar

CA ansvarar, genom att signera ett certifikat som innehåller objektidentifierare för denna policy, för att de uppgifter som finns i ett utgivet certifikat är i överensstämmelse med de rutiner som anges i denna CP.

Om certifikat inte hanteras enligt regler uppsatta i denna CP och CPS kan CA inte ansvara för certifikatens äkthet.

2.2.2 Underliggande CA:s ansvar

Underliggande CA ansvarar för att beställningsuppgifter till CA är korrekta. Hantera alla ingående delar i den underliggande CA:n enligt instruktionerna i CPS och CP.

2.3 Finansiellt ansvar

2.3.1 Skadeersättning

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

2.4 Tolkning och upprätthållande

2.4.1 Styrande lagar

Gällande Svenska lagar och bestämmelser.

2.4.2 Tvistelösning

Inga bestämmelser

2.5 Avgifter

Inga avgifter utgår för tjänster avseende CA

2.6 Publicering och förvaringsplats

2.6.1 Publicering av CA:s information

CP och CPS ska levereras till Myndigheten för samhällsskydd och beredskaps godkända parter som berörs av certifikatutgivning från CA.

2.6.2 Leverans

Leverans sker enligt utgivningsrutin för de olika kategorierna av användare samt underliggande certifikatutgivare.

2.6.3 Tillgänglighet

Enligt överenskommelse med beställare samt med underliggande CA.

2.6.4 Källa

Denna policy kan beställas hos Myndigheten för samhällsskydd och beredskap

Certifikatuppgifter erhålls från en katalogtjänst som kopplas till respektive certifikatutgivare.

2.7 Granskning

2.7.1 Förekomst

CA skall regelbundet genomgå granskning med avseende på följande:

- Utfärdardeklarationen CPS lämplighet och överensstämmelse med CP.
- Den praktiska implementationen av CPS

2.7.2 Granskare

Planerad granskning av CA utförs av Myndigheten för samhällsskydd och beredskaps säkerhetsenhet eller av ansvarig myndighet utsedd part.

2.7.3 Granskarens relation till granskad part

För att kunna utföra en opartisk granskning skall granskare och CA vara organisatoriskt separerade

2.7.4 Granskarens uppgift

Granskaren skall kontrollera att CA uppfyller alla delar av CPS.

2.7.5 Åtgärder vid brister

Eventuell avvikelse från CPS skall noteras och åtgärdas utan dröjsmål.

2.7.6 Rapportering

Resultat av granskning ska rapporteras i enlighet med Myndigheten för samhällsskydd och beredskaps bestämmelser och övriga rutiner.

2.8 Konfidentialitet och sekretess

2.8.1 Konfidentiella uppgifter

CA:s privata nyckel är av hög konfidentialitet och skall hanteras i enlighet med krav för information klassad som sådan. CA skall beakta tillämplig integritetslagstiftning

2.8.2 Ej konfidentiella uppgifter

Följande uppgifter anses inte konfidentiella:

- Information om spärrade certifikat
- Publika nycklar
- Denna CP med tillhörande CPS. (CPS dock intern).

2.8.3 Information avseende spärrning av certifikat

Enligt Myndigheten för samhällsskydd och beredskaps standardregler för detta ändamål

2.8.4 Utlämnande av uppgifter till rättsvårdande myndigheter

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

2.9 Immateriella rättigheter

Denna policy får spridas till berörda parter enligt Myndigheten för samhällsskydd och beredskaps standardregler och bestämmelser

3 Identifiering och autentisering

3.1 Inledande registrering

3.1.1 Certifikatsuppgifter

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

Attribut	Innehåll
Land	Landskod, två tecken (SE)
	Underliggande CA:s namn
Organisation	Organisations namn MSB eller motsvarande
Serienummer	Organisationsnummer (OID)

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 CA:s identitet.

3.1.4 Unika identifierare

Certifikatets namn skall vara unikt inom namndomänen ”Myndigheten för samhällsskydd och beredskap och CA”.

