VGR CPS

Västra Götalandsregionens Certificate Practice Statement intern PKI

Kontaktperson: Mikael Cavrak

OID för policy: 1.2.752.113.10.1.1.1.1

1 Dokumentinformation

Datum	Författare	Version	Kommentar
101001	Conny Balazs, KnowIT Fredrik Rasmusson, Västra Götalandsregionen		
101220	Valter Lindström Monika Göransson Fredrik Rasmusson		
110308	Mikael Cavrak Fredrik Rasmusson		
120209	Fredrik Rasmusson Mikael Cavrak Magnus Svensson	1.0	

Innehållsförteckning

1 Dokumentinformation 2
2 Inledning 5
3 Kontaktuppgifter 5
4 Certificate Practice Statement 6
5 Certificate Policies 7
6 Identifikation 7
7 Användarparter och applicering av CPS 8
8 Certification Authorities 9
8.1 Root CA 9
8.2 Issuing CAs 9
Registration Authority 10
9 ”End Entities” 12
10 Applicering av CPS 12
11 Ansvarsfördelning 13
11.1 ”Policy Authority” 13
11.2 Driftleverantör av CA-system 13
11.3 ”Certification Authority” 13
11.4 ”Registration Authority” 13
11.5 ”Subscriber” 14
11.6 ”Relying Party” 14
11.7 ”Repository” 15
12 Legala förbindelser 16
13 Konfidentialitet 17
13.1 Typ av information som ska hållas konfidentiell 17
13.2 Typ av information som ej betraktas som konfidentiell 17
14 Rättigheter till intellektuellt kapital 18
15 Identifiering och autentisering 19
15.1 Namn 19
15.2 Method för att bevisa innehav av privat nyckel 19
15.3 Autentisering 19
15.4 Rutinmässig “rekey” 19
15.5 “Rekey” efter tillbakadragning av certifikat 19
15.6 Förnyelser av certifikat 19
15.7 “Revocation request” 19
16 Operationella krav 20
16.1 Certifikatansökningar 20
16.2 Certifikatutfärdning 20
16.3 Certifikatacceptans 20
16.4 Certifikat ”suspension” och ”revocation” 20
16.5 Skäl för ”revocation” 20
16.6 Parter som kan efterfråga ”revocation” 20
16.7 Procedur vid efterfrågning av ”revocation” 21
16.8 ”Revocation request grace period” 21

16.9 ”CRL checking” 21
16.10 CRL uppdateringsfrekvens 21
16.11 Krav på ”CRL checking” 22
16.12 ”On-line revocation/status checking” 22
16.13 Krav på ”On-line revocation checking” 22
16.14 Övriga former av ”revocation checking” 22
16.15 Krav på övriga former av ”revocation checking” 22
16.16 Speciella krav gällande ”key compromise” 22
17 Loggning av säkerhetsrelaterade händelser 23
17.1 Typer av händelser som loggas 23
17.2 Frekvens på genomgång av loggar 23
17.3 Sparande av loggar 23
17.4 Skydd av loggar 23
17.5 Loggarkivering 23
17.6 ”Audit collection system” 23
17.7 Eventhanteringssystem och rutiner 24
17.8 Krav på tidsangivelser 24
17.9 ”Key Changeover” 24
17.10 Disaster Recovery 24
17.11 CA Terminering 24
18 Fysiska säkerhetsåtgärder 25
18.1 Fysisk åtkomst 25
18.2 Avfallshantering 25
18.3 Administrativa roller 25
18.4 Uppgifter som kräver mer än en persons inblandning 25
18.5 Krav på autentisering för varje roll 25
18.6 Utfärdande av roller 25
18.7 Utbildningskrav på personal 26
18.8 Frekvens på utbildningsrepetition 26
18.9 Sanktioner för otillbörligt handlande 26
18.10 Krav som ställs på utomstående kontrakterad personal 26
18.11 Generering och lagring av nycklar 26
18.12 CA Policys 26
18.13 Förändringshantering av CA policy samt CPS 27

2 Inledning

Västra Götalandsregionens interna PKI-lösning används för att tillhandahålla certifikat åt interna tillämpningar som kräver detta.

Då en organisation implementerar en PKI-lösning, skall ägaren av lösningen (”Policy Authority”) publicera en CA policy (CP), ”Registration Authority Policy”, ett eller flera ”Registration Authority Practice Statements” samt ett eller flera ”Certificate Practice statements” (CPS). CP beskriver kraven för drift av PKI-lösningen, hur certifikat delas ut samt ”lifetime management” av dessa certifikat. CPS:er beskriver hur CP praktiskt implementeras av respektive ”Certification Authority” (CA).

Ovanstående dokument används så att en användare av PKI-lösningen kan förstå ansvarsfördelning samt vilken nivå av tillit man kan etablera mot certifikat som delas ut av aktuell PKI-lösning.

