VGC RAPS

RA Practice Statement för Västra Götalandsregionens intern PKI

Kontaktperson: Mikael Cavrak

OID för policy: 1.2.752.113.10.1.2.1.3.1

1 Dokumentinformation

Datum	Författare	Version	Kommentar
101001	Conny Balazs, KnowIT Fredrik Rasmusson, Västra Götalandsregionen		
1012020	Valter Lindström Monika Göransson Fredrik Rasmusson		
110308	Mikael Cavrak Fredrik Rasmusson		
120209	Fredrik Rasmusson Mikael Cavrak Magnus Svensson	1.0	

Innehållsförteckning

2 Introduktion

Detta dokument är den Registration Authority Practice Statement (RAPS) som beskriver hur RA-organisationen är utformad för Västra Götalandsregionens interna PKI-hierarki för att uppfylla de krav som anges i RA-policyn för denna PKI-hierarki.

Västra Götalandsregionens interna PKI-hierarki utger elektroniska certifikat, så kallade Västra Götaland Certificate (VGC), för personer och funktioner inom Västra Götalandsregionen. Västra Götalandsregionens interna PKI-lösning används för att tillhandahålla certifikat åt interna tillämpningar som kräver detta.

Denna RAPS beskriver förutsättningar, ansvar och de procedurer och rutiner som tillämpas vid beställning och spärrning av VGC inom RA-organisationen. Målgrupp för dokumentet är Västra Götalandsregionens ”Policy Authority”, RA, ORA, LRA samt ARA berörda av Västra Götalandsregionens interna PKI-hierarki.

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.

Denna RAPS beskriver förhållningssätt, standarder och rutiner som appliceras av RA-organisationen inom ramarna för Västra Götalandsregionens interna PKI-hierarki.

Frågor gällande denna RAPS skall riktas till Västra Götalandsregionens ”Policy Authority”.

2.1 Förändringshantering av CP, RA-policy, RAPS samt CPS

Förändringar till denna RAPS, CPS, RA-policy, CA-policy samt ”certificate profiles” kontrolleras och utförs av Västra Götalandsregionens ”Policy Authority”.

2.2 Refererade dokument

Västra Götalandsregionens PKI Certificate Policy

Västra Götalandsregionens PKI Certificate Practice Statement

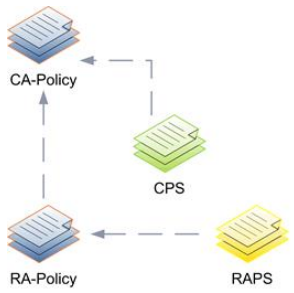
Västra Götalandsregionens PKI Registration Authority Policy

Kontaktuppgifter

Denna RAPS samt andra styrande dokument för Västra Götalandsregionens interna PKI-hierarki administreras av Västra Götalandsregionens ”Policy Authority”. Kontaktuppgifter för denna part är som följer. VGR IT, Västra Götalandsregionen.

OID för policy: 1.2.752.113.10.1.2.1.3.1

3 Relation till övriga styrande dokument



Figur 1. *RAPS relation till övriga styrande dokument.*

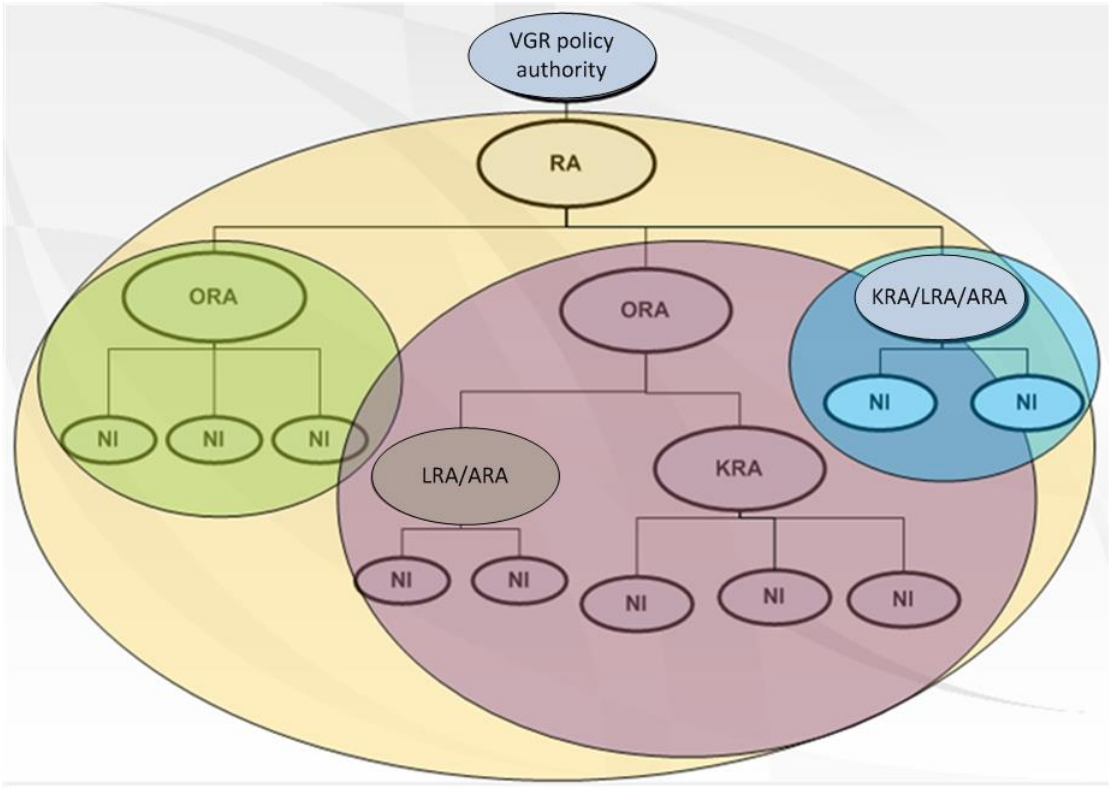
CA-policy är det dokument som beskriver de övergripande kraven för procedurer och rutiner som ska tillämpas vid hantering av VGC.