3.1.5 Konflikter vid namngivning

Inga bestämmelser

3.1.6 Metod att bevisa innehav av privat nyckel

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

3.1.7 Rollcertifikat

Förekommer ej

3.1.8 Identifiering av underliggande CA-administratörer

Administratörer ska identifieras med giltig legitimation 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 ny beställning för underliggande CA.
Livslängd för certifikat:
Rootcertifikat 20 år
Underliggande CA 10 år
Person/utrustningscertifikat Max 18 månader

3.3 Förnyat certifikat efter spärrning

Utgivning av nytt certifikat efter spärrning sker efter samma rutiner som ny beställning 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 driftansvarig för CA begära spärrning av CA certifikat.

CA kan på eget initiativ spärra underliggande CA om denna har information som föranleder behovet att spärra underliggande CA:s.

4 Operationella krav

4.1 Beställning av underliggande CA

Beställningen av underliggande CA ska ställas till Myndigheten för samhällsskydd och beredskap.

Beställningsunderlag ska innehålla:

- Motivering för skapandet av en ny underliggande CA
- Nödvändig namninformation
- Tillgänglighet
- Användningsområde

Säkerhetsfunktionen ska kontrollera informationen i beställningen.

4.2 Utfärdande av underliggande CA

CA ska:

- Verifiera att CP och CPS är godkända.
- Verifiera administratörens behörighet före certifikatutfärdandet.
- Generera certifikat.
- Registrera utgivet certifikat och tillhörande uppgifter i en lista över utgivna certifikat.

4.3 Utlämning av certifikat

CA skall meddela den underliggande CA att certifikatet är färdigt och hur det kan levereras.

4.4 Spärrning och tillfällig indragning av certifikat

CA skall upprätthålla funktion för spärrning av certifikat.
Uppgifter om alla spärrade certifikat skall tillhandahållas minst fram till dess att deras giltighetstid går ut.

4.4.1 Orsaker till spärrning av certifikat

Certifikat skall spärras då:

- Privat nyckel är röjd.
- Certifikatet gavs ut på felaktiga grunder.
- Uppgifterna i certifikatet behöver ändras.
- Certifikat och/eller privat nyckel används på ett sätt som inte är tillåtet.
- CA-service upphör.
- Underliggande CA-tjänst upphör.
- Underliggande CA begär spärrning.
- Behovet finns inte för certifikat

4.4.2 Vem som kan begära spärrning av certifikat

Systemägare eller säkerhetsansvarig hos driftleverantör kan för en underliggande CA begära spärrning av certifikat utgivna till denna.

Systemägare eller säkerhetsansvarig hos driftleverantör kan begära spärrning för certifikat utgivna av CA, eller CA:s certifikat.

4.4.3 Procedur för begäran om spärrning av certifikat

Inga bestämmelser. (MSB CP)

4.4.4 Behandlingstid för spärrning av certifikat

Information om spärrning av certifikat skall vara tillgänglig enligt överenskommelse med underliggande CA.

4.4.5 Spärrkontrollens uppdateringsfrekvens

Efter att en underliggande CA har spärrats skall alla spärrfunktioner uppdateras inom en timme under arbetstid.

4.4.6 Krav på spärrkontroll

Förlitande part har ansvar att kontrollera att certifikatet är giltigt. Denna kontroll utförs på följande sätt:

- CRL

1. Giltighetskontrollen sker genom att förlitande part hämtar CRL från anvisad plats.
2. Förlitande part ska verifiera äkthet samt giltighetstid på hämtad CRL

Om certifikatet är spärrat eller om giltighetskontroll inte kan utföras saknas fog att lita på certifikatet.

4.5 Uppföljning

Regler för loggning och uppföljning i detta avsnitt gäller för alla komponenter som hanterar utgivning av certifikat och spärrlistor. Säkerhetsrelevanta händelser i samband med certifikatutgivning sparas hos driftleverantörens Säkerhetschef.