Frågor gällande detta CPS skall riktas till VGR IT inom Västra Götalandsregionen.

3 Kontaktuppgifter

Detta CPS ägs av Västra Götalandsregionen.

4 Certificate Practice Statement

Detta”Certificate Practice Statement” (CPS) följer de standarder som specificeras av Internet Engineering Task Force (IETF) i RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

Detta dokument förutsätter att läsaren är insatt i koncepten kring PKI. Samtliga komponenter i RFC 2527 är medtagna i detta dokument för att förenkla eventuella jämförelser och policy mappningar i framtiden. De komponenter som är markerade med ”ingen policy” indikerar att ett medvetet beslut tagits att exkludera policykomponenten.

Detta CPS beskriver förhållningssätt, standarder och rutiner som appliceras på samtliga ”Certification Authorities” i Västra Götalandsregionens interna PKI-lösning. Detta CPS appliceras på samtliga parter som på något sätt har ett förhållande till regionens interna PKI-lösning, inklusive ”Certification Authorities”, ”Subscribers”, och ”Relying Parties”.

5 Certificate Policies

En CA utfärdar ett signerat certifikat för att binda en publik nyckel till en viss part; dator eller person. Enligt X.509-koncepten är en CA policy en samling strukturerade regler som indikerar grundläggande förutsättningar för certifikatanvändning. En CA policy kan användas av en certifikatanvändare eller en ”Relying Party” för att kunna besluta huruvida ett certifikat och dess bidning till en part är tillräckligt tillförlitlig för ett visst syfte eller en viss tillämpning.

6 Identifikation

Detta dokument refereras formellt som “Västra Götalandsregionens interna PKI Certificate Practice Statement”.

7 Användarparter och applicering av CPS

Västra Götalandsregionens interna PKI-hierarki har etablerats för att tillhandahålla certifikattjänster inom den egna verksamheten. CA policies" (CP:s) definierar i detalj vilka specifika parter som har behörigheter att ansöka om olika certifikat samt vilka ämnade syften dessa certifikat har. De element som uttrycks i detta CPS skall ej vara motsägelsefulla mot någon implementerad CA policy.

Uppdragstagaren för drift av VGRs interna PKI-hierarki åtar sig att på kvartalsbasis utföra revision för att säkerställa att detta CPS är till fullo implementerat samt att påvisa eventuella avvikelser. Dessa revisionsrapporter skall publiceras till VGRs Policy Authority samt ISSO. VGRs Policy Authority har i tillämpliga fall ansvar för att informera "Relying Parties" gällande avvikelser från detta CPS. VGRs Policy Authority samt ISSO har även mandat att vid givet tillfälle begära revisionsrapport. Säkerhetsdirektören för VGR har alltid mandat att begära och ta del av revionsrapport.

8 Certification Authorities

”Certification Authorities” (CAs) är enheter som är auktoriserade att utföra följande generella funktioner:

- Skapa och signera certifikat
- Distribuera certifikat till lämpliga ”Subscribers” och ”Relying Parties”
- Dra tillbaka utfärdade certifikat
- Distribuera certifikatstatus i form av ”Certificate Revocation Lists” (CRLs) eller andra mekanismer
- Tillhandahålla och peka ut platser där certifikat och certifikatstatus finns tillgänglig

Inom Västra Götalandsregionens interna PKI finns två typer av CA:s, en Root CA samt flera issuing CAs.

8.1 Root CA

CA Namn	Beskrivning av funktion
VGR Root CA	Root CA som fungerar som “trust anchor” för Västra Götalandsregionens interna PKI

8.2 Issuing CAs

CA Namn	Beskrivning av funktion
VGR Issuing CA 1	Issuing CA för Västra Götalandsregionen.
VGR Issuing CA 2	Issuing CA för Västra Götalandsregionen.

Registration Authority

Issuing CAs utför de mest grundläggande certifikatregistreringsfunktionerna, exempelvis utvärdera och antingen godkänna eller neka “Subscriber certificate management transactions” (certifikatansökan, förnyelser av certifika och nycklar samt “revocation requests”). Beronde på vilken “Certificate Policy” som appliceras kan en “Registration Authority” samla in och verifiera “Subscriber information” (exempelvis identitet, position eller roll) som ska stämplas in i aktuellt certifikat. Västra Götalandsregionens interna PKI-hierarki stödjer både automatiska och manuella registreringsfunktioner.

Då en automatisk registreringsfunktion implementeras, appliceras regler i enlighet med gällande CA policy för att automatiskt godkänna eller neka aktuell ”Subscriber certificate management transaction”.

Då en icke automatiserad registreringsfunktion krävs, godkänns eller nekas aktuell ”Subscriber certificate management transaction” i enlighet med gällande CA policy.

