VGC CA Policy

Certifikatspolicy för utgivande av certifikat inom Västra Götalandsregionens interna PKI

Kontaktperson: Fredrik Rasmusson

OID för policy 1.2.752.113.10.1.2.1.1.2

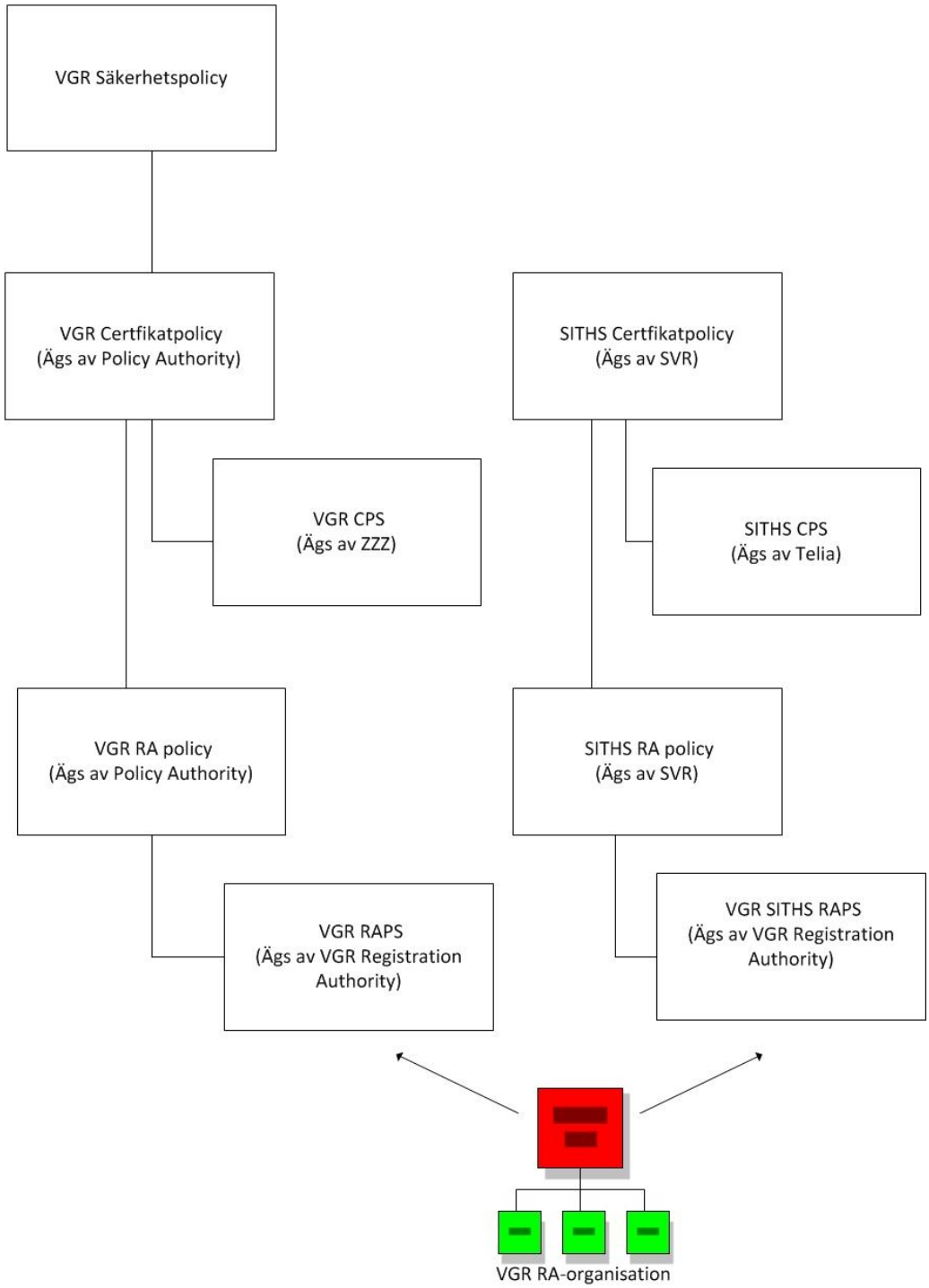
Innehållsförteckning

Certifikatspolicy för utgivande av certifikat inom Västra Götalandsregionens interna PKI

Detta dokument innehåller CA policy för utgivning av certifikat inom Västra Götalandsregionens interna PKI-hierarki, s.k. Västra Götalands Certifikat (VGC). Denna certifikatpolicy kräver upprättande av ett separat CPS. Den förutsätter också att minst en ”Registration Authority”, RA upprättas och att denna/dessa arbetar enligt en särskild RA-policy.