4.5.1 Händelser som ska registreras

Vid användning av programvara knuten till CA-funktion skall relevant in- och utdata samt resultat av begärd operation loggas. Minimalt skall typ av händelse, tidpunkt och i förekommande fall vem som utfört händelsen registreras.
För händelser som inte kan loggas av system skall manuell loggbok föras.

Finns loggmöjlighet i operativsystemet skall denna möjlighet nyttjas.

4.5.2 Kontroll av loggar

Loggar skall granskas så att felaktigheter uppmärksammas

4.5.3 Bevarande av loggar

Loggar som avser CA-funktion skall sparas enligt följande:

- MSB personal CA: loggar sparas i minst 2 år.
- CA: loggar sparas i 5 år

4.5.4 Skydd av loggar

Loggar skall skapas och förvaras på ett sådant sätt att innehållet ej kan förändras

4.5.5 Säkerhetskopia av loggar

Säkerhetskopiering av loggdata skall ske för att möjliggöra återställning vid behov.

4.5.6 System för insamling av revisionsunderlag

Den loggning som utförs på CA utgör underlag för revisionens granskning. Ytterligare insamling för revisionsändamål utförs ej

4.5.7 Bedömning av risker och sårbarheter

Risk och sårbarhetsanalys utförs enligt följande:

- före driftsättning av CA

- före större förändringar av systemet.

4.6 Arkivering

4.6.1 Uppgifter som ska arkiveras

CA:s arkiv skall vara tillräckligt detaljerat för att kunna fastställa giltigheten av en signatur i 2 år efter att använt certifikats giltighetstid gått ut. För att möjliggöra detta skall minst nedanstående uppgifter ingå.

Följande uppgifter skall arkiveras vid driftsättning av CA-systemet:
- Alla program och filer tillhörande CA-systemet
- CA-systemets konfiguration
- Formatspecifikationer
- CPS
- Resultat av säkerhetsgranskning
- Nyckelcermoniprotokoll

Följande uppgifter skall arkiveras vid användning av CA-systemet:
- Eventuella modifieringar av ovanstående uppgifter
- Serienummer för CA-certifikat som används vid signering av certifikat
- Alla certifikat som givits ut samt tillhörande beställnings- och distributionsuppgifter knyta till specifik användare

4.6.2 Arkiveringstid

Arkiveringsuppgifter skall sparas i minst 1 år efter att aktuella certifikat gått ut. Media innehållande arkiveringsuppgifter skall vara av sådan art att uppgifter går att utläsa under denna tid.

4.6.3 Skydd av arkiveringsuppgifter

Arkiveringsuppgifter skall skapas och förvaras på ett sådant sätt att innehållet ej kan förändras eller skadas. Dock kan uppgifter flyttas till ett annat lagringsmedium. Vissa delar av arkiveringsuppgifterna är känsliga vilket innebär att hela arkivet är känsligt och skall således hanteras och förvaras enligt de regler för informationsklassificering som gäller inom Myndigheten för samhällsskydd och beredskap.

4.6.4 Rutiner för backup

Följer standardprocedur för säkerhetskopiering hos driftleverantören.

4.6.5 Rutiner för åtkomst och verifiering av arkivinformation

Arkiverat material ska bevaras så att det är läsbart under angiven arkiveringstid (4.6.2)

Arkiverat material ska inte vara tillgängligt för externa parter annat än i den utsträckning som anges i 2.8.

4.7 Nyckelbyte

Ny CA-nyckel skall genereras och ett nytt självsignerat certifikat skall utfärdas senast tre månader innan den gamla nyckelns giltighetstid går ut.

4.7.1 Röjning av CA-nyckel

Instruktion över de åtgärder som skall vidtagas av administratörer av underliggande CA vid röjning av CA:s nyckel skall finnas i CPS.