Registreringsfunktioner för samtliga CA:s i Västra Götalandsregionens interna PKI följer nedan:

CA Namn	**Beskrivning av registreringsfunktion**
VGR Root CA (Windows RootCA)	Manuell registreingsfunktion. Västra Götalandsregionens interna RA-organisation är implementerad av denna CA.
VGR Issuing CA 1 (Windows Issuing CA)	Automatiserad registreringsfunktion baserad på autentisering av användare mot konton i Västra Götalandsregionens regionala Active Directory. Västra Götalandsregionens interna RA-organisation är implementerad av denna CA. För certfikat utpekade av Västra Götalandsregionens ”Policy Authority” kan alternativa registreringsfunktioner användas, i enlighet med gällande CA policy. T.ex. Manuell registreringsfunktion baserad på autentisering av användare mot konton i Västra Götalandsregionens regionala Active Directory.
VGR Issuing CA 2 (Windows Issuing CA)	Automatiserad registreringsfunktion baserad på autentisering av användare mot konton i Västra Götalandsregionens regionala Active Directory. Västra Götalandsregionens interna RA-organisation är implementerad av denna CA. För certfikat utpekade av Västra Götalandsregionens ”Policy Authority” kan alternativa registreringsfunktioner användas, i enlighet med gällande CA policy. T.ex. Manuell registreringsfunktion baserad på autentisering av användare mot konton i Västra

CA Namn	Beskrivning av registreringsfunktion
	Götalandsregionens regionala Active Directory.

9 ”End Entities”

“End entities” inkluderar “subscribers” och “relying parties”. En “subscriber” är en part vars namn eller identitet finns stämplat i subjectattributet på ett certifikat och som använder sina nycklar i enlighet med detta CPS (samt aktuella CP:s).

En “relying party” är en part som litar på certifikat som Västra Götalandsregionens interna PKI utfärdar (i olika syften). “Relying parties” inkluderar varje part som litar på ett eller flera certifikat ur Västra Götalandsregionens interna PKI.

10 Applicering av CPS

Detta CPS appliceras på samtliga certifikat som utfärdas av en CA inom Västra Götalandsregionens interna PKI-hierarki. CA policies definierar vilka parter som har tillgång till olika certifikat, hur dessa certifikat tilldelas samt vilka ”intended purposes” och användningsområden dessa certifikat har.

11 Ansvarsfördelning

11.1 ”Policy Authority”

Följande ansvar ligger på Västra Götalandsregionens ”Policy Authority”:

- Skapa, underhålla och godkänna samtliga CA policys samt godkänna samtliga CPS.
- Distribuera och informera om CA policys
- Tolka huruvida policys efterföljs
- Specificering av innehållet i utdelade certfikat
- Hantering av konflikter som är ett resultat av innehållet i CA policys
- Hålla sig uppdaterad gällande säkerhetshot och att föregripa hot som bedöms vara aktuella för Västra Götalandsregionens interna PKI
- Säkerställa att samtliga operatörer som hanterar någon del i Västra Götalandsregionens interna PKI har rätt utbildningsnivå

11.2 Driftleverantör av CA-system

Följande ansvar ligger på driftleverantören av CA-systemet för Västra Götalandsregionen:

- Skapa och underhålla samtliga CPS samt lämna in dessa för godkännande
- All form av systemdrift av CA-systemet
- Hålla sig uppdaterad gällande säkerhetshot och att föregripa hot som bedöms vara aktuella för Västra Götalandsregionens interna PKI
- Säkerställa att samtliga operatörer som hanterar någon del i Västra Götalandsregionens interna PKI har rätt utbildningsnivå

11.3 ”Certification Authority”

Följande ansvar ligger på Västra Götalandsregionens CAs:

- Implementera samtliga policys och riktlinjer som beskrivs i aktuella ”Certificate Practice Statements” samt CA policys
- Distribuera sin(a) publika nyckel/nycklar
- Generera, utfärda och distribuera certifikat
- Generera information för certifikatstatus (exempelvis CRLer)
- Upprätthålla säkerhet och tillgänglighet för sina funktioner
- Tillhandahålla möjligheter för ”subscribers” att efterfråga certifikatstatus
- Dra tillbaka certifikat
- Inneha ägarskap och kontroll över all operativ historik

11.4 ”Registration Authority”

Följande ansvar ligger på Västra Götalandsregionens interna RA:

