Region Stockholm

Certifikatspolicy (CP) för PKI RS

Region Stockholm

OID: 1.2.752.97.9.1.4.1
Version: 1.0

Dokumentet ägs och förvaltas av Region Stockholm, Serviceförvaltningen, Digital infrastruktur.

Innehållsförteckning

1 Inledning

Denna certifikatspolicy beskriver de procedurer och rutiner som ska tillämpas vid utfärdande av certifikat för personer och enheter i Region Stockholms PKI (hädanefter benämnd ”PKI RS”). Beskrivning av rutiner och organisation för tillämpning av denna certifikatspolicy finnas i en separat Certification Practice Statement (CPS) med namnet ” Certification Practice Statement (CPS) för PKI RS (OID 1.2.752.97.9.1.4.2).

Denna Certfikatspolicy följer IETF RFC 3647, ”Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” om inget annat anges, och eventuella avvikelser kommer att specificeras där de förekommer.

1.1 Översikt

I toppen av hierarkin för PKI RS är det Region Stockholms Serviceförvaltning (nedan benämnd SF) som äger och förvaltar denna certifikatpolicy och som fastställer det regelverk som deltagarna i PKI RS måste följa. Utfärdare (Registration Authority, RA) är enheter som verifierar certifikatbegäran inom PKI RS. SF kan agera som RA för Region Stockholm samt de förvaltningar, bolag och stiftelser där Region Stockholms ägarandel uppgår till minst 50 procent.

Denna certifikatpolicy beskriver de förfaranden och rutiner som tillämpas inom ramen för PKI RS och omfattar utfärdandet av certifikat till fysiska personer, system och enheter. Inom ramen för PKI RS utfärdas certifikat enligt olika certifikatprofiler som styr certifikatinnehåll. Verksamheter som sköter driften av en eller flera CA-instanser inom ramen för PKI RS måste upprätta en så kallad Utfärdardeklaration (CPS) som måste godkännas av SF. RA som är verksamma inom ramen för PKI RS måste upprätta ett så kallat Registration Authority Practice Statement (RAPS) som måste godkännas av SF.

1.2 Dokumentnamn och identifikation

De rutiner och åtaganden som följer av denna certifikatpolicy är endast tillämpliga i samband med sådana certifikat där nedanstående policy åberopas. Policynamn för denna policy är Certifikatspolicy (CP) för PKI RS - Certifikatspolicy för utfärdande av certifikat inom PKI RS.

Objektidentifierare (OID) för denna policy är 1.2.752.97.9.1.4.1

1.3 Deltagare

1.3.1 Certification Authority

Region Stockholm, SF, Digital infrastruktur innehar det totala ansvaret för PKI RS, inklusive de delar som utförs av eventuella underleverantörer. Region Stockholm, SF, Digital infrastruktur tillser att dess eventuella underleverantörer följer denna certifikatpolicy alla tillämpliga delar.

I enlighet med denna certifikatpolicy ska en CA:

1. garantera att all information i utfärdade certifikat är korrekt och kontrollerad i enlighet med denna certifikatpolicy
2. utfärda certifikat i enlighet med de certifikatprofiler som godkänts av SF
3. publicera och lagra information i enlighet med avsnitt 2
4. utföra de åtgärder för identifiering som anges i avsnitt 4.1
5. spärra certifikat och upprätta spärrlistor enligt avsnitt 4.9
6. implementera kontrollåtgärder enligt avsnitt 4.9, 5 och 6
7. förfoga över tillräckliga, finansiella och andra resurser, för att kunna bedriva verksamhet och bära risken för skadeståndsskyldighet
8. genomföra revisioner i enlighet med denna certifikatpolicy
9. upprätta ett så kallat Certification Practice Statement (CPS), också benämnd Utfärdardeklaration, som måste godkännas av Region Stockholm, SF, Digital infrastruktur och försäkra dess efterlevnad.

Detta policydokument omfattar följande utfärdare:
(x i CA-namnet indikerar löpnummer för CA på samma tillitsnivå)

Region Stockholm RSA Rot CA är off-line och utfärdar inte certifikat till slutanvändare.

Rot- CA:s uppgifter är att:

- utfärda och hantera underliggande CA-certifikat och dess livscykel
- skapa och publicera spärrlistor (CRL) periodiskt och i händelse av spärr av CA
- publicera CA-certifikat som utfärdats av rot-CA.

Region Stockholm RSA CA0x L3 som utfärdar certifikatför följande syften

- Logga in med smartkort
- Digital signatur
- Kryptering
- Autentisera klient

Region Stockholm RSA CA0x L2 som utfärdar certifikat för följande syften:

- Serverautentisering
- Klientatuentisering

1.3.2 Registration Authority

Ett CA kan delegera ansvar för beställning, identifiering, autentisering, utlämnande, och spärr av certifikat till ett eller flera RA. Detta ansvar beskrivs i förekommande fall i en RA-policy som är underställd denna certifikatpolicy. RA måste upprätta ett så kallat Registration Authority Practice Statement (RAPS) där det framgår hur RA:n uppfyller kraven för utgivning som listas i RA-policyn. En RAPS måste godkännas av SF.

En Registration Authority har som uppgift att:

- etablera procedurer för utfärdande av certifikat
- identifiera och autentisera ansökande part
- vidarebefordra beställning av certifikat till CA
- initiera eller vidarebefordra begäran om revokering av certifikat
- hantera ansökan om förnyelse av certifikat eller nycklar.

1.3.3 Certifikatsinnehavare

En certifikatinnehavare kan vara en fysisk person som tjänstgör vid eller har en etablerad relation med Region Stockholm eller en server eller annan enhet som ägs eller förvaltas av Region Stockholm eller någon av de förvaltningar, bolag eller stiftelser där Region Stockholms ägarandel uppgår till minst 50 procent.

CA ansvarar för att de väsentliga kraven på certifikatinnehavaren enligt denna certifikatpolicy erinras certifikatinnehavaren.

1.3.4 Förlitande parter

Förlitande parter är en organisation eller person som agerar med tillit till ett certifikat som utfärdats inom ramen för PKI RS. Förlitande part och SF kan i förekommande fall reglera denna partsrelation med ett Förlitandepartsavtal.

1.3.5 Andra aktörer

SF tillser att eventuella andra aktörer som verkar inom ramen för PKI RS följer denna certifikatpolicy i alla tillämpliga delar.

1.4 Certifikatsanvändning

1.4.1 Tillåten certifikatsanvändning

Certifikat utgivna av Region Stockholm RSA CA0x L3 får användas av fysiska personer för att signera och kryptera information. Certifikat utgivna av Region Stockholm RSA CA0x L3 ska vara placerade på en av SFs PKI RS förvaltning godkänt hårdvarutoken och som beskrivs i ETSI EN 319 411-2 som "QSCD".

I övrigt gäller följande: Ett certifikat kan användas för andra ändamål, förutsatt:

- att förlitande parten kan förlita sig på certifikatet
- att användningen inte är förbjudet enligt lag
- att användningen är förenlig med upprättade avtal.

Korrekt användning av nyckel, som listas i alla certifikat under rubriken "Nyckelanvändning och "Avancerad nyckelanvändning", ska tas i beaktande vid användandet av certifikat och deras tillhörande privata nyckel.

Det är utanför Region Stockholms kontroll att förhindra att privata nycklar används för oönskade ändamål eller ändamål som inte ryms inom CA:s avsikt. Det ligger i innehavarens intresse och ansvar att bara använda den privata nyckeln i tillförlitliga applikationer och känd utrustning. En innehavare ska aldrig använda den privata nyckeln för att signera data eller dokument som denne inte i förhand har granskat och godkänt.

1.4.2 Otillåten användning av certifikat

Användning som inte är listad ovan är otillåten.

1.5 Förvaltning av Policy

SFs PKI RS förvaltning äger och förvaltar denna certifikatpolicy och ansvarar för att:

1. specificera och godkänna certifikatpolicyn i enlighet med en definierad process för översyn, inklusive ansvar för att sprida, upprätthålla och spåra ändringar i certifikatpolicyn
2. definiera krav och riktlinjer för användning av digitala certifikat och specificera dem i certifikatpolicyn och berörda avtal
3. godkänna nya och ändrade Certificate Practice Statements (CPS)
4. återkommande granska att de kontroller som definierats i certifikatpolicyn efterlevs
5. i förekommande fall särskilt definiera krav och riktlinjer som avser beställning identifiering, autentisering, utlämnande och spärr av certifikat och specificera dem i RA-policyn och berörda avtal
6. i förekommande fall godkänna nya och ändrade Registration Authority Practice Statements (RAPS)
7. i förekommande fall återkommande granska att de kontroller som definierats i RA-policyn efterlevs
8. tillse att revision återkommande genomförs och att resultatet tillämpas.