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

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

Tillämpningsanvisning RAPS (detta dokument) beskriver RA-organisationen och rutiner för att uppfylla de krav och förpliktelser som anges i CA-policy, CPS och RA-policy.

4 RA-organisation



Figur 2. *Roller inom RA-organisation*

4.1 Organisationens roller

RA området tecknar överenskommelse med Västra Götalandsregionens ”Policy Authority” om rätt att använda VGC. I överenskommelsen åtar sig RA området att upprätta en organisation för beställning och återkallande av VGC, en RA-organisation. Ett exempel på en RA-organisation illustreras i figur 2.

RA har det övergripande ansvaret för RA-organisationen. För effektivare administration av RA-organisationen kan en eller flera RA personer/funktioner etableras. Verksamhetsansvarig för organisationen upprättar och bemannar RA och meddelar detta till Västra Götalandsregionens ”Policy Authority”. Förändringar av RA personal/funktioner meddelas direkt till Västra Götalandsregionens ”Policy Authority”. RA upprättar och bemannar ORA (om så är tillämpbart), LRA samt ARA. ORA /LRA/ARA ansvarar för hanteringen av VGC inom sin del av RA-organisationen. Organisationen upprättar även en supportorganisation samt definierar behöriga beställare för kommunikation med Västra Götalandsregionens ”Policy Authority”.

Inom varje förvaltning (motsvarande) kan en ansvarig person, ORA, utses för certifikatshantering för en eller flera förvaltningar. Om ORA-rollen ej tillämpas äger RA detta ansvar själv. Dennes uppgift är att bygga upp och bemanna en organisation av LRA-personer samt ARA-funktioner inom sin del av RA-organisationen. RA/ORA svarar även för den praktiska hanteringen av certifikat och kort ute i verksamheten.

RA/ORA utfärdar VGC till nyckelinnehavare (NI) i enlighet med gällande CA-policy inom Västra Götalandsregionen, som kan vara personer eller funktioner. VGC för personer kan tilldelas anställda inom organisationen eller till personer som utför uppdrag åt organisationen.

LRA utfärdar VGC till nyckelinnehavare (NI) i samband med beställning av certifikat för personer. VGC för personer kan tilldelas anställda inom organisationen eller till personer som utför uppdrag åt organisationen enligt gällande CA-policy

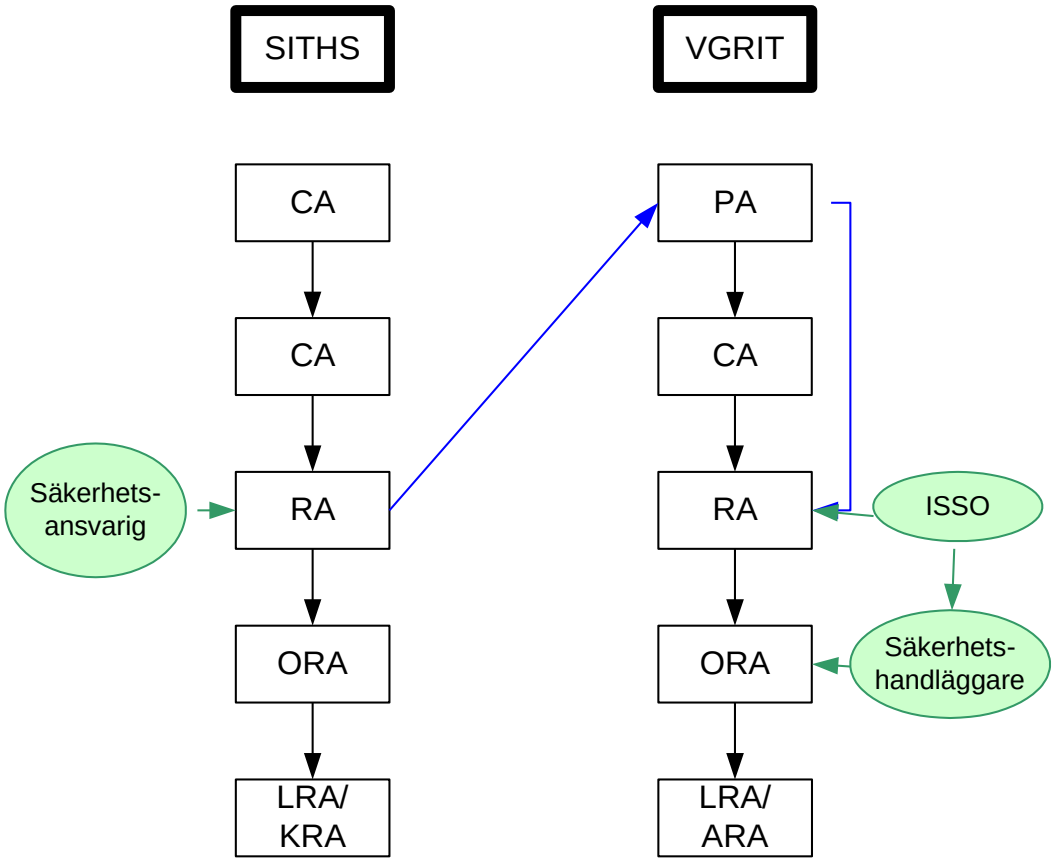
Säkerhetsansvarig (ISSO) ansvarar för verksamhetens efterlevnad av utgivningsprocesser av kort och certifikat. Uppdraget innebär även planering av säkerhetsrevisioner.