- Identifiera och autentisera ”subscribers” enligt följande:
  - Verifiering av att identifierande data som aktuell ”subscriber” tillhandahåller är giltig.
  - Att verifiering sker med hjälp av giltig legitimation då så krävs enligt SPC 151
  - Verifiering av att aktuell ”subscriber” får ansöka om aktuellt certifikat
  - Verifikation av organisationens godkännande av beställning
  - Hantering av bindning mellan ”subscriber” identifieringsdata och publik nyckel för ”subscriber” (för personcertifikats nyttjande av e-legitimation)
  - Mottaga och hantera spärrbegäran (”certificate revocation requests”)
- Ta emot publik nyckel från aktuell ”subscriber” eller generera ett asymmetriskt nyckelpar åt aktuell ”subscriber”

11.5 ”Subscriber”

Följande ansvar ligger på ”subscribers” mot Västra Götalandsregionens interna PKI:

- Ta del av och godkänna innehållet i detta CPS
- Att inte modifiera något certifikat som lyder under detta CPS
- Tillhandahålla korrekta publika nycklar och korrekt användaridentitet vid registrering
- Tillhandahålla information åt aktuell ”issuing CA” som är korrekt och komplett
- Vidta lämpliga säkerhetsåtgärder för att skydda sina privata nycklar
- Att omedelbart rapportera förlust eller stöld av privata nycklar till aktuell RA-funktion
- Att omedelbart rapportera felaktig information som finns i certifikat till RA-funktion
- Att använda sina nyckelpar endast i samråd med gällande bestämmelser och policys

11.6 ”Relying Party”

Följande ansvar ligger på ”relying parties” mot Västra Götalandsregionens interna PKI:

- Ta del av och godkänna innehållet i detta CPS
- Bekräfta giltigheten av certifikat utfärdade av Västra Götalandsregionens interna PKI genom att använda procedurer enligt X.509 standarder
- Verifiera att ”subscriber” innehar asymmetrisk privat nyckel som är kopplad till certifikatets publika nyckel
- Att endast använda publika nycklar i ”subscriber” certifikat för godkända tillämpningar

Föregående lista är inte en definitiv lista över steg en ”relying party” bör ta för att bestämma sig huruvida ett visst certifikat skall betraktas som tillförlitligt eller ej. Varje ”relying party” är ansvarig för att besluta, enligt dennas gällande policys, när och till vilken grad ett visst certifikat skall betraktas som tillförlitligt. Detta ”Certificate Practice Statement” ska assistera en ”relying party” att utvärdera vilken nivå av tillförlitlighet man vill implementera mot ett visst certifikat från Västra Götalandsregionens interna PKI. Om en ”relying party” ej uppfyller samtliga sina åtaganden i detta dokument tar Västra Götalandsregionen inget ansvar för möjliga konsekvenser.

11.7 ”Repository”

Västra Götalandsregionens interna PKI-hierarki och dess CA:s skall tillhandahålla ”repository services” för att uppfylla följande funktioner:

- Lagra och distribuera certifikat
- Lagra och distribuera certifikatstatus (exempelvis CRLer)
- Lagra och distribuera publik PKI information
- Lagra och tillhandahålla korrekta ”certificate templates” åt ”subscribers”

Inom VGR används VGR AD som ”repository” för den interna PKI-hierarkin. Det är enligt gällande CA policy ej tillåtet att arkivera privata nycklar i ”repositoryt”.

12 Legala förbindelser

Västra Götalandsregionens interna PKI lämnar inga garantier eller löften mot ”subscribers” eller ”relying parties” förutom det som beskrivs i detta ”Certificate Practice Statement”. Vidare avsäger sig Västra Götalandsregionen legalt ansvar för eventuellt uppkomna fel i tjänster som levereras av en individuell CA.

Eventuella förluster som en ”subscriber” eller ”relying party” skulle lida, genom användandet av certifikat från Västra Götalandsregionens interna PKI, avsäger sig Västra Götalandsregionen ansvar för.

13 Konfidentialitet

13.1 Typ av information som ska hållas konfidentiell

Följande information betraktas av Västra Götalandsregionen som konfidentiell och lämnas inte ut till "subscribers" eller "relying parties":

- Västra Götalandsregionens interna PKI-hierarkis driftprocedurer och teknisk dokumentation
- ”Subscriber” registreringsrecords enligt följande:
  - Certifikatansökningar, oavsett om de är godkända eller nekade
  - Detaljer angående hur autentisering hanteras
  - Certifikatinformation som samlas in under certifikatansökningar vid sidan av den information som inkluderas i ”subscriber”-certifikat
- Skälet till tillbakadragning av certifikat, med undantag för certifikat som dras tillbaka av följande skäl:
  - ”Key compromise” av privat nyckel för en ”Certificate Authority”, i sådana fall måste relevanta ”relying parties” och ”subscribers” meddelas detta
  - Avveckling av en ”Certificate Authority”, i sådana fall skall berörda parter informeras om detta i förväg
- Logginformation
- Privata nycklar

13.2 Typ av information som ej betraktas som konfidentiell

Västra Götalandsregionens interna PKI-hierarki kan publicera certifikatinformation (information som finns i ett individuellt certifikat), CRLer relaterade till Västra Götalandsregionens interna PKI-hierarki samt CA certifikat till ett eller flera ”repositorys” som tillhandahåller läsbar tillgång till dessa data.