SFs PKI RS förvaltning ansvarar för att publicera en aktuell version av:

1. denna certifikatpolicy (CP)
2. i förekommande fall RA-policy
3. i förekommande fall Förlitandepartsavtal.

1.5.1 Förvaltningsorganisation för certifikatpolicy

PKI RS förvaltning har sin linjetillhörighet inom SF.

1.5.2 Kontaktinformation

Adress	**Region Stockholm** SF Box 22550, 104 22 Stockholm **Besöksadress** Lindhagensgatan 98 104 22 Stockholm
Telefon	Telefon växel: 08 – 123 100 00
E-post	pki-rs.sf@regionstockholm.se
Webb	https://www.regionstockholm.se/pki-policydokument

1.5.3 Överensstämmelse

SFs PKI RS förvaltning bestämmer lämpligheten och tillämpligheten av denna certifikatpolicy.

1.5.4 Godkännandeprocess

Godkännande av denna certifikatpolicy och efterföljande ändringar och tillägg ska göras av SFs PKI RS förvaltning.

Ändringar ska vara i form av en uppdaterad certifikatpolicy.

1.6 Definitioner och förkortningar

Se bilaga 1 för definitioner och förkortningar.

2 Publicering och lagring av certifikatsinformation

2.1 Lagringsplatser

PKI RS förvaltning ansvarar för att följande information finns tillgänglig på följande platser:

1. Denna certifikatpolicy publiceras på https://open.sp.sll.se/sites/kundwebb/forvaltningosystem/ och http://pki.regionstockholm.se/PKI_RS-klass-1-CA.v1.capolicy.htm
2. CA-certifikat publiceras på http://pki.regionstockholm.se/aia/
3. Spärrlistor (CRL) publiceras på http://pki.regionstockholm.se/crl

2.2 Publicering av certifikatsrelaterad information

PKI RS förvaltning ansvarar för att göra följande information och tjänster tillgängliga:

1. denna certifikatpolicy
2. en utfärdardeklaration (CPS) refererande till denna certifikatspolicy
3. i förekommande fall RA-policy (RAP)
4. samtliga CA-certifikat
5. spärrlista innehållande information om vilka certifikat som spärrats.

2.3 Tidpunkter och frekvenser för publicering

CA information och certifikat ska publiceras utan dröjsmål efter varje förändring.

Spärrlista avseende denna rot-CA utfärdas minst en gång var 6 månad, samt omedelbart efter att ett CA certifikat spärras. Spärrlista för slutanvändarcertifikat ska publiceras minst en gång per dygn. Ett certifikat kan komma att tas bort från spärrlistan när dess giltighetstid löper ut. Informationen på publiceringsplatsen skall vara åtkomligt 24/7. Undantag kan göras för systemunderhåll.

2.4 Behörighetskontroll för lagringsplatser

Informationen på lagringsplatser enligt sektion 2.1 är publik, och PKI RS förvaltning gör inga kontroller eller avsiktliga begränsningar av åtkomsts till denna. SF ansvarar för att genomföra återkommande kontroller för att säkerställa att obehöriga inte via publika lagringsplatser kan lägga till, ta bort eller ändra publicerad information.

3 Identifiering och autentisering

3.1 Namngivning

3.1.1 Olika typer av namn

Certifikat utfärdade till fysiska personer ska innehålla följande identifierare:

- För- och efternamn + HSA-id (Subject / CN)
- AD-kontonamn/ UPN (Subject Alternative Name / User Principal Name)

Certifikat utfärdade till servrar och andra enheter ska innehålla följande information:

- DNS-namn (FQDN) eller
- IP-adress

3.1.2 Krav på meningsfull information i certifikatet

Personuppgifter i certifikat utfärdade till fysiska personer ska kunna verifieras mot Nationella HSA-katalogen och Region Stockholms katalog över anställda (EK).

3.1.3 Anonyma eller pseudonyma innehavare

Certifikat utfärdade till fysiska personer får endast använda pseudonymer när det enligt lag eller förordning krävs för att skydda identiteten på en fysisk person och först efter godkännande av SF. I förekommande fall kan ansvaret för godkännande delegeras till RA.

3.1.4 Regler för tolkning av identitetsuppgifter

Inga krav stipuleras.

3.1.5 Unika namn

Certifikatets subjekt ska innehålla unika identifierare.

3.1.6 Erkännande av olika typer av varumärken

Ej tillämpbart.

3.2 Ursprungsidentifiering

3.2.1 Metod att bevisa innehav av privat nyckel

Innehavaren måste visa att den ensam innehar och förfogar över det hårdvarutoken på vilken den privata nyckeln genereras.

3.2.2 Autentisering av organisationsidentitet

Ej tillämpbart.

3.2.3 Kontroll av uppgiven identitet

Ursprungsidentifieringen och autentisering av ansökanden ska göras vid fysiskt möte. Certifikat från Region Stockholm RSA CA01 L3 v2 utfärdas endast till innehavare av ett hårdvarutoken och som beskrivs i ETSI EN 319 411–2 som "QSCD". Exempel på en sådant hårdvarutoken är Region Stockholms eTjänstekort (SITHS).

3.2.3.1 Krav på identitetskontroll

Sökanden ska legitimera sig på likvärdigt sätt som vid utgivning av en fullgod identitetshandling.

3.2.3.2 Procedur för autentisering

Kontroll ska göras att sökandes uppgifter finns registrerade i ett officiellt register.

3.2.4 Icke-verifierade identiteter

Ej tillämpbart vid utfärdande av certifikat till fysiska personer.

3.2.5 Kriterier för interoperabilitet (korscertifiering mellan CA:s)

Inga krav stipuleras.

3.3 Identifikation och autentisering vid begäran om förnyelse av nycklar

Förnyelse av nycklar är inte tillåten inom ramen för denna CP.

3.4 Identifiering och autentisering vid begäran om spärrning

Proceduren för att spärra certifikat måste föregås av en validering som säkerställer att spärren faktiskt begärts av:

- innehavaren,
- i förekommande fall den RA som utfärdat certifikatet, eller
- PKI RS förvaltning

Orsaken till spärr kan vara, men är inte begränsat till:

- förlust eller misstanke om kompromettering av privat nyckel
- otillåtet användande av certifikat
- dödsfall
- kompromettering av utfärdande CA
- verksamheten för utfärdande CA:s upphör.

Metoden för validering för varje begäran av spärrning ska loggas. Vid avsteg från kraven på validering ska orsaken dokumenteras.

PKI RS förvaltning får endast spärra certifikat när nyckelinnehavaren, eller i förekommande fall RA, inte är i stånd att begära spärrning eller vid misstanke om oegentligheter relaterat till ett utfärdat certifikat eller dess privata nyckel. Avsteg får i dessa fall göras från kraven på validering.

4 Operationella krav

4.1 Certifikatsansökan

En ansökan om certifikat ska göras personligen och genom att fysiskt besöka av PKI RS förvaltning utsedd utfärdarfunktion, (RA). RA vidarebefordrar efter utförda kontroller ansökan till CA funktionen i de fall den inte själv kan utfärda certifikatet.

4.1.1 Vem får ansöka om certifikat

Följande får ansöka om certifikat:

- fysiska personer som är anställda av eller har en avtalsrelation med Region Stockholm
- serveradministratörer eller motsvarande

4.1.2 Ansökningsprocedur och ansvarsfördeling

4.1.2.1 Certifikat utfärdade till fysiska personer

Den ansökande ska:

- göra en ansökan med sanningsenlig och korrekt information
- demonstrera innehav eller exklusiv kontroll av den privata nyckeln som motsvarar den publika nyckeln som levererades till certifikatutfärdaren.
- godkänna villkor för innehav och användande

4.1.2.2 Certifikat utfärdade till fysiska personer genom certifikatsväxling

Den ansökande ska:

- autentisera sig med av DIGG godkänd e-legitimation
- presentera en godkänd mobil enhet för registrering
- godkänna villkor för innehav och användande

4.1.2.3 Certifikat utfärdade till servrar eller andra enheter

Den ansökande ska

- vara registrerad som rättighetshavare i utfärdandesystemet
- förfoga över den server eller enhet som certifikatet utfärdas till

4.2 Ansökningsprocess för certifikat

4.2.1 Utföra identifierings och autentiseringsfunktioner

Ett CA, eller i förekommande fall RA, ska utföra identifiering och autentisering av all nödvändig information i enlighet med kraven i avsnitt 3.

En ansökan ska uppfylla följande procedurer:

1. CA, eller i förekommande fall RA, ska säkerställa att alla tillämpliga villkor accepteras av den sökande. I detta förfarande deklarerar den tänkta nyckelinnehavaren all relevant information
2. den sökande identifieras och autentiseras av CA, eller i förekommande fall RA. All ansökningsinformation verifieras
3. ansökningshandlingar arkiveras.