Detta dokument ägs och förvaltas av Västra Götalandsregionens SITHS RA. Relationen mellan Västra Götalandsregionens interna PKI och SITHS kan beskrivas enligt följande:

- SITHS CA policy samt RA-policy är styrande för Västra Götalandsregionens CA policy samt RA policy
    - Västra Götalandsregionens CA policy samt RA policy dikteras av de vilkor som är definierade i SITHS CA policy samt RA policy. Dock är Västra Götalandsregionens CA policy samt RA policy fristående från SITHS motsvarande policys.



Beslut gällande besättning av VGR Policy Authority ligger och dikterar att SITHS VGR Registration Authority innehar denna roll för VGRs interna PKI.

Revisionshistorik

Datum	Författare	Version	Kommentar
101001	Conny Balazs, KnowIT Fredrik Rasmusson, Västra Götalandsregionen	0.9	
120209	Fredrik Rasmusson Mikael Cavrak Magnus Svensson	1.0	
131028	Fredrik Rasmusson Mikael Cavrak	1.1	

1 Introduktion

1.1 Översikt

Denna certifikatpolicy beskriver de procedurer och rutiner som tillämpas vid utfärdande av certifikat för personer och funktioner inom Västra Götalandsregionens regionala PKI-hierarki, s.k. VGC.

Beskrivning av rutiner och organisationer för tillämpning av denna certifikatspolicy skall finnas i en separat Certification Practice Statement (CPS), publicerad av den eller de CA som tillämpar denna policy.

Om den eller de CA som tillämpar denna policy väljer att kontraktera Registration Authority (RA) för identifiering av nyckelinnehavare och insamling av egenskaper hos nyckelinnehavaren, skall denna RA arbeta enligt RA-policy och en av RA publicerad Registration Authority Practice Statement (RAPS) som beskriver rutiner och organisation för tillämpning av RA-policyn.

1.2 Identifiering

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 VGR CA Policy - Certifikatspolicy för utgivande av certifikat inom Västra Götalandsregionens interna PKI

Objektidentifierare (OID) för denna policy är 1.2.752.113.10.1.2.1.1.1

1.3 Målgrupp och tillämplighet

1.3.1 Policy Authority (PA)

Policy Authority äger är ytterst ansvarig för förvaltning av Västra Götalandsregionens interna PKI-hierarki samt dess tillhörande policys:

- CA-policy
- CPS
- RA-policy
- RAPS
- Certifikat profil för Västra Götalandsregionens interna PKI-hierarki

Policy Authority är ytterst ansvarig för samtliga identiteter (certifikat) som utfärdas ur Västra Götalandsregionens interna PKI-hierarki.

1.3.2 Certification Authority (CA)

CA skall publicera ett CPS som innehåller referens till denna certifikatpolicy. Organisation som ger ut certifikat enligt denna policy (CA) skall ha ett skriftligt överenskommelse från ägaren av Västra Götalandsregionens regionala PKI-hierarki på vilkens uppdrag certifikat utfärdas. Denna överenskommelse skall referera till den CPS som tilllämpas för att följa denna CA-policy.

CA är skyldig att inneha tillräckliga resurser i form av egna medel och försäkringar för att kunna fullgöra sina åtaganden enligt denna certifikatpolicy. CA är ansvarig för att upprätthålla samtliga tjänster inom ramarna för utfärdade certifikats livstid. Exempelvis ett certifikat som utfärdas med en giltighetstid på 10 år innebär att CA är skyldig att upprätthålla sina tjänster minst 10 år fram i tiden.

1.3.3 Registration Authorities (RA)

Samtliga anlitade RA skall arbeta efter RA-policy och en till denna policy knuten RAPS. RA skall garantera att man till fullo uppfyller samtliga berörda krav i denna certifikatpolicy.