Följande information skall ej heller behandlas som konfidentiell:

- Information som redan innehas av en "subscriber" eller "relying party" skall ej betraktas som konfidentiell
- Information som mottagande part i god tro fått från tredje part som äger aktuell information skall ej betraktas som konfidentiell
- Information som är publikt tillgänglig, utan att bryta mot detta CPS, vid mottagandet av informationen skall ej betraktas som konfidentiell

14 Rättigheter till intellektuellt kapital

Intellektuellt kapital associerat med följande områden tillhör Västra Götalandsregionen:

- Detta ”Certificate Practice Statement”
- Samtliga CA policys som är associerade med Västra Götalandsregionens interna PKI-hierarki
- Policys och rutiner för drift av Västra Götalandsregionens interna PKI-hierarki
- Certifikat och CRLs utfärdade av CAs inom Västra Götalandsregionens interna PKI-hierarki
- Namn som används för att identifiera enheter inom Västra Götalandsregionens interna PKI-hierarki
- CAs, infrastruktur och ”subscriber” nyckelpar
- Smart card och läsare utfärdade åt ”subscribers”

15 Identifiering och autentisering

15.1 Namn

"Subject Name" samt "Distinguished Name" för alla certifikat skall följa aktuell CA policy och representeras som en enda sträng.

15.2 Method för att bevisa innehav av privat nyckel

Då en "subscriber" genererar nyckelpar måste aktuell certifikatförfrågan innehålla aktuell publik nyckel. Då en "Issuing CA" genererar nyckelpar skall aktuell CA tillhandahålla nycklar till aktuell certifikatförfrågan.

15.3 Autentisering

Autentisering av samtliga certifikatförfrågningar skall ske i samråd med aktuell CA policy och aktuell "issuance policy".

15.4 Rutinmässig "rekey"

Rutinmässig "rekey" av samtliga certifikat skall ske i samråd med aktuell CA policy.

15.5 "Rekey" efter tillbakadragning av certifikat

Ifall att ett CA-certifikat måste dras tillbaka måste antingen aktuell CA utföra "rekey" eller omedelbart avvecklas.

Rutinen för "rekey" efter "revocation" eller "expiration" av ett "subscriber"-certifikat innebär komplett förfrågan om ett nytt certifikat, vilket kräver generering av nytt nyckelpar i enlighet med aktuell CA policy.

15.6 Förnyelser av certifikat

Förnyelse av CA-certifikat, då ett nytt certifikat med förlängd tidslängd skapas för ett redan existerande nyckelpar stöds i enlighet med aktuell CA policy.

Förnyelser av "subscriber"-certifikat stöds i de fall att aktuell CA policy tillåter detta.

15.7 "Revocation request"

För att ett certifikat skall dras tillbaka krävs ett beslut av Västra Götalandsregionens "Policy Authority" eller av denna utsedda parter med behörigheter att utföra detta. Västra Götalandsregionens "Policy Authority" förbehåller sig rätten att dra tillbaka individuella certifikat enligt gällande CA policy.

16 Operationella krav

16.1 Certifikatansökningar

Innan ett certifikat kan delas ut måste aktuell ”subscriber” erlägga en ansökan om aktuellt certifikat. Alla ansökningar skall ske enligt gällande CA policy.

16.2 Certifikatutfärdning

Certifikat genereras, utfärdas och publiceras endast i enlighet med gällande CA policy. Notera att utfärdning kan ske antingen automatiskt eller manuellt enligt gällande CA policy.

16.3 Certifikatacceptans

Certifikatacceptans innebär följande:

- Att aktuell ”subscriber” förbinder sig till ansvar i enlighet med detta CPS samt gällande CA policy
- Representerar och säkerställer att ingen obehörig part har haft tillgång till den privata nyckeln associerad med aktuellt certifikat
- Att aktuell ”subscriber” har tillhandahållit sanningsenlig och korrekt information under ansökningsprocessen

Då en ”subscriber” tar emot ett certifikat är aktuell ”subscriber” skyldig att verifiera att informationen i aktuellt certifikat är korrekt och komplett samt att certifikatet ej är skadat eller korrupt. I de fall där certifikatet bedöms icke korrekt skall Västra Götalandsregionens ”Registration Authority” kontaktas.

16.4 Certifikat ”suspension” och ”revocation”

Västra Götalandsregionens interna PKI-hierarki stödjer”revocation” av certifikat, ”suspension” stöds ej.