4.2.2 Godkännande eller avslag på ansökan

Ett CA, eller i förekommande fall RA, kan godkänna en ansökan om följande kriterier är uppfyllda:

- lyckad identifiering och autentisering av all erforderlig information i enlighet med avsnitt
- sökanden är behörig att få ett certifikat utställd enligt avsnitt

Ett CA, eller i förekommande fall RA, kommer att avslå en ansökan om:

- identifiering och autentisering av all erforderlig information i enlighet med avsnitt 3 misslyckats
- den sökande inte är tillgänglig för erforderliga kontroller
- inte godkänner villkoren för utfärdande.

4.2.3 Tid att behandla certifikatsansökan

CA, eller i förekommande fall RA, ska hantera certifikatansökningar utan onödigt dröjsmål. En certifikatansökan är under behandling till dess den godkänns eller avslås.

4.3 Certifikatsutgivning

4.3.1 CA aktiviteter vid certifikatsutfärdande

Ett certifikat skapas och utfärdas först efter godkännande av en certifikatansökan från en behörig företrädare för ett CA, eller i förekommande fall av en behörig företrädare för ett RA. Varje certifikatansökan ska kunna spåras till ansökande part.

4.3.2 Information till sökande vid certifikatutfärdande

Ett CA ska vid utfärdandet av ett certifikat informera sökande om att ett certifikat är utfärdat för denne och informera hur certifikatet tillgängliggörs.

4.4 Certifikatacceptans

4.4.1 Mottagningsbevis

Följande handlingar utgör acceptans av certifikatet och de allmänna villkor som reglerar användandet

- certifikatet har laddats ner, använts och/eller installerats
- användande av certifikatet för något av dess avsedda syften.

4.4.2 CA:s publicering av certifikatet

Inga krav stipuleras.

4.4.3 Anmälan om utfärdande av certifikat

PKI RS anmäler inte utfärdande av certifikat till någon annan än användaren.

4.5 Användning av nycklar och certifikat

4.5.1 Nyckelinnehavarens användning av privata nyckeln och certifikatet

Användning av den privata nyckel som motsvarar den publika nyckeln i certifikatet är endast tillåten för de ändamål som beskrivs i denna policy i sektion 1.4.1 och vad som är tillåtet enligt de villkor som beskrivs i allmänna villkor för upprättade avtal.

4.5.2 4.5.2 Förlitande parts användning av publik nyckel och certifikat

Förlitande parter måste samtycka till villkoren i upprättade avtal. Förlitande part ska självständigt bedöma lämpligheten att använda ett certifikat för varje givet syfte i enlighet med:

- upprättade avtal
- denna certifikatpolicy.

Den publika nyckeln eller certifikatet får endast användas:

- under förutsättning att certifikatet inte är spärrat
- i överensstämmelse med värdet i fälten ”Nyckelanvändning” eller ”Avancerad nyckelanvändning” i certifikatet
- i enlighet med upprättade avtal
- i enlighet med denna certifikatpolicy.

Förlitande part är skyldig att kontrollera status på certifikatet på det sätt som stipuleras i denna CP.

4.6 Förnyelse av certifikat

Certifikatförnyelser sker på samma sätt och enligt samma villkor som utfärdande av nya certifikat.

4.7 Förnyelse av certifikatets nyckelpar

Denna certifikatpolicy medger inte att nyckelpar återanvänds.

4.8 Certifikatsmodifiering

Certifikatsmodifiering sker genom utfärdande av nytt certifikat.

4.9 Spärr av certifikat

CA ska tillhandahålla en tjänst för spärr av certifikat. CA ska kontinuerligt skapa en signerad spärrlista där den mest aktuella spärrlistan ska tillgängliggöras och tillhandahållas i enlighet med denna certifikatpolicy. Spärrlistan ska innehålla spärrade certifikat vars giltighetstid inte passerat.

Denna certifikatpolicy medger inte tillfällig spärr av certifikat.

4.9.1 Omständigheter för spärr

Ett CA spärrar ett certifikat av någon av följande orsaker:

- om innehavaren avslutar sin anställning
- om innehavaren förlora eller blir bestulen på certifikatet och dess bärare
- om någon väsentlig information som finns i certifikatet ändras
- vid begäran från innehavaren
- om ett CA avslutar sitt uppdrag som CA
- vid certifikatanvändning som är i strid med denna certifikatpolicy
- vid misstanke om oegentligheter.

4.9.2 Behöriga att begära spärr

Följande kan begära en spärr av ett certifikat:

- nyckelinnehavaren
- i förekommande fall den RA som utfärdat certifikatet
- PKI RS förvaltning

PKI RS förvaltning får endast spärra certifikat när nyckelinnehavaren eller i förkommande fall RA inte är i stånd att begära spärrning. Vid misstanke om oegentligheter relaterat till ett utfärdat certifikat får ett certifikat spärras av PKI RS förvaltning och Region Stockholm SOC.

4.9.3 Rutin för hantering av spärrbegäran

Innehavaren är skyldigt att tillhandahålla tillräckligt med information för att spärrbegäran skall kunna hanteras av spärrande instans. Spärr kan göras via e-post, telefonsamtal eller personligt besök under förutsättning att säker identifiering kan göras.

Begäran om spärr ska arkiveras tillsammans med information om:

- vem som inkommit med spärrbegäran
- hur begäran mottogs
- tidpunkt för när begäran mottogs
- anledningen till spärr
- hur den enskilde som begärde spärr identifierades och autentiserades
- resultatet av spärr (lyckad/misslyckad)
- tidpunkt för registrering i CA-systemet.

4.9.4 Behandlingstid vid begäran av spärr

Spärrbegäran ska göras så snart som möjligt efter det att behov konstaterats.

4.9.5 Behandlingstid vid utförande av spärr

Spärrbegäran ska göras omgående utan dröjsmål efter mottagandet av en validerad begäran. Offentliggörande i spärrlistan ska ske inom ett dygn.

4.9.6 Krav på spärrkontroll

Förlitande part ska kontrollera status på certifikat genom att:

- hämta aktuell spärrlista från anvisad lagringsplats, eller
- göra en statusförfrågan via OCSP-protokollet mot anvisad OCSP-responder.

Förlitande part ska försäkra sig om OCSP-responsens eller spärrlistans äkthet genom att verifiera dess digitala signatur och certifikatkedja. Om ett certifikat är spärrat eller om spärrkontroll inte går att genomföra ska inte certifikatet accepteras.

4.9.7 Frekvens på utgivning av spärrlista

- CRL för utfärdande CA ska minst en gång var 6 månad och utan dröjsmål vid förändringar.
- CRL för slutanvändarcertifikat ska utfärdas minst en gång per dygn.

4.9.8 Maximal latenstid för CRL

Uppdaterad spärrlista ska tillgängliggöras utan dröjsmål.

4.9.9 Tillgång till realtidsspärr och giltighetskontroll (OCSP)

PKI RS tillhandahåller certifikatsstatuskontroll över OCSP-protokollet på adressen http://ocsp.regionstockholm.se/ocsp.

4.9.10 Krav på realtidsspärr och giltighetskontroll

Förlitande part är skylig att kontrollera ett certifikats giltighet. Om inte förlitande part kan kontrollera ett certifikats giltighet kan denne inte acceptera certifikatet med för CA bindande verkan.

4.9.11 Andra sätt att tillhandahålla spärrkontroll

Inga krav stipuleras.

4.9.12 Särskilda krav om nycklar röjs

Om någon part misstänker att privata CA-nycklar är röjda ska PKI RS förvaltningen meddelas utan dröjsmål. Om de privata nycklarna för ett CA misstänks vara röjda ska PKI RS förvaltning informera samtliga parter enligt punkt 1.3 ovan.

4.9.13 Omständigheter för tillfällig spärr

Denna certifikatpolicy medger inte tillfällig spärr.

4.10 Tjänster avseende certifikatstatus

4.10.1 Operationella egenskaper

Status för utfärdade certifikat är tillgängligt via spärrlista på adress http://pki.regionstockholm.se/crl och OCSP-tjänst på adress http://ocsp.regionstockholm.se/ocsp

4.10.2 Tillgänglighet

Tjänster för kontroll av certifikatsstatus ska vara tillgängliga 24/7 med undantag för avbrott i samband med schemalagt systemunderhåll.

4.10.3 Tillval av funktioner

Inga krav stipuleras.

4.11 Avslut av innehav

Innehavet av certifikat upphör genom att förlängning inte sker i samband med giltighetstidens utgång eller att certifikatet spärras utan att ersättas av ett nytt.

4.12 Nyckeldeponering och nyckelåterställning

PKI RS tillhandahåller inte nyckeldeponering eller nyckelåterställning.

5 Faciliteter, förvaltning och verksamhetsstyrning

5.1 Fysisk säkerhet

Fysisk säkerhet syftar till att skydda de system som generera nycklar, identifierar innehavare, utfärdar certifikat, spärrar certifikat och de kringliggande system som säkrar spårbarhet i processen. Det kan vara skydd mot konsekvenser av naturkatastrofer, olyckor och fel i tekniska system samt mänskliga misstag och slarv eller sabotage.