1.3.4 Nyckelinnehavare (NI)

Slutanvändarcertifikat utfärdas till följande typer av nyckelinnehavare:

Typ av nyckelinnehavare	*Certifikatstyp*	*Certifikatsnivå*	*Förnyelse tillåten*
Adminstrationsroll IT-Infrastruktur	Person	Sekundärcertifikat	NEJ
OCSP Responder (Funktion)	Funktion	Primärcertifikat	JA
Tjänst Active Directory	Funktion	Primärcertifikat	JA
Klientdatorer IT-Infrastruktur	Funktion	Primärcertifikat	JA
Servrar IT-Infrastruktur	Funktion	Primärcertifikat	JA
Mobila enheter	Funktion	Primärcertifikat	JA
Tjänst MDM Mobila enheter	ServiceKonto	Primärcertifikat	JA
Tjänst NDES	Funktion	Primärcertifikat	JA

Tabell 1 - Se VGC Certificate Profile för detaljer

VGC certifikat utformas i enlighet med standarder för VGC som administreras av Västra Götalandsregionens ”Policy Authority”. Detta dokument benäms som Västra Götalandsregionens certifikatprofil.

1.3.5 Tillämplighet

Denna certifikatpolicy är relevant för CA, av CA kontrakterade RA, leverantörer av systemkomponenter, revisorer, förlitande parter (certikatbrukare) samt nyckelinnehavare certifierade i utfärdade certifikat.

Certifikat utgivna enligt denna certifikatpolicy kan identifiera följande olika användningsområden för det certifierade nyckelparet i enlighet med konventioner stipulerade i 6.1.9.

1. Elektroniska signaturer för användning i oavvislighetstjänster

2. Identifiering och autenticering

3. Konfidentialitetskryptering

Det ligger utanför CA: s kontroll att förhindra att privata nycklar används på ett otillbörligt sätt eller i strid med nyckelinnehavarens intentioner. Varje nyckelinnehavare måste uppmanas att endast använda privata nycklar i utrustning och applikationer som är trovärdiga och tillförlitliga i detta avseende samt att inte med den privata nyckeln signera data som inte i förväg granskats och godkänts av nyckelinnehavaren. Västra Götalandsregionen avsäger sig alla former av juridiskt ansvar för hur utfärdade certifikat brukas.

Korscertifikat som signerar CAs utanför Västra Götalandsregionens interna PKI-hierarki är ej tillåten av samtliga CAs som lyder under denna CA policy.

2 Allmänna villkor

2.1 Förpliktelser

2.1.1 Förpliktelser för CA

2.1.1.1 Generella förpliktelser

Utfärdande CA åtar sig att i enlighet med denna certifikatpolicy:

a) generera nycklar för primärcertifikat, då nycklar ej genereras av tillämpningen lokalt, enligt listan i stycke 1.3.4

b) utfärda certifikat enligt listan i stycke 1.3.4

c) bruka katalogtjänst för publisering av certifkat och tillhörande information i enlighet med avsnitt 2.6

d) utöva tillsyn enligt kapitel 4, 5 och 6

e) utföra identifiering enligt kapitel 3

f) informera nyckelinnehavare och förlitande parter vilka använder certifikat hur dessa får brukas

g) spärra certifikat och ge ut spärrlistor i enlighet med kapitel 4

h) uppfylla alla allmänna villkor i kapitel 2.

i) publisera driftrapport kvartalsvis som inbegriper tillgänglighet på CA-tjänster, antal utfärdade certifikat, avvikelser från normala driftförhållanden, planerade underhåll av CA-systemet samt redovisning av administrativa CA-roller. Denna rapport skall tillställas samtliga roller med revisionsansvar för Västra Götalandsregionens interna PKI.

2.1.1.2 Skydd av CA:s privata nyckel

Utfärdande CA förpliktar sig att skydda sina privata CA-nycklar i enlighet med denna certifikatpolicy.

2.1.1.3 Restriktioner gällande bruk av privat CA-nyckel

CA:s privata nycklar används enbart för att signera data enligt följande:

a) Signering av certifikat

b) Signering av spärrlistor

c) Signering av interna loggar och annan information som är relevant i samband med drift av CA-systemet

d) Signering av annan information som är intimt förknippat med CA:s roll som TTP, t ex vid tidsstämpling.