16.5 Skäl för ”revocation”

”Revocation” kan endast ske i enlighet med Västra Götalandsregionens ”Policy Authority” och dess rutiner av följande skäl:

- Aktuell ”subscriber” tappar sin status som giltig ”subscriber” enligt gällande CA policy
- Identifierande information eller attribut i ett ”subscriber”-certifikat ändras innan certifikatet slutar gälla
- Aktuell ”subscriber” bryter mot detta CPS eller gällande CA policy
- Känt eller misstänkt missbruk av privat nyckel för aktuell ”subscriber”
- Känt eller misstänkt missbruk av en CAs privata nyckel
- Övriga fall som Västra Götalandsregionens ”Policy Authority” bedömer som skäl nog att utföra ”revocation”

16.6 Parter som kan efterfråga ”revocation”

Förrutom Västra Götalandsregionens ”Policy Authority”, och av denna utsedda parter, kan en ”subscriber” begära ”revocation” av ett eget certifikat.

16.7 Procedur vid efterfrågning av ”revocation”

Då Västra Götalandsregionens ”Policy Authority”, eller av denna utsedda parter tar emot en förfrågan om ”revocation är man ansvarig för följande:

- Att godkänna/neka förfrågningar
- I de fall som godkänns, utföra ”revocation av aktuellt certifikat
- Dokumentera skäl för godkännande/nekande enligt regelverk som utfärdas av Västra Götalandsregionens RA-funktion.

16.8 ”Revocation request grace period”

Västra Götalandsregionens”Policy Authority”, eller av denna utsedda part, är skyldiga att verifiera och agera på förfrågningar om ”revocation” eller ”suspension” inom tjugofyra timmar från det att förfrågan skickats. Ett specifikt certifikat som genomgått ”revocation” eller ”suspension” skall reflekteras i aktuell CRL som publiceras i den nästkommande schemalagda uppdateringen.

16.9 ”CRL checking”

Aktuella CRLs kommer att publiceras av CA, enligt gällande schema och vara åtkomliga för ”relaying parties” och ”subscribers” via LDAP (VGR AD) och via http:

ldap:///CN=VGC%20Issuing%20CA1,CN=vgca0001,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=vgregion,DC=se?certificateRevocationList?base?objectClass=cRLDistributionPoint

ldap:///CN=VGC%20Issuing%20CA1,CN=vgca0002,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=vgregion,DC=se?certificateRevocationList?base?objectClass=cRLDistributionPoint

http://crl.vgregion.se/VGC%20Issuing%20CA1.crl

http://crl.vgregion.se/VGC%20Issuing%20CA2.crl

16.10 CRL uppdateringsfrekvens

CRL:er för CAs i Västra Götalandsregionens interna PKI-hierarki publiceras enligt följande tabell:

CA Namn	CRL uppdateringsfrekvens
VGR Root CA	2 år
VGR Issuing CA 1	8 dagar för baseline, 2 timmar för delta
VGR Issuing CA 2	8 dagar för baseline, 2 timmar för delta

16.11 Krav på ”CRL checking”

”Relying parties” och ”subscribers” skall verifiera ett certifikats status genom att undersöka aktuell CRL, alternativt aktuell OCSP provider, innan ett specifikt certifikat betraktas som tillförlitligt. Västra Götalandsregionen tar inget ansvar för situationer som kan uppkomma då en ”subscriber” eller ”relying party” ej verifierar status på ett certifikat via gällande CRL eller om man väljer att lita på ett utgånget eller tillbakadraget certifikat.

16.12 ”On-line revocation/status checking”

”Relaying parties” och ”subscribers” som stödjer OCSP kan utföra revocation/status checking via en OCSP responder som tillhandahålls av CA.

16.13 Krav på ”On-line revocation checking”

”Relying parties” och ”subscribers” skall verifiera ett certifikats status genom att undersöka aktuell OCSP responder, alternativt aktuell CRL, innan ett specifikt certifikat betraktas som tillförlitligt. Västra Götalandsregionen tar inget ansvar för situationer som kan uppkomma då en ”subscriber” eller ”relying party” ej verifierar status på ett certifikat via gällande OCSP responder eller om man väljer att lita på ett utgånget eller tillbakadraget certifikat.

16.14 Övriga former av ”revocation checking”

Ingen policy.

16.15 Krav på övriga former av ”revocation checking”

Ingen policy.

16.16 Speciella krav gällande ”key compromise”

Västra Götalandsregionens ”Policy Authority” skall använda kommersiellt lämpliga och tillämpningsbara ansträngningar för att notifiera samtliga ”relying parties” vilka är berörda om man finner att en CAs privata nyckel blivit utsatt för ”key compromise”.