Om användarens privata nyckel har röjts skall användare samt säkerhetschef omedelbart notifieras och certifikatet spärras

För system där certifikaten används ansvarar systemägaren för att inga certifikat utgivna av röjd CA används.

4.7.2 Bevarande av funktionen för certifikatutgivning för utgivande administratörer

Enligt systemens kontinuitetsplan.

4.8 CA:s upphörande

Med CA:s upphörande avses att all verksamhet och alla åtaganden förknippade med CA upphör.

CA skall informera certifikatinnehavare om CA:s upphörande minst tre månader innan upphörandet.

CA förbinder sig att förstöra CA:s privata nycklar i samband med upphörandet.

Efter CA:s upphörande frånsäger sig CA allt ansvar för användning av utgivna certifikat och privata nycklar.

5 Säkerhetsskydd

5.1 Fysiskt säkerhetsskydd

5.1.1 Krav på lokaler

CA-systemet skall vara skyddat från obehörig access i larmad och övervakad miljö. CA:s privata nycklar skall förvaras på ett sådant sätt att de ej kan exponeras eller manipuleras.

5.1.2 Fysiskt tillträde

Det ska utföras tillträdeskontroll på vem som får tillträde till det utrymme där utgivande CA förvaras. Endast begränsad skara av behörig personal ska ha tillträde till CA lokaler.

Om annan än normalt behörig personal ska vistas i dessa lokaler ska de ledsagas av behörig personal.

Det skall krävas minst två behöriga personer för att få full access till CA:s privata nyckel.

5.1.3 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.

5.1.4 Kylning av systemet

Enligt driftleverantörens standard rutiner

5.1.5 Rutin för brandskydd

Enligt driftleverantörens standard rutiner

5.1.6 Rutin för lagring av media

Enligt driftleverantörens standard rutiner

5.1.7 Avveckling av hårdvara

Hårdvara som kan innehålla känslig information skall förstöras enligt driftleverantörens rutiner för avveckling av känslig information.

5.1.8 Backup på annan plats

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

5.2 Procedurorienterad säkerhet

CA har det totala ansvaret för generering av privata nycklar och certifikat även om en del av arbetet kan åläggas en betrodd part.

5.2.1 Betrodda roller

För att uppnå fullgod säkerhet och tillgänglighet i CA-systemet skall det finnas utpekade skilda ansvarsområden beskrivna i CPS.

5.2.2 Bemanning

Direkt access till CA, skall kräva två behöriga administratörers samtidiga närvaro. Driftansvarig ansöker om behörighet hos säkerhetschef.

5.2.3 Identifiering och autentisering av varje roll

Det skall framgå i CPS hur identifiering av respektive roll sker gentemot systemet.

5.3 Personal

5.3.1 Bakgrund, kvalifikationer, erfarenheter och personkontroll

Administratörer av CA-systemet ska:

- vara tillförlitliga
- ha erhållit för ändamålet adekvat utbildning.
- Vara säkerhetskontrollerade enligt 5.3.2

5.3.2 Säkerhetskontroll

Administratörer av CA ska vara säkerhetskontrollerade i enlighet med fastställt regelverk från systemägaren.

5.3.3 Utbildningskrav

För de administratörer som arbetar med CA gäller att de har genomgått relevant utbildning för att på ett säkert sätt kunna hantera systemet enligt CPS.

5.3.4 Krav på återkommande utbildning

Administratörer som arbetar med CA skall fortlöpande utbildas i systemet.

5.3.5 Påföljd för obehörig handling

Enligt driftleverantörens standard rutiner

5.3.6 Krav på kontraktering av personal.

Enligt fastställda bestämmelser från systemägaren

5.3.7 Dokumentation till personal

Säkerhetsinstruktion ska utgå från säkerhetschef samt information om säkerhets på arbetsplats

6 Teknikorienterad säkerhet

6.1 Generering, lagring och leverans av nyckelpar

6.1.1 Nyckelgenerering

CA:s privata nyckel skall förvaras på minst två mot förändringar skyddade anordningar.