Registeransvarig ansvarar för register över utfärdade VGC certifikat. Registeransvarig för respektive ORA-område är ORA. ORA för VGR IT är tillika registeransvarig för RA-område.

Inom Västra Götalandsregionens interna PKI-hierarki finns följande roller:

Roll
Säkerhetshandläggare
Registeransvarig
RA
ORA
LRA
ARA

Inbördes relation mellan SITHS och VGR Interna PKI:



5 Nyckelinnehavare och certifikatstyper

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

Typ av nyckelinnehavare (NI)	Certifikattyp	Certifikatsform
Person med giltig e-legitimation	VGC Person	Sekundärcertifikat
System eller tjänst	VGC Funktion	Primärcertifikat

Personer och funktioner finns upplagda som objekt i Västra Götalandsregionens Active Directory-katalog (vgregion.se). Detta är en förutsättning för att kunna ge ut VGC för personer och funktioner.

5.1 VGC Person

VGC Person utfärdas till fysisk person anställd inom organisationen. VGC Person kan utfärdas till personer inom en organisation som har avtal med Västra Götalandsregionen och till personer som utför uppdrag åt Västra Götalandsregionen. VGC Person lagras i Västra Götalandsregionens Active Directory-katalog och på bärande kort.

5.2 VGC Funktion

VGC Funktion utfärdas till funktion inom organisationen eller funktion inom organisation som har avtal med Västra Götalandsregionen. Funktionen kan vara en verksamhetsfunktion, en tjänst eller ett system.

6 Allmänna villkor

6.1 Förpliktelser och åtaganden

Möjlighet till ställföreträdande personer finns på alla nivåer i organisationen.

1.1.1 Områdeschef VGR IT – Västra GötalandsRegionens Policy Authority

Områdeschef VGR IT ansvarar för att upprätta avtal med Västra Götalandsregionens ”Policy Authority” och tillsätter RA/ORA samt ställföreträdande RA enligt Västra Götalandsregionens ”Policy Authority”:s beslut. Då RA slutar sitt uppdrag meddelar Västra Götalandsregionens ”Policy Authority” detta till områdeschef VGR IT inom skälig tid. Behörigheter för RA tas då bort och delas ut till efterträdare.

1.1.2 RA – Västra Götalandsregionens „Policy Authority“

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

1.1.3 RA – ORA

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

1.1.4 RA/ORA – LRA

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

1.1.5 RA/ORA – ARA

RA eller ORA utser ARA i RA-organisationen, och ger behörighet samt ansvarar för att dessa funktioner följer gällande rutiner. RA/ORA har en förteckning på behöriga ARA inom det egna ansvarsområdet, och ARA-områdena är klart definierade. Då en ARA slutar sitt uppdrag meddelar ORA för området detta till RA inom skälig tid och behörigheter för ARA tas bort.

1.1.6 LRA/ARA – NI

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

Om NI inte har kontroll över utfärdade kort, eller tillhörande PIN- och PUK-koder, kontaktas LRA.

1.1.7 RA/ORA – behörig representant

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

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

7 Missbruk av certifikat

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

8 Friskrivning från ansvar

Västra Götalandsregionen och personer inom RA-organisationen ansvarar inte för följder av:

- Att någon nyckel ändras på otillbörligt sätt
- Att NI använder certifikat på otillbörligt sätt
- Felaktigheter i CA:s certifikatsutfärdande

9 Revision

9.1 Extern kontroll

Västra Götalandsregionens ”Policy Authority” har rätt att revidera ansluten RA-organisation och meddelar skriftligen RA-organisationen detta. Även Västra Götalandsregionens säkerhetsansvarige (ISSO) har denna rättighet.

9.2 Intern kontroll

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

10 Konfidentialitet

Frågor om konfidentialitet beträffande uppgifter om den personal för vilka certifikat utfärdas regleras av bl.a. tryckfrihetsförordningen, sekretesslagen och Patientsäkerhetslagen samt Socialtjänstlagen (SoL).

RAPS tillämpas så att gällande lagar om konfidentialitet uppfylls.

11 Rutiner för identifiering

11.1 VGC Person

1.1.8 Identifiering vid beställning av VGC Person

Vid initial beställning av VGC Person och när man efter en kortförlust ska få ett nytt kort med VGC Person krävs personlig närvaro av NI med giltig legitimation.

Vid nästkommande beställning av VGC Person på befintligt kort krävs inte personlig närvaro av NI som har/eller har haft ett giltigt VGC. Den elektroniska ID-handlingen (e-legitimationen) på befintligt kort räcker.

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

1. Personlig närvaro av NI med giltig legitimation (SIS godkänd eller motsvarande).
2. RA/ORA har personlig kännedom om NI och går i god för NI:s identitet.

Sättet som NI identifieras på dokumenteras av xRA.

1.1.9 Identifiering vid spärrning av VGC person

Då RA/ORA/LRA via CA begär spärrning av VGC Person identifierar sig RA/ORA/LRA elektroniskt mot CA.