5.1.1 Placering och konstruktion

Anläggningen som rymmer centrala CA-funktioner är fysiskt placerad i en starkt skyddad datorhall. I denna datorhall är viktiga komponenter inlåsta i separata och fristående säkerhetsskåp. Datorhallen som är låst och larmad befinner sig i en byggnad som även den är låst och larmad. Dessa skyddas gemensamt genom aktiv bevakning.

5.1.2 Fysiskt tillträde

Åtkomst till utrymmen som ger tillgång till systemet för framställning av certifikat eller funktioner som kan påverka till CA-funktionens integritet ska vara begränsad till behörig personal samt ske enligt följande:

- inpassering till utrymmen skall kräva identifiering med kort eller motsvarande
- allt tillträde skall loggas och kunna spåras
- om icke behörig personal har uppdrag som kräver åtkomst till dessa utrymmen ska detta ske i sällskap med behörig personal. Dessa aktiviteter ska vara aviserade i förväg och loggas.

5.1.3 Strömförsörjning och luftkonditionering

Strömförsörjning och kylning ska ha tillräcklig kapacitet och tillgänglighet för att möjliggöra att tillgänglighet till vitala funktioner för CA upprätthålls. Detta innebär att adekvata backup-system ska finnas tillgängliga för infrastruktur som används för att tillhandahålla funktionen såsom strömförsörjning, ventilation, luftkonditionering och för övervakning av temperatur och luftfuktighet.

5.1.4 Vattenexponering

CA-funktionen och dess underliggande tekniska plattform ska vara skyddad mot vattenexponering.

5.1.5 Brandskydd och förebyggande åtgärder

CA-funktionen och dess underliggande tekniska plattform ska skyddas mot brand genom förebyggande åtgärder som rökdetektorer och temperaturgivare. Släckningsfunktioner och rutiner ska finnas för att förhindra spridning av brand och rökgaser. Samtliga proaktiva åtgärder ska utformas och utföras enligt gällande lokala brandföreskrifter.

5.1.6 Lagring av media

Media som rör CA-funktionen, och är i direkt eller indirekt beroende av funktionen, ska förvaras på ett säkert sätt. CA-kritisk information som lagras på media ska skyddas från brand, vatten och andra yttre miljörisker. Säkerhetskopierat data ska skyddas på likvärdigt sätt.

5.1.7 Avfallshantering

Media innehållande känsliga data skall destrueras så att det inte på något sätt går att återskapa till läslig form.

5.1.8 Säkerhetskopia på annan plats

Säkerhetskopior av kritiska systemdata och andra känsliga uppgifter ska lagras på en säker plats skild från produktionsplatsen.

5.2 Procedurorienterad säkerhet

5.2.1 Betrodda roller

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

- Security Officer (Säkerhetsansvarig för CA-tjänsten.)
- CA-administratör (genererar nya rot- och CA-certifikat)
- CA-operatör (genererar och levererar certifikat till nyckelinnehavaren).
- RA-operatör (validerar och registrerar nyckelinnehavens uppgifter i CA-systemet).
- Auditör - (granskare av CA-funktionen)

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

Innehavare av betrodda roller ska vara pålitliga och ha god kännedom om de aktivtiter som rollen omfattar. För att undvika att en enda person får behörigheter att själva utföra operationer som normal ska kräva två personer ska rollerna fördelas på ett sätt som eliminerar risken för det och att det över tid sker revidering av rollinnehavare.

5.2.2 Roller med krav på dualitet

Kritiska operation i PKI kräver att minst två personer (värdet **M** i uttrycket M av N) deltar. Dessa operationer omfattar, men begränsas inte till:

- generering, deaktivering och destruering av CA-nycklar
- aktivering av signeringsnycklar för CA
- backup av CA:s privata nyckel
- signering av underliggande CA:s certifikat
- initiering och aktivering av HSM

Det finns inget krav på specifikt antal innehavare av respektive roll, men det ska vara tillräckligt många för att garantera att underliggande uppgifter skall kunna utföras vid var tid, men inte fler än vad som krävs.

Hanterandet av kryptografisk hårdvara kräver flera betrodda personer under hela dess livscykel, från mottagande av leverans och hantering av nycklar fram till slutlig destruktion.

5.2.3 Identifiering och autentisering av rollinnehavare

Rollinnehavare ska identifiera och autentisera sig vid tilldelning av roll och innan denne tillåts utföra någon av de aktiviteter som rollen innehar behörighet till. Vid systemkritiska operationer skall detta ske med stark autentisering/tvåfaktorsautentisering.

5.3 Personal

5.3.1 Krav på kompetens och erfarenhet

Personal som innehar roller enligt 5.2.1, som ur säkerhetssynpunkt betraktas som kritiska, ska vara särskilt utvalda och pålitliga samt ha uppvisat lämplighet för sådana befattningar. Personal ska inte inneha andra uppgifter som kan vara i konflikt med de åtaganden och ansvar som följer av de roller som de har i CA-systemet.

5.3.2 Kontroll av bakgrund

Personal som hanterar CA, och i förekommande fall RA, ska prövas enligt de instruktioner som återfinns i Region Stockholms ”Tillämpningsanvisning - Informationshantering vid rekrytering, anställning och avslut av anställning.” (LS 2016-0067), stycket ”Rekrytering”

5.3.3 Utbildningskrav

Alla innehavare av de administrativa rollerna har genomgått de utbildningar och den träning som krävs för att på ett säkert sätt utföra sina arbetsuppgifter inom ramen för denna certifikatpolicy och inom ramen för Region Stockholms säkerhetspolicy.

Träning och utbildning ska minst innefatta följande områden:

- hårdvara och mjukvaruversioner som används
- rollbeskrivningar och tillhörande arbetsmoment som förväntas utföras av funktionen
- incidenthantering och rapporteringsrutiner och tillhörande procedurer
- återställningsrutiner och katastrofhanteringsrutiner.

5.3.4 Frekvens och krav på repetitionsutbildning

CA, och i förekommande fall RA, ska tillhandahålla fortbildning för sina anställda i den omfattning och frekvens som krävs för att säkerställa att personalen upprätthåller minst den kompetensnivå som krävs för att utföra sina arbetsuppgifter på ett tillfredsställande sätt.

5.3.5 Sekvens och frekvens av arbetsrotation

Inga krav stipuleras.

5.3.6 Påföljd för obehöriga handlingar

Personal som genom sitt beteende visar sig vara olämplig för sina arbetsuppgifter ska befrias från känsliga roller inom CA-systemet.

5.3.7 Krav på konsulter

CA, och i förekommande fall RA, kan tillåta tjänsteleverantörer eller konsulter att bli betrodda personer endast i den utsträckning som krävs för att möta ett definierat behov samt under följande villkor:

- när det saknas egna resurser för ändamålet
- om tillitsnivån på externa resurser är minst densamma som för egna resurser
- om det kan fastställas att externa resurser inte har någon intressekonflikt som kan påverka CA negativt.

I övrigt ska tjänsteleverantörer eller konsulter endast ges åtkomst till faciliteter, som används för CA-funktioner, under övervakning av betrodd personal. Tjänsteleverantörer och konsulter ska i förväg ha ingått ett sekretessavtal.

5.3.8 Dokumentation till anställda

Rutiner och processbeskrivningar som är relevanta för varje definierad roll och funktion ska göras tillgänglig för all personal som har ansvar och fyller en eller flera roller definierade i denna policy.

5.4 Säkerhetsloggning

5.4.1 Händelser som ska loggas

I och i direkt anslutning till CA-systemet ska minst följande händelser loggas:

- Operativa händelser, omfattande men inte begränsat till:
  - skapande av användarkonton
  - initiering av transaktioner, med information om vem som begärde transaktionen, tidpunkt, vilken typ av transaktion som initierats samt uppgift om resultatet av initieringen
  - installation och uppdatering av programvara
  - relevant information om säkerhetskopiering
  - start och stopp av systemet
  - datum och tid för uppgradering av maskinvara
  - datum och tid för säkerhetskopiering och tömning av loggar
  - datum och tid för säkerhetskopiering och tömning av arkivdata
  - generering av CA:s egna nycklar och eventuella underordnade CA:s nyckelprocedurer
  - förändringar i egenskapsinformation för CA eller dess nycklar
  - förändringar i kryptografiska livscykelhanteringar (eg., kvitton, användande, om-installation eller de-aktivering)
  - utlämnande och innehav samt användning av aktiveringsdata för CA:s privata nyckelmaterial, fysiska accessloggar
  - system- eller konfigurationsförändringar och underhållsaktiviteter
  - uppgifter rörande destruktion av media innehållande nyckelmaterial, aktiveringsdata eller slutkundsinformation.
- Livscykelhändelser relaterat till certifikat, omfattande, men inte begränsat till:
  - utfärdande
  - förnyelse
  - spärr.
- Behörig personal-händelser, omfattande men inte begränsad till:
  - in- och utloggning
  - in- och utloggningsförsök
  - försök att skapa, radera, sätta lösenord eller ändra systemprivilegier för priviligierade konton.
- Avvikelser- och incidentrapporter såsom, men inte begränsad till
  - otillåtna inloggningar till system och nätverk
- Nekade läs och skrivförsök i kataloger
- Förändringar i certifikatpolicy, t ex giltighetstid.