17 Loggning av säkerhetsrelaterade händelser

17.1 Typer av händelser som loggas

Följande händelser skall loggas av samtliga CAs som är en del av Västra Götalandsregionens interna PKI-hierarki:

- Signifikanta CA nyckelhanteringshändelser såsom, ”CA key generation”, ”CA key backup” samt andra händelser som potentiellt utsätter den privata nyckeln för åtkomst för annan part än aktuell CA
- CA och ”subscriber” ”certificate life cycle”-händelser såsom:
  - Förfrågningar om certifikat, förnyelser, ”rekey” samt ”revocation”
  - Lyckade och misslyckade förfrågningar
  - Generering och utfärdning av certifikat
  - ”Revocation” av certifikat
  - ”Suspension” av certifikat
  - Utfärdning av CRL:er
- Säkerhetsrelaterade händelser på en CA såsom:
  - Systemkrasher, hårdvarufel och andra onormala tillstånd
  - Inloggningar
  - Policy förändringar
  - Kontohantering
  - Fysisk tillgång till en specifik CA i Västra Götalandsregionens interna PKI-hierarki

17.2 Frekvens på genomgång av loggar

Loggar skall analyseras minst kvartalsvis av auktoriserad personal för upptäckt av obehöriga aktiviteter. Redovisning av analys skall biläggas revionsrapport vid varje givet tillfälle.

17.3 Sparande av loggar

Systemloggar sparas i sju månader varefter de överskrivs av systemet, detta för att logganalys skall kunna ske över de två senaste revisionskvartalen. Vid upptäckta oegentligheter får loggar ej skrivas över eller på annat sätt förbli oåtkomliga intill dess att ISSO eller VGRs säkerhetsdirektör fattar beslut angående detta. Loggar över fysisk tillgång till CAs för Västra Götalandsregionens interna PKI-hierarki lagras i loggbok i minimum 5 år.

17.4 Skydd av loggar

Loggar skyddas genom en kombination av fysiska och logiska accesskontroller.

17.5 Loggarkivering

Sker enligt manuella rutiner efter beslut av ISSO samt VGRs säkerhetsdirektör. Rutiner för loggarkivering skall följa Västragötalandsregionens riktlinjer för informationssäkerhet.

17.6 ”Audit collection system”

Sker via VGR IT´s inloggningstjänsters SCOM.

17.7 Eventhanteringssystem och rutiner

Eventhantering sker i VGR IT´s inloggningstjänsters SCOM.

17.8 Krav på tidsangivelser

Samtliga ”Issuing CAs” i Västra Götalandsregionens interna PKI-hierarki synkroniseras med Västra Götalandsregionens domänkontrollanter i den gemensamma IT-plattformen. Alla tidsangivelser i exempelvis loggar följer därmed tiden som synkroniseras från denna källa. Västra Götalandsregionens Root CA synkroniseras manuellt med domänkontrollanter i den interna IT-infrastrukturen, detta skall kontrolleras vid varje uppstart av Root CA.

17.9 ”Key Changeover”

Samtliga CAs kommer att upphöra att utfärda certifikat och kommer antingen att genomgå ”rekey” eller tas ur drift innan certifikatet för aktuell CA slutar gälla. Samtliga CAs kommer att utfärda CRL:er tills dess att aktuell CA ej längre är i drift.

17.10 Disaster Recovery

Västra Götalandsregionens ”Policy Authority”, eller av denna utsedda parter, har ansvaret att hantera backuper av hela PKI-hierarkin, inklusive CAs, data, CA privata nycklar samt hårdvarutokens kopplade till eventuella HSM:er.

Backuper av Root CA skall ske innan någon typ av förändring sker, inklusive administrativa förändringar. Endast fullständiga systembackuper skall tas av Root CA, detta inkluderar även all data kopplad till Root CA.

Backuper av Issuing CAs skall ske kontinuerligt minst en gång per dygn och inkludera system state eller motsvarande, detta inkluderar CAs databaser samt loggar för databaser. Minst två fullständiga backuper av Issuing CAs skall alltid finnas tillgängliga. Förutom dessa nämnda backuprutiner skall system state säkerhetskopieras internt av CA-servrars operativsystem på daglig basis.

Vid behov att genomgå katastrofåterställning kommer Västra Götalandsregionens IT-incidentledning i samråd med Västra Götalandsregionens ”Policy Authority” att bedöma situationen och agera enligt sina rutiner och policys. Vid frånvaro av Västra Götalandsregionens ”Policy Authority” kan Västra Götalandsregionens IT-incidentledning agera enligt egna beslut.

17.11 CA Terminering

I de fall då det är nödvändigt att terminera en specifik CA kommer Västra Götalandsregionens ”Policy Authority” att planera och koordinera detta i samråd med sina ”subscribers” och ”relying parties” för att minimera påverkan. Västra Götalandsregionens ”Policy Authority” skall i sådana fall notifiera berörda parter med så bra framförhållning som situationen kräver.