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

1. Av NI signerad elektronisk beställning, t ex genom signerad e-post.
2. Personlig närvaro av NI med giltig legitimation (SIS godkänd eller motsvarande).
3. RA/ORA /LRA har personlig kännedom om NI och går i god för NI:s identitet.
4. Som reservrutin, om det misstänks föreligga risk för missbruk av en privat nyckel, associerad med ett certifikat, kan en förenklad form av identifiering göras. Detta görs genom motringning och/eller genom att ställa kontrollfrågor.

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

1. Signerad elektronisk beställning av verksamhetsansvarig, t ex genom signerad e-post eller sin personliga e-legitimation.
2. Personlig närvaro av verksamhetsansvarig med giltig legitimation (SIS godkänd eller motsvarande).
3. RA/ORA/ LRA har personlig kännedom om verksamhetsansvarig och går i god för verksamhetsansvarigs identitet.

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

11.2 VGC Funktion

1.1.10 Identifiering vid beställning av VGC Funktion

Vid utfärdande av VGC Funktion sker alltid identifiering av behörig representant genom ett giltigt identitetskort eller giltiga behörigheter i Västra Götalandsregionens Active Directory-katalog (vgregion.se).

1.1.11 Identifiering vid spärrning av VGC Funktion

Vid utfärdande av VGC Funktion sker alltid identifiering av behörig representant genom ett giltigt identitetskort eller giltiga behörigheter i Västra Götalandsregionens Active Directory-katalog (vgregion.se).

12 Rutiner för certifikatshantering

12.1 Beslut om tilldelning av VGC

Verksamhetsansvariga inom respektive RA/ORA/LRA/ARA-område beslutar om tilldelning av VGC inom sitt ansvarsområde.

12.2 Beställning av VGC

12.2.1 VGC Person till nytt kort

1. En förutsättning för att NI skall kunna få tilldelat ett nytt kort är att gällande rutiner inom Västra Götalandsregionens SITHS-förvaltning åtföljs eftersom det är denna organisationer som utfärdar nya kort.
2. NI:s verksamhetsansvarige kontaktar sin RA/LRA. RA/LRA förvissar sig om att NI har uppdrag inom det egna ansvarsområdet samt att uppgifterna som ska ingå i VGC Person är korrekta.
3. RA/LRA gör en beställning av VGC i CA-systemet.
4. Personen identifieras enligt paragrafen ”Identifiering vid beställning av VGC Person” och identifieringssättet dokumenteras.
5. Beställningen av VGC till nytt kort fullgörs och signeras av RA/LRA.

12.2.2 VGC Person till befintligt kort

1. NI kontaktar sin RA/ORA/LRA som förvissar sig om att NI har uppdrag inom det egna RA/ORA/LRA-området samt att uppgifterna som ska ingå i VGC är korrekta.
2. Personen identifieras enligt paragrafen ” Identifiering vid beställning av VGC Person” (via e-legitimationen).
3. RA/ORA/LRA gör en beställning av VGC- i CA-systemet. Giltighetstiden sätts till anställningens/uppdragets slut eller maximalt till primärcertifikatets giltighetstid.
4. Beställningen av VGC Person signeras av RA/ORA/LRA och därefter kan NI få ut sitt VGC Person som samtidigt lagras i Västra Götalandsregionens Active Directory-katalog (vgregion.se).

12.2.3 VGC Funktion (PKCS#12)

1. Behörig representant kontaktar sin RA/ORA/ARA.
2. Personen identifieras enligt paragrafen ”Identifiering vid beställning av VGC Funktion”.
3. RA/ORA/ARA kontrollerar att representanten är behörig beställare av VGC Funktion enligt överenskommelse med verksamhetsansvarig samt att behörig representant och aktuell organisation/funktion finns upplagd i Västra Götalandsregionens Active Directory-katalog (vgregion.se)på rätt nivå och med rätt uppgifter.
4. RA/ORA/ARA beställer VGC Funktion och anger behörig representant. Behörig representant måste ha ett giltigt ID i Västra Götalandsregionens Active Directory-katalog (vgregion.se).
5. CA genererar VGC och nyckelpar. RA/ORA/ARA sparar ner PKCS#12-objektet med VGC.
6. Utlämning av VGC sker genom personlig närvaro av behörig representant till mobilt media.
7. Koder/lösenord för aktuellt VGC lämnas till behörig representant på separat mobilt media alternativt skickas lösenord för PKCS#12 objektet till behörig representant via säker e-post.
8. RA/ORA/ARA arkiverar kvittens om utlämnande av VGC .

Mottagande av koder och nycklar sker enligt paragrafen ” Utlämnande av privat nyckel i samband med utfärdande av VGC Funktion (PKCS#10 och PKCS#12)”.

12.2.4 VGC Funktion (PKCS#10)

1. Behörig representant kontaktar sin RA/ORA/ARA.
2. Personen identifieras enligt paragrafen ”Identifiering vid beställning av VGC Funktion”.
3. RA/ORA/ARA kontrollerar att representanten är behörig beställare av VGC Funktion enligt överenskommelse med verksamhetsansvarig samt att behörig representant och aktuell funktion finns upplagd i Västra Götalandsregionens Active Directory-katalog (vgregion.se) på rätt nivå och med rätt uppgifter.
4. Behörig representant överlämnar certifikatsunderlag (CSR) till RA/ORA/ARA, t.ex. genom signerad e-post.
5. RA/ORA/ARA beställer VGC Funktion med hjälp av CSR och anger behörig representant.
6. CA genererar VGC. Därefter skickar CA PKCS#10-objekt med VGC till RA/ORA/ARA. RA/ORA/ARA sparar ner PKCS#10-objektet med VGC och överlämnar detta till behörig representant, t.ex. genom signerad e-post.
7. Behörig representant kvitterar mottagandet av VGC Funktion för PKCS#10 och RA/ORA/ARA arkiverar uppgifter om utlämnandet av VGC Funktion.
8. Mottagande av koder och nycklar sker enligt paragrafen ” Utlämnande av privat nyckel i samband med utfärdande av VGC Funktion (PKCS#10 och PKCS#12)”.