I system för nerläsning av certifikat till av smarta kort ska följande information loggas:

1. referens till kortbeställning
2. chipnummer
3. kortnummer
4. serienummer
5. datum och tid för personalisering.

5.4.2 Kontroll av loggmaterial

Loggmaterial ska granskas och analyseras regelbundet. Logganalysen ska innefatta genomgång av materialet och signifikanta logghändelser ska dokumenteras i en sammanfattning. Analysen ska även verifiera att loggmaterial inte otillbörligt har förändrats. Åtgärder som vidtagits som resultat av en logganalys ska dokumenteras.

5.4.3 Lagringstid för loggmaterial

Loggmaterial ska bevaras i minst 10 år.

5.4.4 Skydd av loggmaterial

Loggmaterial ska skyddas mot otillbörlig förändring genom de logiska skyddsmekanismerna i operativsystemet samt genom att systemet i sig inte är fysiskt och logiskt åtkomligt annat än för behörig personal. Alla loggposter ska vara individuellt tidstämplade. Loggmaterial ska kontrolleras en gång varje månad under överinseende av minst två personer med betrodda roller enligt denna certifikatpolicy.

5.4.5 Säkerhetskopiering

Inkrementella säkerhetskopior av loggmaterial ska ske minst dagligen och fulla säkerhetskopior ska ske minst varannan dag.

5.4.6 Logginsamling

Insamling av logg sker till interna databaser.

5.4.7 Information till loggad part

Händelse som loggas ska inte meddelas den som utförde transaktionen som initierade loggningen.

5.4.8 Sårbarhetsanalys

Sårbarhetsanalys på CA och CA-system ska göras årligen. Alla eventuella sårbarheter åtgärdas direkt efter upptäckten. Efter åtgärd ska uppföljningsanalys utföras.

5.5 Arkivering

5.5.1 Information som ska arkiveras

CA ska arkivera följande, omfattande men inte begränsat till:

- signerad begäran om utfärdande av certifikat eller spärr av certifikat
- alternativt underskriven kvittens på mottagning av smartkort eller annan bärare
- underskrivna handlingar rörande utlämning och mottagande av nycklar och PIN
- avtal rörande certifikat och nycklar
- certifikatens innehåll
- uppgift om förnyelse av certifikat, samt de meddelanden som utväxlats med certifikatinnehavaren i samband med förnyelsen
- historik rörande tidigare CA-nycklar
- uppgifter om certifiering av annan CA:s publika nyckel inklusive de uppgifter på vilka beslut om sådan certifiering grundats
- begäran om spärr och de meddelanden som utväxlats och loggats i samband med händelsen
- information om spärrade certifikat som tillhandahållits av CA
- protokoll från revisioner av CA inklusive resultat från revision om uppfyller sina åtaganden enligt denna certifikatpolicy
- i de fall information är digitalt signerat ska relevant material för signeringsverifiering lagras.
- protokoll från generering av CA-nycklar och andra aktiviteter som omfattar rot-CA

5.5.2 Lagringstid för arkiv

Arkiverad information ska bevaras och skyddas i enlighet med Regionens informationssäkerhetspolicy och -riktlinjer.

5.5.3 Skydd av arkiv

Den funktion som upprätthåller ett arkiv ska skydda arkivet så att endast auktoriserade, betrodda personer har möjlighet att få tillgång till arkivet. Arkivet ska vara skyddat mot obehörig åtkomst, ändring, borttagande eller annan manipulering. Media som hanterar arkiverat data och applikationer som krävs för att bearbeta arkiverat data ska bibehållas för att säkerställa att arkivdata kan läsas under den tidsperiod som anges i denna certifikatpolicy.

5.5.4 Rutiner för säkerhetskopiering av arkiv

Inga krav stipuleras.

5.5.5 Krav tidsstämpling av poster

Certifikat, spärrlistor och andra poster innehållande spärrdata ska innehålla datum- och tidsinformation. Om signering av poster sker bör ska valideringsfunktionella delar tas i beaktande för 7att möjliggöra framtida validering.

5.5.6 Internt eller externt system för insamling av arkivmaterial

Inga krav stipuleras.

5.5.7 Rutiner för åtkomst och verifiering av arkivmaterial

Arkiverat material som omfattas av sekretess ska inte hållas tillgängligt för externa parter i sin helhet annat än vad som krävs genom lag och beslut i domstol. Information om enskilda händelser kan erhållas på begäran av den som har behov av att förlita sig på ett utfärdat certifikat. Arkiverat material som inte omfattas av sekretess kan lämnas ut utan prövning. Till denna kategori hör även information som är allmänt tillgängligt. Arkiven bevaras så att de är läsbara under den angivna bevaringstiden. Parter görs dock uppmärksamma på att teknik för lagring av arkivmaterial kan komma att ändras och att CA i sådant fall inte åtar sig att behålla funktionell utrustning för tolkning av gammalt arkivmaterial om detta är äldre än 5 år. I dessa fall åtar sig dock CA istället att ha beredskap för att sätta upp nödvändig utrustning mot uttagande av en avgift som svarar mot kostnaderna. Om CA upphör med sin verksamhet kommer samtliga certifikatinnehavare informeras och arkivet hållas tillgängligt under den tid som angivits i denna policy. Begäran om att arkiverad information ska lämnas ut görs hos CA.

5.6 Byte av CA-nycklar

I händelse av förnyelse av CA:s nycklar skall dessa publiceras i enlighet med publicering av ursprunglig CA-information i denna certifikatpolicy.

5.7 Hantering vid kompromettering och katastrof

5.7.1 Förfarande vid allvarliga incidenter

Om ett intrångsförsök eller annan form av möjlig kompromettering av en CA blir känt, ska detta omgående utredas för att fastställa arten och graden av skada. Omfattningen av möjliga skador bedöms utifrån detta, till exempel huruvida CA-certifikat behöver spärras.

5.7.2 Korrupta resurser, programvara och/eller data

I händelse av att resurser, programvara eller data blir korrupt ska detta skyndsamt rapporteras till SFs PKI RS förvaltning som vidtar nödvändiga åtgärder för att skyndsamt återställa systemen till produktionsstatus.

5.7.3 Hantering vid misstanke om, eller konstaterande, av röjda CA-nycklar

I händelse av att en CA-nyckel har röjts ska bedömning enligt 5.7.1 göras. Om beslut har fattats om spärrning ska CA-certifikatet spärras, spärrinformationen omedelbart publiceras samt nytt CA-certifikat med nya nycklar skapas. Såväl nyckelinnehavare som förlitande parter ska informeras. Utfärdade certifikat behöver snarast bytas ut.

Är det CA:s självsignerade rotcertifikat som har röjts, måste förlitande parters applikationer lägga in det nya rotcertifikatet i sina system.

5.7.4 Kontinuitetsplaner

SF ska upprätta och underhålla en väl fungerande katastrofplan innehållande såväl manuella instruktioner och återstartrutiner för de scenarios som återkommande riskanalyser belyser som mest sannolika och har störst konsekvens.

5.8 Upphörande av CA

Följande åtgärder ska vidtas vid upphörande av CA:

- samtliga certifikatinnehavare och förlitande parter med vilka CA har avtal eller andra etablerade relationer ska meddelas så snart detta är känt i och så långt i förväg som är möjligt
- resurser för certifikatsstatuskontroll skall stängas av
- arkiverad information ska finnas åtkomligt i enlighet med denna certifikatpolicy.

6 Tekniska skyddsåtgärder

6.1 Generering och installation av nyckelpar

6.1.1 Generering av nyckelpar

De rekommendationer för vilka kryptoalgoritmer som ska användas definieras i ETSI TS 119 312.

6.1.1.1 Generering av nyckelpar för CA

Generering av nyckelpar ska utföras i kryptografisk hårdvarumodul certifierad lägst enligt standarden FIPS 140-2 nivå 3 eller motsvarande. Processen för generering av nycklar skall ske enligt ett fastställt manuskript med flerpersonerskontroll i skyddad miljö.

6.1.1.2 Generering av nyckelpar för slutanvändare

Generering av nyckelpar för slutanvändare skall ske på ett hårdvarutoken som möter kraven på QSCD (Qualified Signature Creation Device) "Anordning för skapande av kvalificerade underskrifter" som anges i ”Regulation (EU) No 910/2014 [i.1]”. Alternativt kan generering av nycklar ske av RA i en kontrollerad miljö och därefter läsas in till QSCD:n. Efter att privata nyckeln är installerad på QSCD:n ska den inte gå att extrahera.