2.1.2 Förpliktelser för RA

2.1.2.1 Generella förpliktelser

Åtagandet i 2.1.1.1 från utfärdande CA:s sida gäller oavsett om det är RA organisationen eller annan, som på uppdrag av RA organisationen, utför tjänsterna.

2.1.2.2 Skydd av privat RA-nyckel

Åtagandet i 2.1.1 från utfärdande CA:s sida gäller oavsett om det är RA organisationen eller annan, som på uppdrag av RA organisationen, hanterar RA:s nycklar.

2.1.2.3 Restriktioner gällande bruk av privata nycklar

Åtagandet i 2.1.1 från utfärdande CA:s sida gäller oavsett om det är RA organisationen eller annan, som på uppdrag av RA organisationen, utför tjänsterna. RA anlitad av utfärdande CA förbinder sig, genom avtal med CA, att privata nycklar som används i samband med realisering av processer enligt denna certifikatpolicy inte används för något annat syfte.

2.1.3 Förpliktelser för nyckelinnehavare

2.1.3.1 Generella förpliktelser

Förpliktelser för nyckelinnehavare anges i den kvittens text som nyckelinnehavaren måste acceptera i samband med certifikat utfärdande. De förpliktelser som anges nedan finns med i de allmänna villkor som nyckelinnehavaren måste godkänna.

Vid ansökan om certifikat måste nyckelinnehavaren uppfylla sin del i de registrerings- och identifieringsprocesser som stipuleras i avsnitt 3 och 4 (SPC151).

2.1.3.2 Skydd av nyckelinnehavarens privata nyckel

Nyckelinnehavare förpliktar sig att skydda sin privata nyckel i enlighet med villkor accepterade av nyckelinnehavaren vid erhållandet av certifikatet.

Det åligger nyckelinnehavare att informera CA så fort minsta misstanke uppstår om att den privata nyckeln har blivit komprometterad.

2.1.3.3 Restriktioner gällande bruk av nyckelinnehavarens privata nyckel

Nyckelinnehavare ansvarar för att privata nycklar endast används i sådana sammanhang och utrustningar att man med fog inte kan förvänta sig att de privata nycklarna kan missbrukas.

I detta avseende skall applikationer vara av de typer som anges i 1.3.4.1.

2.1.4 Förpliktelser för förlitande part

2.1.4.1 Användning av certifikat för avsedda ändamål

Förlitande part skall säkerställa att han förlitar sig på uppgifterna i ett certifikat i den utsträckning som är lämpligt med hänsyn till transaktionens karaktär. Därvid skall förlitande part:

a) noga beakta de restriktioner i användningsområde som framgår av certifikatet eller av avtal mellan

utfärdande CA och förlitande part

b) bedöma om den allmänna säkerhetsnivå som framgår av denna certifikatpolicy är erforderlig med

hänsyn till riskerna som är förknippade med den aktuella transaktionen

c) i sin riskbedömning ta med de ansvarsfriskrivningar som framgår av denna certifikatpolicy eller avtal.

Förlitande part erinras särskilt om sitt ansvar för att i eget intresse försäkra sig om att privata nycklar associerade med utfärdade certifikat används i typer av applikationer enligt 1.3.4.1 samt att beakta eventuella konsekvenser av att detta inte efterlevs.

2.1.4.2 Verifieringsansvar

Det är förlitande parts eget ansvar att verifiera certifikat i enlighet med en lämplig certifieringskedja som utgår från en av den förlitande parten betrodd CA-nyckel.

2.1.4.3 Ansvar att kontrollera spärr och suspendering av certifikat

Det är förlitande parts eget ansvar att kontrollera ett certifikats giltighet i enlighet med 4.4.6 innan certifikatet används.

2.2 Ansvar

2.2.1 Ansvar för CA

2.2.1.1 Garantier och ansvarsbegränsningar

Utfärdande CA ansvarar inför alla som har rimlig anledning att förlita sig på uppgifterna i ett utfärdat certifikat, att denne i enlighet med denna certifikatpolicy kontrollerat att uppgifterna i utfärdade certifikat är korrekta.