Nyckelgenerering skall ske i en kontrollerad miljö. Ingen information om den privata nyckeln hanteras utanför systemet för nyckelgenerering annat än genom säker överföring till avsedd plats.

Finns risk för att nyckelinformation temporärt lagrats i utrustning som används vid nyckelgenereringen skall denna destrueras enligt anvisning för detta.

6.1.2 Nyckellängder

Rootcertifikat 4096 bitar

Underordnad CA 2048 bitar

Utgivna certifikat minst 1024 bitar men rekommenderat 2048 bitar

6.1.3 Parametrar för publika nycklar

MSB CP styr

6.1.4 Kontroll av parametrar

Regler från MSB (nyckelanvändning, certifikatprofil dokumentation)

6.1.5 Hårdvara för nyckelgenerering

Nyckelgenerering utförs i en för ändamålet avsedd hårdvara.

6.2 Skydd av privat nyckel

CA skall skydda certifikatinnehavarens privata nyckel med de säkerhetsmekanismer som smartkort eller HSM erbjuder.

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 eller utsedd behörig person samt behörig administratör.

6.2.3 Nyckeldeponering

Ingen nyckeldeponering utförs.

6.2.4 Säkerhetskopia av privat nyckel

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 information av mycket hög konfidentialitet 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 privat nyckel

Ingen arkivering av privat nyckel får förekomma.

6.2.6 Aktivering av privat nyckel

Aktivering av CA:s privata nyckel ska kräva att två personer deltar i processen.

6.2.7 Deaktivering av privat nyckel

Säkerhetschef beslutar om deaktivering av privat nyckel.

6.2.8 Förstöring av privat nyckel

När CA:s privata nyckel upphört att gälla skall denna förstöras enligt dokumenterad destruktionsrutin från säkerhetschef

6.3 Övriga aspekter på hantering av nyckelpar

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

CA skall i certifikat ange giltighetsperioden för utfärdat certifikat. Under certifikatets giltighetstid skall CA tillhandahålla erforderlig service för spärrning av certifikat.

CA kan utge flera på varandra följande certifikat tillhörande samma privata nyckel så länge den privata nyckelns användningstid ej överstigs.

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 skyddas 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 ska skyddas.

6.5 Säkerhet i datorsystem

6.5.1 Specifika säkerhetskrav

Installation av operativsystem och system för certfikatutgivning sker i direkt anslutning till formatering av diskar och med leverantörens original programvara.

Vid installation av CA samt vid nyckelceremoni ska minst två personer deltaga i processen. Säkerhetschef samt behörig administratör.

Vid registrering av initiala behörigheter i systemet ska minst två personer deltaga i processen.

Alla ovanstående operationer loggas i ett protokoll över installations- och konfigurationsprocessen. Detta protokoll signeras av deltagande personer och arkiveras på ett säkert sätt av säkerhetschef.

6.5.2 Säkerhetsklassning

Inga bestämmelser

6.6 Säkerhets vid utveckling och underhåll

6.6.1 Kontroller under Systemutveckling

Programutveckling för CA systemet skall ske i en separat miljö hos leverantören.

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 kan medges för 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

Systemet för certfikatutgivning skyddas av en brandvägg med tillräcklig skyddsnivå för att motstå hot och angrepp som misstänks kan inträffa. Brandväggen ska vara konfigurerad så att endast nödvändiga protokoll för systemet för certifikatutgivning kan passera.

Informationsbärare som innehåller uppgifter som läses in i CA-systemet ska ha sitt ursprung säkerhetsställt och kontrolleras innan inläsning.

6.8 Komponenter med kryptologisk funktionalitet

Med komponenter med kryptologisk funktionalitet avses specifik hårdvara för lagring av kryptologiska nycklar, t ex CA:s privata nyckel.

Denna komponent med funktion enligt ovan ska vara godkänd av Myndigheten för samhällsskydd och beredskap.