QSCD lämnas ut personligen eller tillhandahålls av innehavaren. Generering av nycklar och installation av certifikat sker under innehavarens närvaro och överinseende.

6.1.2 Leverans av privat nyckel

6.1.2.1 Leverans av privat nyckel till CA

CA:s privata nyckel lämnar aldrig den kryptografisk hårdvarumodulen.

6.1.2.2 Leverans av privat nyckel till slutanvändare

Den privata nyckeln, som förvaras i QSCD, överlämnas personligen till slutanvändaren.

6.1.3 Leverans av publik nyckel till certifikatutfärdaren

Slutanvändarens publika nyckel överförs till CA efter nyckelgenerering över en krypterad förbindelse.

6.1.4 Leverans av publik nyckel till Förlitande part

Förlitande parter som önskar använda CA:s publika nyckel ska hämta den från den plats där den är publicerad enligt punkt 2 i detta dokument.

6.1.5 Nyckellängder

6.1.5.1 Nyckellängder för CA

CA:s nycklar ska vara genererade som:

- ECC med en nyckellängd på minst 384 bitar
- RSA med en nyckellängd om minst 4096 bitar

6.1.5.2 Nyckellängder för slutanvändarcertifikat

Slutanvändares nycklar ska vara genererade som RSA med en nyckellängd om minst 2048 bitar.

6.1.6 Nyckelparameterar vid skapande av publika nycklar

6.1.6.1 Nyckelparameterar vid skapande av CA:s publika nycklar

Samtliga CA nycklar ska skapas i en kryptografisk hårdvarumodul certifierad enligt standarden FIPS 140-2 nivå 3. Nyckellänger och nyckeltyper bestäms med utgångspunkt från vad som vid aktuell tidpunkt är känt om sårbarheter.

6.1.6.2 Nyckelparameterar vid skapande av slutanvändares publika nycklar

Slutanvändares nyckelparametrar bestäms av den mall som gäller för den aktuella certifikatstypen. Chiptypen på QSCD ska möta kraven som definieras i Common Criteria Level EAL5+ Secure Signature Protection Profiles BSI-PP-0005-2002 och BSI-PP-0006-2002.

6.1.7 Användningsområden för nycklar ("KeyUsage")

Alla utfärdade certifikat ska innehåll information i enlighet med RFC5280, som definierar certifikatets användningsområde för de associerade nycklarna.

6.1.7.1 CA-nycklar får endast användas för att signera följande data:

- Certifikat
- Spärrlistor (CRL)
- OCSP respons
- Interna loggar

6.1.7.2 Nycklar för slutanvändare får endast användas för att signera följande data:

Certifikat som utfärdas i enlighet med denna certifikatpolicy kan ha följande nyckelanvändningsområden:

- digitala signaturer
- nyckelkryptering
- oavvislighet

6.2 Skydd av privata nycklar

6.2.1 Skydd av och krav på kryptografisk modul

Rot och utfärdande CA:s nycklar ska skapas i en HSM som är certifierad enligt 140-2 nivå 3 och EAL4+ krav.

Slutanvändarens privata nycklar skapas och förvaras i chippet på korten som är utrustat med ett QSCD. Den QSCD som används för generering och förvaring av nycklar ska i förväg godkännas av Region Stockholm och minst möta kraven för certifiering enligt Common Criteria EAL 5+.

6.2.2 Flerpersonkontroll av privat nyckel (M av N)

Flerpersonkontroll krävs för att initiera kryptografiska operationer på HSM. För operationer som omfattar förändringar i konfigurationen av HSM som kan påverka funktionaliteten, eller förändringar kopplade till roller, krävs särskild roll där 2 av 4 (M av N) innehavare av rollen måste vara närvarande.

6.2.3 Deponering av privata nycklar

Privata nycklar får inte deponeras.

6.2.4 Säkerhetskopiering av privat nyckel

CA ska säkerhetskopiera privata nycklar för CA för att kunna återställa dem vid katastrofer och fel på utrustning i enlighet med denna certifikatpolicy. Privata nycklar för CA som säkerhetskopieras ska skyddas fysiskt och kryptografiskt på en nivå motsvarande, eller högre än, den för de kryptografiska moduler som de normalt lagrats i.

Privata nycklar för CA får inte säkerhetskopieras för annat syfte än backup.

6.2.5 Arkivering av privat nyckel

Privata nycklar arkiveras inte.

6.2.6 Överföring av privata nycklar till/från kryptografisk hårdvarumodul

Vid överföring av en privat nyckel i en kryptografisk hårdvarumodul ska använda mekanismer som förhindra förlust, stöld, modifiering, röjande eller otillåten användning av den privata nyckeln. Detta sker endast i backup-syfte och kräver samma behörigheter.

6.2.7 Lagring av privat nyckel på kryptografisk hårdvarumodul

Privata nycklar för CA ska lagras krypterade i en kryptografisk hårdvarumodul.

6.2.8 Metod för att aktivera privata nycklar

PKI RS privata CA-nycklar aktiveras genom att minst två personer i betrodda roller närvarar och använder sitt kryptografiska token och tillhörande aktiveringsdata

6.2.9 Metod för att avaktivera privata nycklar

CA nycklar avaktiveras genom utloggning från HSM, stänga sessionen eller stänga av HSM.

6.2.10 Metod för destruktion av privata nycklar

Privata nycklar ska destrueras på ett sätt som säkerställer att det inte finns några rester kvar av nyckeln som kan leda till återuppbyggnaden av nyckeln.

6.2.11 Gradering av kryptografisk hårdvarumodul

Se avsnitt 6.2.1.

6.3 Andra aspekter på hantering av nyckelpar

Inga privata nycklar eller annan konfidentiell information får lämna sin utpekade skyddade miljö. Vid underhåll eller motsvarande scenario när skyddande åtgärder inte kan uppfyllas, måste alla nycklar, all konfidentiell information samt lagringsmedia förstöras i enlighet med denna certifikatpolicy.

6.3.1 Arkivering av publika nycklar

Publika nycklar som används för verifiering ska arkiveras rutinmässigt i samband med utfärdande av certifikat. (Se sektion 5 för detaljer)

6.3.2 Giltighetstid för certifikat och nyckelpar

En CA ska inte utfärda certifikat med utgångsdatum som infaller efter det utgångsdatum som nyckelparet för CA har. Certifikatets giltighetstid bestämmer associerade nycklars operationella livslängd (se punkt 4.7). I övrigt gäller följande maximala giltighetstider:

Certifikatsprofil	Giltighetstid
Rotcertifikat ECC	30 år
Rotcertifikat RSA	30 år
Utfärdande CA	25 år
Slutanvändarcertifikat	5 år
Adminstratörscertifikat PKI	2 år

6.4 Aktiveringsdata

6.4.1 Generering av aktiveringsdata

Aktiveringsdata för privata nycklar ska genereras på ett sådant sätt att det förhindrar förlust, stöld, modifiering, obehörigt röjande eller obehörig användning av de privata nycklarna som skyddas av aktiveringsdata.

I de fall lösenord används som aktiveringsdata skall de ha en komplexitet som förhindrar att de på ett enkelt sätt kan gissas eller på elektronisk väg avslöjas.

6.4.2 Skydd av aktiveringsdata

Aktiveringsdata för privata nycklar ska skyddas på ett sådant sätt att det förhindrar förlust, stöld, modifiering, röjande eller otillåten användning av de privata nycklarna som skyddas av aktiveringsdata.

6.4.3 Övriga aspekter på aktiveringsdata

6.4.3.1 Överföring av aktiveringsdata

Aktiveringsdata för privata nycklar ska överföras på ett sådant sätt att det förhindrar förlust, stöld, modifiering, röjande eller otillåten användning av de privata nycklarna som skyddas av aktiveringsdata.

6.4.3.2 Förstörande av aktiveringsdata

Aktiveringsdata för privata nycklar ska förstöras på ett sådant sätt att det förhindrar förlust, stöld, modifiering, röjande eller otillåten användning av de privata nycklarna som skyddas av aktiveringsdata. Detta omfattar även kopior av aktiveringsdata som förvaras för att eliminera risken för utlåsning från produktionssystem.

6.5 Säkerhetskontroller av datorer

6.5.1 Specifika tekniska krav på datorsäkerhet

PKI RS CA ska konfigurera sina system, inklusive arbetsstationer med fjärråtkomst, på så sätt att de:

1. identifierar och autentiserar varje enskild operatör unikt innan åtkomst till system och applikationer tillåts
2. begränsar åtkomst för användaren till vad som omfattas av dennes betrodda roll
3. genererar och arkiverar händelseloggar för samtliga transaktioner
4. upprätthåller gränserna mellan domäner vid kritiska processer
5. stöder återställning efter systemfel eller nyckelhaveri
6. möjliggör uppdelning av arbetsuppgifter enligt denna policy.