12.3 Spärr av VGC

12.3.1 Godkända anledningar till att begära spärr av VGC

VGC spärras om något av följande har inträffat:

- Förhållanden som påverkar certifikatsinnehållet har ändrats
- Någon uppgift i VGC är eller misstänks vara felaktig
- NI har tappat kontrollen över kortet eller koderna
- NI:s e-legitimation har blivit spärrad
- NI:s e-legitimation är inte tillgängligt för NI (kortförlust)
- Den privata nyckeln har röjts
- Kort återlämnas

12.3.2 Undantag

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

12.3.3 Spärrbegäran

Följande roller kan begära spärrning av VGC:

- NI kan av RA/ORA/LRA/ARA begära spärrning av sitt eget VGC
- Verksamhetsansvarig kan av RA/ORA/LRA/ARA begära spärrning av VGC inom egen organisation
- Behörig representant kan av RA/ORA/ARA begära spärrning av det VGC Funktion som representanten ansvarar för
- RA/ORA/LRA/ARA kan begära spärrning av VGC inom det egna ansvarsområdet.

12.3.4 Spärrning

Följande roller kan utföra spärr av VGC via CA:

- NI kan själv spärra sitt eget VGC i de förutsättningar ”Policy Authority” godkänner detta.
- RA kan spärra VGC hos CA inom eget RA-område
- ORA kan spärra VGC hos CA inom eget ORA-område
- LRA kan spärra VGC Person hos CA inom eget LRA-område
- ARA kan spärra VGC hos CA inom eget ARA-område

13 Arkivering

13.1 RA

RA ansvarar för att följande arkiveras:

- RA-organisationens avtal med Västra Götalandsregionens ”Policy Authority”
- RA-organisationens godkända RAPS
- RA-organisationens förteckning av utsedda RA och dess ställföreträdande, inklusive historik
- RA-organisationens förteckning av utsedda ORA personer och ställföreträdande samt deras områden, inklusive historik
- Där ORA personer inte förekommer ansvarar RA för förteckning av RA-organisationens utsedda LRA/ARA, behöriga representanter och dess ställföreträdande samt deras områden, inklusive historik
- RA-organisationens förteckning över avtal med andra parter, t ex driftleverantörer eller andra ingående organisationer, inklusive historik och uppgifter vid utfärdande av VGC Funktion, t.ex. kvittens, identitet på behörig representant och datum för utlämnandet av VGC.

13.2 ORA

ORA ansvarar för att följande arkiveras:

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

13.3 LRA/ARA

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

- Uppgifter om utlämnade VGC
- Uppgifter om spärrade VGC

14 Avbrottshantering och avveckling

14.1 Rutiner för avbrottshantering

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

14.2 Avveckling av RA-organisation

Vid avveckling av RA-organisation åligger det områdeschef VGR IT att avveckla RA-organisationen enligt följande procedur:

- Informera alla NI och alla parter som Västra Götalandsregionen har avtal eller överenskommelser med
- Avsluta åtagande och behörigheter för RA-organisationen och tillse att alla arkiv och loggar bevaras/överlämnas enligt gällande anvisningar inom Västra Götalandsregionen.

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

- Informera alla NI och alla parter som RA/ORA har avtal och/eller överenskommelser med
- Avsluta åtagande och behörigheter för ORA/LRA/ARA-organisationen och tillse att alla arkiv och loggar bevaras/överlämnas enligt gällande anvisningar inom Västra Götalandsregionen.

15 Fysisk och personalorienterad säkerhet

15.1 Fysisk säkerhet

Vid utlämnande av nycklar och koder beaktas den fysiska säkerheten. RA/ORA/LRA-arbetsplatsen skall finnas i låsbart utrymme med låsbara skåp för förvaring av arkivmaterial enligt paragrafen ”arkivering”.

Då RA/ORA/LRA lämnar arbetsplatsen lämnas inte kort obevakade.

Koder förvaras så att inte obehörig får tillgång till dessa. NI uppmanas att förvara koder och bärare av VGC på fysiskt åtskilda ställen.

15.2 Personorienterad säkerhet

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

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

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

16 Teknikorienterad säkerhet

16.1 Utlämnande av privat nyckel

1.1.12 Utlämnande av privat nyckel i samband med utfärdande av VGC Funktion (PKCS#10 och PKCS#12)

Nycklar och koder utlämnas av RA/ORA/ARA till behörig representant för NI, sedan denne identifierat sig, se paragrafen ” Rutiner för identifiering”. Mottagande av nycklar och koder kvitteras av den behöriga representanten. Kvittens ska sparas enligt gällande arkiveringsregler enligt paragrafen ”Arkivering”. Den behöriga representanten ska förvara nycklar och koder på fysiskt åtskilda platser.

Exempelvis vid installation av PKCS#12-objekt på en server skall PKCS#12-objektet ifråga raderas från servern där installationen utförts.