18 Fysiska säkerhetsåtgärder

18.1 Fysisk åtkomst

Samtliga ”Issuing CAs” är placerade och hanteras enligt de standarder som Västra Götalandsregionen har för kritiska driftsservrar och är skyddade från otillbörlig fysisk åtkomst. Root CA för Västra Götalandsregionens interna PKI-hierarki är inte ansluten till något nätverk och är, när den inte används, inlåst i ett skyddsskåp som skyddar från såväl otillbörlig åtkomst som vatten-, gas- och brandskador m.m.

18.2 Avfallshantering

Känsliga dokument destrueras innan de slängs. Media som används för att transportera eller lagra känslig information förstörs innan de slängs.

Kryptografiska enheter, smart cards och andra enheter som kan innehålla privata nycklar förstörs fysiskt innan de slängs i enlighet med gällande CA policy.

18.3 Administrativa roller

Samtliga administrativa roller för Västra Götalandsregionens interna PKI hierarki definieras och dikteras av Västra Götalandsregionens CA-policy.

18.4 Uppgifter som kräver mer än en persons inblandning

Följande administrativa händelser skall utföras av minst två personer i samråd:

- All drift av Västra Götalandsregionens interna Root CA

18.5 Krav på autentisering för varje roll

Sker via någon av följande mekanismer:

- Användarnamn/lösenord
  - Användarnamn skall definieras enligt Västra Götalandsregionens driftrutiner
  - Lösenord skall bestå av minst 12 tecken med hög komplexitet
- Smart cards
  - PIN-koder består av minst 6 tecken

18.6 Utfärdande av roller

Västra Götalandsregionen utfärdar följande roller enligt dessa regler:

- Certification Authority Administrator (CAA) Administrativ produktions-/driftspersonal för CA - utfärdas av Västra Götalandsregionen och Västra Götalandsregionens säkerhetsdirktör
- ISSO – utfärdas av Västra Götalandsregionens säkhetsdirektör
- System Administrator (SA) Teknisk produktions-/driftspersonal för CA utfärdas av Västra Götalandsregionens ISSO och CAA

18.7 Utbildningskrav på personal

All personal som arbetar i någon roll inom Västra Götalandsregionens interna PKI-hierarki måste uppfylla följande utbildningskrav:

- God kännedom om PKI-koncept
- Policys och rutiner som ska följas vid handhavande och drift av komponenter i PKI-hierarkin
    - Detta CPS samt relevanta CA policys
- Systemutbildning för all mjuk/hårdvara som används inom aktuellt område

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 Västra Götalandsregionens säkerhetspolicy.

18.8 Frekvens på utbildningsrepetition

Sker i enlighet med Västra Götalandsregionens utbildningsrutiner, dock minst årligen för CAA och SA.

18.9 Sanktioner för otillbörligt handlande

Sker i enlighet med Västra Götalandsregionens regelverk.

18.10 Krav som ställs på utomstående kontrakterad personal

Sker i enlighet med Västra Götalandsregionens regelverk för externt kontrakterad personal.

18.11 Generering och lagring av nycklar

Samtliga nyckelpar som är en del av Västra Götalandsregionens interna PKI-hierarki skall genereras i enlighet med gällande CA policy.

Samtliga nyckelpar levereras till aktuell mottagare i enlighet med gällande CA policy, i de fall nycklar genereras av en ”subscriber” sker ingen nyckelleverans.

”Subscriber”-nycklar lagras i hårdvara eller mjukvara i enlighet med gällande CA policy.

Backupkopior av privata nycklar för CAs i Västra Götalandsregionens interna PKI-hierarki lagras i enlighet med gällande rutiner och policys hos Västra Götalandsregionens IT-organisation. Åtkomst till backupkopior sker enligt samma regelverk som för åtkomst till nyckelpar i produktionsmiljön.

Eventuell förstörelse av privata CA-nycklar sker i form av fysisk förstörelse av samtliga lagringsmedium som innehåller aktuell nyckel.

18.12 CA Policys

Samtliga certifikat som utfärdas av Västra Götalandsregionens interna PKI-hierarki skall följa de CA policys som ägs och förvaltas av Västra Götalandsregionens ”Policy Authority”. Aktuella CA policys finns på följande länk: http://cps.vgregion.se/VGC-CA%20Policy.htm.

Samtliga certifikat skall även följa de ”certificate profiles” som medföljer gällande CA policys som finns på följande länk: http://cps.vgregion.se/VGC%20Certificate%20profile.htm.

18.13 Förändringshantering av CA policy samt CPS

Förändringar till detta CPS, CA policys samt ”certificate profiles” kontrolleras och utförs av Västra Götalandsregionens ”Policy Authority”. Eventuella spörsmål eller förfrågningar om förändringar skall skriftligen kommuniceras till Västra Götalandsregionens ”Policy Authority”.