PKI RS CA ska säkerställa att all kommunikation mellan betrodda roller och CA-systemet. Alla servrar som innehåller information om certifikatsstatus (OSCP/CDP) ska:

7. vara konstruerade på ett sätt som gör att varje enskild operatör kan identifieras och autentiseras unikt innan åtkomst till system och applikationer tillåts
8. begränsa åtkomst för användaren till vad som omfattas av dennes betrodda roll
9. upprätthåller gränserna mellan domäner vid kritiska processer
10. stödja återställning efter systemfel eller nyckelhaveri.

Ett CMS (Certificate Management System) ska kunna tillhandahålla följande säkerhetsfunktioner

11. varje användare skall identifieras och autentiseras unikt innan åtkomst till system och applikationer tillåts
12. åtkomst för användaren ska var begränsad till vad som omfattas av dennes betrodda roll
13. generera och arkivera händelseloggar för samtliga transaktioner
14. upprätthåller gränserna mellan domäner vid kritiska processer
15. Stöder återställning efter systemfel eller nyckelhaveri.

Program- och hårdvarufunktioner som inte används av CA eller RA ska avaktiveras.

6.5.2 Klassning av säkerhet för datorer

Inga krav stipuleras.

6.6 Säkerhetskontroller genom livscykeln

6.6.1 Systemutvecklingskontroller

All hård- och mjukvara som upphandlas för att sköta driften av CA-systemet ska granskas i syfte att så långt det är möjligt försäkra sig om att inga ingående komponenter skall vara möjliga att manipulera. Den utrustning som ska användas i CA-systemet ska vara utvecklad i en kontrollerad miljö och under strikt kontrollerade processer. Leverantörer ska använda ett kontrollerat och väl dokumenterat kvalitetsledningssystem.

Mjukvara för CA och RA ska ha stöd för minst ett av dess protokoll:

- Certificate Management Protocol (CMP) [RFC 4210],
- Enrollment over Secure Transport (EST) [RFC 7030]
- Certificate Management Using Cryptographic Message Syntax (CMC); se [RFC 5272].

Spårbarhet ska finnas så att det går att kontrollera att den utrustning som används i produktionsmiljön har transporterats från leverantören under kontrollerade former och att ingen obehörigen haft tillgång till utrustningen. De system som används för utfärdande skall inte ha någon hård- eller mjukvara installerad som inte ingår i konfigurationen för utfärdande CA.

6.6.2 Kontroller för systemadministration

Mjukvara för CA och RA ska löpande verifieras för att garantera dess integritet. CA, och i förekommande fall RA, ska ha rutiner för att styra och övervaka konfigurationen av CA- och RA-system. Handböcker och dokumentation som i detalj anger hur roller och behörigheter förs ska upprätthållas av CA och löpande granskas av SF.

6.6.3 Säkerhetskontrollernas livscykel

Inga krav stipuleras.

6.7 Nätverkssäkerhet

Vital infrastruktur för CA- och RA-funktioner ska vara säkrade för att hindra obehörig åtkomst, manipulation, och överbelastningsattacker. Kommunikation av känslig information ska skyddas med kryptografiska metoder som är minst i nivå med CA-systemets metoder.

6.8 Tidsstämpling

Certifikat, CRL, loggar etc. ska innehålla tid och datum direkt spårbar till UTC(SP). Tidsinformation behöver inte vara kryptografiskt säkerställd med tidsstämplar.

7 Certifikat, CRL och OCSP profiler

7.1 Certifikatsprofil

Alla certifikat som utfärdats inom PKI RS med hänvisning till denna policy ska följa de certifikatprofiler som beskrivs i Bilaga "Certifikatsprofiler PKI RS" Dessa certifikatsprofiler underhålls av SF.

7.2 CRL-profil

Spärrlistan ska följa RFC3280/5280 där de mest grundläggande fälten och värden specificeras nedan.

Fält	Värde
Version (Version)	X509v2
Utfärdare (Issuer)	Den CA som har utfärdat och signerat CRL.
Startdatum (Effective Date)	Utgivningsdatum för CRL.
Nästa uppdatering (Next Update)	Det datum då nästa CRL ska ges ut
Signeringsalgoritm (Signature Algorithm)	sha-512WithRSAEncryption
Återkallade Certifikat (Revoked Certificates)	Lista med återkallade certifikat. Innehåller serienummer på det återkallade certifikatet och datumet för återkallande.

7.2.1 Versionsnummer

Endast X.509 v2 CRL:er utfärdas.

7.2.2 CRL och tillägg till CRL

Inga krav stipuleras.

7.3 OCSP-profil

OCSP tjänsten följer specifikationerna enligt RFC2560.

8 Revision av efterlevnad och andra bedömningar

8.1 Revisionens omfattning

Inga krav stipuleras.

8.2 Frekvens och omständigheter för utvärdering

Revision av PKI-ramverket ska under en treårsperiod vara föremål för internrevision.

8.3 Identitet och krav på kvalifikation för revisor

Inga krav stipuleras.

8.4 Revisors relation till reviderad enhet

Revisionen ska utföras av oberoende intern eller externt anlitad kontrollfunktion.

8.5 Åtgärd vi upptäckt av brist

SF ansvarar för att upprätta åtgärdsplaner som resultat av revisionsrapporten och tillse att bristerna åtgärdas.

8.6 Behöriga att ta del av revisionsrapport

Revisionsrapporten, med undantag för detaljerade uppgifter som kan äventyra säkerheten i PKI RS, kan efter begäran delges deltagarna i PKI RS.

9 Frågor samt övrigt

9.1 Avgifter

9.1.1 Avgifter för utfärdande eller förnyelse av certifikat

Inga krav stipuleras.

9.1.2 Avgifter för tillgång till certifikat

Inga krav stipuleras.

9.1.3 Avgifter för spärr eller tillgång till statusinformation

Inga krav stipuleras.

9.1.4 Avgift för annan service

Inga krav stipuleras.

9.1.5 Riktlinjer för återbetalning

Inga krav stipuleras.

9.2 Finansiellt ansvar

9.2.1 Försäkringar

Region Stockholm ska upprätthålla en rimlig nivå av försäkringsskydd för fel och försummelser.

9.2.2 Andra tillgångar

Region Stockholm ska ha tillräckliga finansiella resurser för att upprätthålla sin verksamhet och utföra sina arbetsuppgifter och de måste även kunna hantera risken för ansvar mot innehavare och förlitande parter.

9.2.3 Försäkring eller garanti till innehavare

Inga krav stipuleras.

9.3 Sekretess för myndighetsinformation

Information hänförlig till certifikat, spärrlistor, mm som förvaras hos en myndighet eller för myndighetens räkning är ofta att anse som allmän handling. Enligt den i 2 kap. tryckfrihetsförordningen beskrivna offentlighetsprincipen har allmänheten rätt att ta del av allmänna handlingar som inte är sekretesskyddade enligt offentlighet- och sekretesslagen (2009:400). Allmän handling som är offentlig kommer att tillhandahållas av Region Stockholm till den som begär det på stället eller lämnas ut i form av utskrift. Offentlighetsprincipen ger inte allmänheten rätt att ta del av allmän handling på något annat sätt, såsom via egen terminal, filöverföring eller datamedia. Detta avsnitt reglerar information som omfattas av sekretess. Med detta begrepp avses information som inte rutinmässigt ska spridas till allmänheten. Om informationen omfattas av sekretess lämnas den inte ut av Region Stockholms. Beslut härom kan dock överklagas och handlingen kan därför komma att lämnas ut efter beslut av domstol.

9.3.1 Typ av information som omfattas av sekretess

Uppgifter som rör utfärdandet av certifikat och användning av PKI RS, som inte undantas i avsnitt 9.3.2 eller som på annat sätt definieras som publik i denna certifikatpolicy, anses vara konfidentiella och kommer inte att lämnas ut utan samtycke av certifikatinnehavaren eller annan berörd avtalspart, såvida inte utlämnande ska ske enligt vad som är föreskrivet i lag.
Loggar kommer inte att göras tillgängliga av Region Stockholms i sin helhet, om inte annat följer av lag eller författning eller domstol eller annan myndighets beslut.

9.3.2 Typ av information som inte omfattas av sekretess

För att tillgodose funktionen av Region Stockholms verksamhet såsom CA anses inte följande uppgifter som sekretesskyddade:

- certifikat, inklusive publika nycklar
- uppgift om spärr
- redovisning av revision utom vad som specificeras under punkt 8.6
- denna policy och tillhörande CPS
- allmänna villkor för certifikatinnehavare

9.4 Persondataskydd

9.4.1 Sekretess

CA ska tillämpa sekretess för att inte röja namn på ansökande av certifikat eller annan identifierande information om dem, utom den information som listas i avsnitt 9.3.2. I övrigt hanteras personuppgifter enligt Region Stockholms principer for hantering av personuppgifter. (Se bilaga 2)

9.4.2 Information som ska behandlas som privat

PKI RS behandlar all persondata som inte görs offentligt, genom att innehållet i certifikatet publiceras, som privat och därmed sekretessbelagd.