16.2 Skydd av privat nyckel

För privata nycklar tillhörande VGC Funktion gäller att de förvaras och distribueras på ett säkert och skyddat sätt så att de inte faller i orätta händer samt att de inte i något fall exponeras eller brukas på otillbörligt sätt, innan de nått rätt mottagare. Därför skall NI skydda denna utrustning där VGC förvaras eller används. NI skall därför:

- Välja säkerhetskoder som inte är lätta att lista ut
- Hålla säkerhetskoderna hemliga och inte anteckna säkerhetskoderna på ett sätt eller en plats som gör att de kan kopplas till VGC

16.3 Arkivering av privata nycklar

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

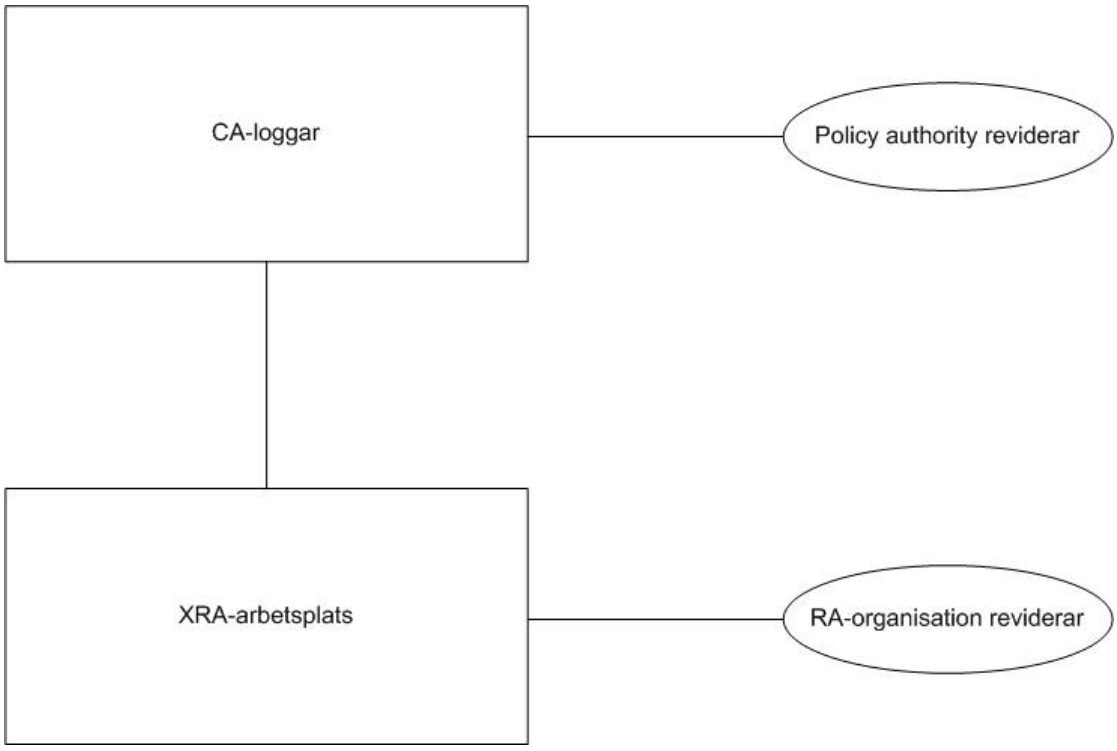
Privata nycklar tillhörande VGC Funktion får endast arkiveras för backupändamål. Om sådan lagras skall den göras enligt rutin i bilaga 5.

17 Processer för säkerhetsrevision

17.1 Loggning

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

Loggning sker också lokalt inom RA-organisationen. De lokala loggarna är likaså av två slag, manuellt förd administrativ dokumentation och systemloggar på operativsystemnivå.



Figur 3 - Loggar på olika nivåer

Alla loggar bör regelbundet analyseras av RA-organisationen samt göras tillgänglig för revision.

1.1.13 Analys av logg

Verksamhetsansvarig eller annan utsedd person som inte utfärdar VGC (oberoende part) skall regelbundet analysera logg som genererats inom RA-organisationen. Loggar analyseras halvårsvis under månaderna April samt Oktober för upptäckt av obehöriga aktiviteter samt vid behov. Resultat av logganalys skickas till ”Policy Authority”, RA samt berörd ORA.

1.1.14 Bevarandetid för logg

Loggar bevaras i CA-systemet i minst 10 år.

17.2 Definitioner

Endast begrepp och termer som används i detta dokument tas upp nedan.

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

Behörig representant: Anställd hos uppdragsgivare som har befogenhet att beställa och spärra certifikat hos CA.

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

CA: Part som utfärdar certifikat genom att signera certifikat med sin privata CA-nyckel. Förkortning av Certification Authority.

CA-nyckel: Nyckelpar där den privata nyckeln används av CA för att signera certifikat och där den publika nyckeln används för att verifiera samma certifikat.

Certification Authority: Se CA.

Certification Practice Statement: Se CPS.

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

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

CRL: Se spärrlista. Förkortning av Certificate Revocation List.

CSR: underlag innehållande bland annat publik nyckel och uppgifter ifrån t ex en webbserver. CSR används vid skapandet av ett certifikat till den aktuella servern. Förkortning av Certificate Signing Request.

Dekryptering: Processen att omvandla krypterad (kodad) information till dekrypterad (läsbar) information. Se vidare kryptering.