9.4.3 Information som inte klassas som privat

Certifikat, spärrlistor och den information som finns i dessa är att betrakta som harmlös information och klassas därför inte som privat.

9.4.4 Ansvar att skydda persondata

Deltagare i PKI RS ska skydda persondata i enlighet med denna certifikatpolicy.

9.4.5 Samtycke till hantering av personuppgifter.

Hantering av persondata kräver samtycke av den som informationen avser.

9.4.6 Tillhandahållande av sekretessbelagd information till Polis, åklagare eller annan

Av tryckfrihetsförordningens bestämmelser om den s.k. offentlighetsprincipen följer att en myndighet, i detta fall Region Stockholm, är skyldig att lämna ut allmänna offentliga handlingar till den som begär det. Vidare kan myndigheten vara skyldig att lämna ut uppgifter som omfattas av sekretess till polis och åklagare. Vägrar myndigheten att lämna ut allmänna handlingar, t.ex. på grund av sekretess, kan frågan komma att avgöras av domstol.

Privata nycklar kopplade till utfärdade certifikat kan dock inte tillhandahållas av Region Stockholm efter domstolsbeslut, eftersom certifikatinnehavares privata nycklar enligt denna certifikatpolicy inte får finnas sparade hos Region Stockholm eller någon av dess underleverantörer.

9.4.7 Andra omständigheter för utlämnande av information

Inga krav stipuleras.

9.5 Immateriella rättigheter

Inga krav stipuleras.

9.6 Rättsligt företrädande och garantier

9.6.1 Garantiutfästelser från CA

- att det inte finns väsentliga felaktigheter i uppgifterna i certifikatet som känns till av eller härrör från part som godkänt eller publicerat certifikatet
- att det inte finns några fel i certifikatet som orsakats av part som godkänt eller utfärdat certifikatet, som ett resultat av att inte ha hanterat ansökan eller utfärdat certifikatet med rimlig aktsamhet
- att certifikatet uppfyller alla väsentliga krav i denna certifikatpolicy.

9.6.2 Garantiutfästelser från RA:

RA garanterar:

- att det inte finns väsentliga felaktigheter i uppgifterna i certifikatet som känns till av eller härrör från part som godkänt eller publicerat certifikatet
- att det inte finns några fel i certifikatet som orsakats av part som godkänt eller utfärdat certifikatet, som ett resultat av att inte ha hanterat ansökan eller utfärdat certifikatet med rimlig aktsamhet
- att certifikatet uppfyller alla väsentliga krav i denna certifikatpolicy.

9.6.3 Garantiutfästelser från innehavare

Innehavaren av certifikatet förbinder sig att:

- skydda den privata nyckeln så att den inte blir känd för någon obehörig
- se till att förse PKI RS med korrekt och fullständig information
- verifiera att informationen i certifikatet är korrekt innan det används
- omgående upphöra med all användning av certifikatet om:
    - någon väsentlig information som lämnades till PKI RS eller som finns i certifikatet förändras eller blir missvisande
    - det har konstaterats eller kan misstänkas att certifikatet obehörigen använts eller att den privata nyckeln som är kopplad till certifikatet blivit känd av annan person
- endast använda certifikatet för ändamål som är lagliga och godkända enligt denna policy
- följa reglerna enligt denna policy vid beställning och användande av certifikat
- omgående upphöra med användning av certifikatet och den kopplade privata nyckeln efter att certifikatets giltighetstid upphört.

9.6.4 Garantier förlitande part

Förlitande parter garanterar:

- att de har tillräcklig information för att fatta ett välgrundat beslut om i vilken utsträckning de väljer att förlita sig på informationen i ett certifikat
- det egna ansvaret för att avgöra om de vill förlita sig på sådan information
- att de skall bära de rättsliga konsekvenserna av deras misslyckande att uppfylla alla väsentliga krav i denna certifikatpolicy.

9.6.5 Garantier för övriga parter

Inga krav stipuleras.

9.7 Fullmaktsförhållanden

Utfärdande av certifikat i enlighet med den åberopade certifikatpolicyn och denna policy medför inte att Region Stockholm, såsom CA, skall betraktas som agent, fullmäktig eller på annat sätt som representant för certifikatinnehavare eller förlitande part.

9.8 Ansvarsbegränsning

Inga krav stipuleras.

9.9 Ekonomisk kompensation och ersättningar

Inga krav stipuleras.

9.10 Villkor och upphävande

9.10.1 Villkor

Denna certifikatpolicy träder i kraft vid publicering i enlighet med punkt 2.1 i denna certifikatpolicy. Ändringar i denna certifikatpolicy träder i kraft vid publicering av ny version i enlighet med punkt 2.1 i denna certifikatpolicy.

9.10.2 Upphävande

Denna certifikatpolicy, som kan ändras över tid, ska vara giltig tills den ersatts av en ny version.

9.10.3 Effekt av uppsägning och vidarelevnad

Vid upphävande av denna certifikatpolicy är alla deltagare ändå bundna av dessa villkor för återstoden av giltighetstiderna för certifikaten.

9.11 Kommunikation mellan deltagare

Om inte annat avtalats ska deltagarna använda kommersiellt rimliga metoder för att kommunicera med varandra, med beaktande av ämnet för kommunikationen.

9.12 Ändringar

9.12.1 Förfarande för ändring

Ändringar i denna certifikatpolicy kan bara göras av SF efter godkännande av systemägare PKI - RS inom SF i samråd med SF Informationssäkerhetssamordnare. Ändringar ska antingen vara i form av ett dokument som innehåller en ändrad form av certifikatpolicy eller en uppdatering. Uppdateringar ersätter eventuella utpekade eller motstridiga bestämmelser i den refererade versionen av certifikatpolicyn.

9.12.2 Information om ändring

SF förbehåller sig rätten att göra smärre förändringar av certifikatpolicyn utan förvarning. Beslutet om vad som räknas till smärre förändring ligger helt hos SF. Vid större förändringar ska SF i god tid innan meddela CA, och i förekommande fall RA, om förändringarna. Förslaget till förändringarna ska också publiceras i enlighet med denna certifikatpolicy.

SF förbehåller sig även rätten att göra större förändringar av certifikatpolicyn utan förvarning för att stoppa eller förhindra ett brott mot säkerheten för PKI RS. Sådana ändringar trader i kraft omedelbart efter publiceringen. SF ska skyndsamt meddelas CA, och i förekommande fall RA, om dessa förändringar.

9.12.3 Omständighet under vilka OID måste ändras

Om SF fastställer att en ändring är nödvändig i OID som motsvarar en certifikatpolicy, ska ändringen innehålla nya OID för certifikatpolicyn. Annars ska ändringar inte kräva en förändring av certifikatpolicyns OID.

9.13 Procedur för konfliktlösning

Uppkommer tvist angående tolkning eller tillämpning av denna certifikatspolicy och parterna inte kan komma överens, ska tvisten avgöras genom skiljedom enligt svensk rätt.

9.14 Tillämpliga lagar

Svensk lag utan tillämpning av dess lagvalsregler ska gälla för tolkningen av detta avtal.

9.15 Efterlevnad av tillämpliga lagar

Svensk lag ska efterlevas.

9.16 Bilaga 1 - Definitioner och förkortningar

Definition	Förkortning	Betydelse
Qualified Signature Creation Device	QSCD	Hårdvarutoken som kan lagra privata nycklar på ett säkert sätt men bl.a. skydd i form av PIN
Certifikatutfärdare	CA	Certification Authority – en som utfärdar digitala certifikat enligt ett regelverk
CA certifikat		Ett certifikat som innehåller information om CA och som signerar användarcertifikat
Kryptografisk Hårdvarumodul	HSM	Av Hardware Security Module. Hårdvara som används för att kryptera, dekryptera, skapa och lagra krypteringsnycklar
HSM		Se ”Kryptografisk Hårdvarumodul”
Lagvalsregler		Regler som fastställer vilket lands regler som skall tillämpas i ett visst rättsförhållande.

9.17 Bilaga 2 – Referenser

Behandling av anställdas personuppgifter	Vid frågor om behandling av personuppgifter, kontakta PKI RS-förvaltning Mail: pki-rs.sf@regionstockholm.se
Informationshantering vid rekrytering, anställning och avslut av anställning	Vid frågor om Informationshantering vid rekrytering, anställning och avslut av anställning, kontakta PKI RS-förvaltning Mail: pki-rs.sf@regionstockholm.se