Digital signatur: En form av elektronisk signatur som skapas genom att signatären signerar digital information med sin privata nyckel enligt en speciell procedur. Den digitala signaturen kan användas dels för att spåra vem som signerat informationen och dels för att verifiera att informationen inte förändrats sedan den signerades.

e-ID-kort: Elektroniska ID-kort i form av ett aktivt kort innehållande certifikat och nycklar samtidigt som kortets framsida kan utgöra en visuell ID-handling.

e-legitimation: De certifikat på eID-kortet/eTjänstekortet som innehåller personliga identitetsuppgifter, t.ex. personnummer.

eTjänstekort: Företagskort med e-legitimation.

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

KRA: Kort Registration Authority, en person som av RA eller i förekommande fall ORA tilldelats uppgiften att hantera eTjänstekort.

Kryptering: Processen att omvandla tolkningsbar information (klartext) till krypterad information. Syftet med den krypterade informationen är att den inte skall kunna tolkas av någon som inte innehar exakt rätt nyckel (vid symmetrisk kryptering) eller exakt rätt privat nyckel (vid asymmetrisk kryptering) som krävs för att korrekt dekryptera informationen.

Logg: En sekventiell och obruten lista över händelser i ett system eller en process. En typisk logg innehåller loggposter för enskilda händelser vilka var och en innehåller information om händelsen, vem som initierade den, när den inträffade, vad den resulterade i etc.

Lokal RA: se LRA.

LRA: En funktion som av RA eller ORA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt därtill hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärrning, nyckelgenerering mm.

LRA-område: Den del av en organisation inom vilken en LRA har rätt att utfärda certifikat.

Nyckelinnehavare: I detta sammanhang en person, en organisation, en organisatorisk enhet eller en function som innehar exklusiv kontroll av den privata nyckel vars publika motsvarighet certifieras i ett certifikat.

ORA: Organisation Registration Authority, en person som av RA tilldelats uppgiften att administrera behörigheter och hantera eTjänstekort och certifikat inom det egna ORA-området, dvs. den del av RA-organisationen som ORA ansvarar för.

PIN-kod: Kod som används för att ge access till privat nyckel lagrad på eID-kort eller i PKCS#12-fil. Koden är vanligtvis numerisk, fyr-, fem- eller sexställig. Det finns en PIN-kod för samtliga privata autenticeringsnycklar och privata signeringsnycklar. PIN-koderna skall vara hemliga för alla utom för nyckelinnehavaren.

PKCS#10 fil: Fil innehållande certifikat för en nyckelinnehavare. Certifikatet är skapat utifrån ett underlag en så kallad CSR.

PKCS#12 fil: Fil innehållande privata nycklar och certifikat för en nyckelinnehavare. Filen är signerad av CA och krypterad.

Policy: På principer grundat handlande eller grundprinciper för ett företags eller en organizations handlande. I detta dokument avses principerna, inte själva handlandet, samt syftar man här antingen på RA-policy eller på CA-policy.

Primärcertifikat: Ett certifikat, som utfärdats på grundval av identifiering av nyckelinnehavaren på annat sätt än att denne företett ett annat certifikat. Identifieringen sker då vanligtvis genom att nyckelinnehavaren istället företer en identitetshandling.

Privat nyckel: Den privata delen av ett nyckelpar som används inom asymmetrisk kryptering. Den private nyckeln används främst för att skapa digitala signaturer samt för dekryptering av krypterad information.

Publik nyckel: Den publika delen av ett nyckelpar som används inom asymmetrisk kryptering. Den publika nyckeln används främst för att verifiera digitala signaturer samt för att kryptera information.

PUK-kod: Kod som kan användas för att ändra eller skapa nya PIN-koder. PUK-koden är betydligt längre än PIN-koden, 12 siffror eller mer.

RA: En part som av CA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt därtill hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärrning, nyckelgenerering mm.

RA-policy: En namngiven uppsättning reg¬ler för RA:s roll i framställning, utgivning och spärrning av certifikat och som reglerar tillämpligheten av certifikaten inom ett specifikt användningsområde.

RAPS: En dokumentation av hur en RA tillämpar en RA-policy.

Registration Authority: Se RA.

Registration Authority Practice Statement: Se RAPS.

Sekundärcertifikat: Certifikat som utfärdas på grundval av ett annat certifikat, primärcertifikatet. Detta innebär att utfärdande CA litar på den CA som utgett primärcertifikatet, d.v.s. accepterar certifieringen av den publika nyckeln till nyckelinnehavaren, vilket i sin tur förutsätter tillit till att identifieringen av nyckelinnehavaren vid utfärdandet av primärcertifikatet är korrekt.

Spärrlista: En digitalt signerad lista över spärrade certifikat. Spärrlistan förkortas ofta CRL.

Spärrning: Processen att spärra ett certifikat genom att lägga in information om certifikatet i en spärrlista.

Skriftlig: Där denna policy specificerar att information skall vara skriftlig, tillgodoses detta krav generellt även av digitala data under förutsättning att dess informationsinnehåll är tillgängligt på ett sådant sätt att det är användbart för involverade parter.

Symmetrisk kryptering: Kryptosystem som kännetecknas av att både sändare och mottagare av krypterad information an¬vänder samma hemliga nyckel både för kryptering och dekryptering.

Uppdragsgivare: Den organisation som genom avtal ger i uppdrag till en CA att utfärda certifikat för organisationens anställda, organisatoriska enheter och funktioner.

Verifiering: Processen att säkerställa att ett antagande är korrekt. Detta begrepp avser främst processen att säkerställa att en digital signatur är framställd av den som av den signerade informationen framstår som dess utställare.

18 Bilaga 1 - Rutiner vid missbruk av certifikat

Då missbruk av certifikat misstänks eller kommer tillkänna skall ORA/LRA/ARA omedelbart informeras och vidta lämpliga åtgärder för att stoppa missbruket, till exempel genom att begära spärrning av aktuella certifikat och/eller behörigheter i CA-systemet. Vid eventuellt missbruk av certifikat skall RA och säkerhetsansvarig meddelas. RA samt eventuell ORA skall utreda missbrukets omfattning, informera berörd personal, t.ex. berörda LRA-personer, om aktuell händelse samt vilka åtgärder som vidtagits för att förhindra missbruket.

Erfarenheter av utredningar i samband med missbruk av certifikat skall återkopplas till verksamheten.

I allvarliga fall av missbruk av certifikat skall Västra Götalandsregionens ”Policy Authority” samt säkerhetsansvarig inom Västra Götalandsregionen underrättas.

19 Bilaga 2 - Plan för genomförande av intern kontroll

Löpande intern kontroll skall genomföras i syfte att säkerställa efterlevnaden av RAPS och RA-policy inom Västra Götalandsregionen. Riskanalys avseende Västra Götalandsregionens RA-organisation kommer att ligga till grund för Västra Götalandsregionens plan för genomförande av intern kontroll. Riskanalys skall genomföras löpande eller då säkerhetspåverkande förändringar sker.

För att kontrollera det manuella arbetet inom Västra Götalandsregionens RA-organisation kommer återkommande kontroller att göras bland RA/ORA/LRA/ARA-personal/funktioner för att tillse att fastställda rutiner och regler följs.

Vid upptäckt av brister i det manuella arbetet kommer åtgärder att vidtas för att korrigera dessa, till exempel genom utökad utbildning av RA/ORA/LRA-personer, förändring av rutiner eller utbyte av RA/ORA/LRA-personer.

All revision sker löpande eller efter behov, dock minst med 12 månaders intervall.

Samtliga funktionsavbrott skall utredas. Ansvarig för att detta sker är RA eller av denna utsedd part.

20 Bilaga 3. Kontinuitetsplan med rutiner för avbrottshantering

20.1 Avbrott i beställning, spärrning samt andra funktioner för administration av certifikat

I händelse av att beställning, spärrning samt andra funktioner för administration av certifikat inte kan genomföras skall ”Policy Authority”, RA samt ORA omedelbart informeras. Dessa ska undersöka felets omfattning och beräknad tid för åtgärd. Information om driftstörningen skall omedelbart gå till RA samt till samtliga LRA och ORA.

Under avbrottet skall RA/LRA/ORA manuellt registrera inkommande spärrbeställningar och vid särskilt kritiska fall tillse att behörigheter kopplade till dessa certifikat tillfälligt dras in.

När CA-systemet åter är i drift skall skall ”Policy Authority”, RA samt ORA informeras om detta samt orsak till avbrottet. RA/ORA vidareförmedlar denna information till samtliga LRA samt säkerhetshandläggare och ISSO.

Då avbrott som påverkar ovanstående inträffar i CA-systemet eller Västra Götalandsregionens Active Directory-katalog (vgregion.se) är det driftorganisation för CA-systemet och Västra Götalandsregionens Active Directory-katalog (vgregion.se) som ansvarar för att informera RA och berörd verksamhet..

Alternativa inloggnings- och signeringsmetoder i drabbade applikationer användas i enlighet med respektive systems kontinuitetsplan, informationsansvarig är incidenkoordinator (IK) inom VGR IT enligt gällande rutiner.

20.2 Avbrott i möjligheten att använda certifikat

Under avbrott då man inte har åtkomst till den senaste spärrlistan och/eller en online tjänst för certifikatverifiering (OCSP/SCVP-tjänst) för att verifiera att ett certifikat är giltigt kan den gamla versionen av spärrlistan användas i enlighet med gällande CPS.

I händelse av att man inte längre kan lita på hela eller delar av Västra Götalandsregionens PKI-hierarki skall hela Västra Götalandsregionens RA-organisation samt ISSO informeras. Applikationer som använder påverkade certifikat för inloggning och/eller signering skall ha en funktionalitet som möjliggör att andra förenklade inloggnings- och signeringsmöjligheter kan tillämpas tills nya certifikat skapats.

Då avbrott som påverkar ovanstående inträffar i CA-systemet eller i Västra Götalandsregionens Active Directory-katalog är det driftorganisation för CA-systemet och Västra Götalandsregionens Active Directory-katalog (vgregion.se) som ansvarar för att informera RA.

20.3 Återkoppling till verksamheten

Ovanstående rutiner för eventuella avbrott skall testas enligt beslut av Västra Götalandsregionens ”Policy Authority” och erfarenheter av sådana tester skall återkopplas till verksamheten samt ISSO och säkerhetsansvarig..

21 Bilaga 4 - Lista på organisationer som omfattas av denna RAPS

21.1 RA-organisation i Västra Götalandsregionen

RA-område	RA-personer
Västra Götalandsregionen	Personal i leverans Identitet och åtkomst.

RA-område	Säkerhetshandläggare
Västra Götalandsregionen	

22 Bilaga 5 - Rutin för arkivering av privata nycklar

Arkivering av privata nycklar sker endast i enlighet med gällande certifikatpolicy samt tillhörande CPS. Backuper, på servrar innehållande funktionscertifikat, ska förvaras på ett säkert och skyddat sätt så att dessa inte faller i orätta händer och därmed medger att privata nycklar och ev