2.2.1.2 Friskrivningar

Utfärdande CA ansvarar inte för skada på grund av att uppgifterna i ett certifikat eller en spärrlista är felaktiga, såvida utfärdande CA inte gjort sig skyldig till grov vårdslöshet.

2.2.2 Ansvar för RA

Utfärdande CA ansvarar för de tjänster som RA utför på CA:s uppdrag. Det åligger CA att i avtalet med RA återspegla det ansvar som CA har enligt denna policy.

2.3 Finansiellt ansvar

2.3.1 Fullmaktsförhållanden

CA, eller av CA anlitad RA, är fristående i förhållande till transaktionen mellan förlitande part och nyckelinnehavare. CA representerar således inte någon av parterna i deras transaktion.

2.4 Tolkning och verkställighet

2.4.1 Tillämplig lag

Västra Götalandsregionen avsäger sig alla former av juridiskt ansvar kopplade till de certifkkat som utfärdas ur den interna PKI-hierarkin, varvid tillämplig lag ej är applicerbart.

2.4.2 Procedurer för konfliktlösning

Västra Götalandsregionen avsäger sig alla former av juridiskt ansvar kopplade till de certifkkat som utfärdas ur den interna PKI-hierarkin, varvid tillämplig lag ej är applicerbart.

2.5 Avgifter

2.5.1 Avgifter för utfärdande ochcertifikat

Inga föreskrifter.

2.5.2 Avgifter för certifikatsåtkomst

Inga föreskrifter.

2.5.3 Avgifter för åtkomst till spärrlistor

Inga föreskrifter.

2.5.4 Avgifter för åtkomst till Policy och CPS

Inga föreskrifter.

2.6 Publicering och förvaringsplats

2.6.1 Publicering av CA-information

Det åligger utfärdande att CA att göra följande information publikt tillgänglig:

a) CPS som refererar till denna policy

b) spärrlistor med spärrade certifikat

c) utfärdade CA-certifikat, egensignerade CA-certifikat och korscertifikat för korscertifierade CA.

Varje publicerad spärrlista (CRL) tillhandahåller vid publiceringstillfället all tillgänglig spärrinformation för samtliga spärrade certifikat som spärrlistan är avsedd att förmedla.

Utfärdande CA tillhandahåller CA certifikat för samtliga publika CA-nycklar så länge dessa kan användas för verifiering av giltiga certifikat.

2.6.2 Åtkomstkontroll

Information som enligt denna certifikatpolicy publiceras via katalogtjänst tillhandahålls i enlighet med Västra Götalandsregionens bestämmelser.

2.7 Revision

Utfärdande CA ska genomföra löpande intern revision av att denna policy efterlevs. Vid revisionen ska speciellt följande undersökas:

a) CPS:ens lämplighet och överensstämmelse med denna policy

b) Jämförelse mellan CA:s interna rutiner och handböcker och denna policy

c) Avtal och annat som rör samverkan med RA.

Vid upptäckt av brister eller behov av förändringar skall CA vidta lämpliga åtgärder i form av att:

1. förändra tillämpade rutiner, och/eller uppdatera denna policy.

Om policy uppdateras på sådant sätt att den nya policyn bedöms medföra en förändrad säkerhetsgrad så skall en ny policy med en ny identitet upprättas (se 1.2).

Västra Götalandsregionens Policy Authority, SITHS RA samt Västra Götalandsregionens säkerhetsdirektör har mandat att vid givet tillfälle genomföra/låta genomföra revision enligt ovanstående.

2.8 Konfidentialitet

2.8.1 Typ av information som skall hållas konfidentiell

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

2.8.2 Typ av information som inte anses vara konfidentiell

Följande informationsobjekt anses inte vara konfidentiella:

a) utfärdade certifikat inklusive publika nycklar

b) spärrlistor

c) villkor för nyckelinnehavare eller

d) Certification Practice Statement, CPS

e) CA Policy

2.8.3 Tillhandahållande av information vid domstolsbeslut

Utfärdande CA tillhandahåller certifikatinformation i enlighet med tillämplig lag. Privata nycklar kopplade till utfärdade certifikat kan inte tillhandahållas då dessa inte får finnas sparade hos utfärdande CA.

2.9 Immateriella rättigheter

I enlighet med lagen om upphovsrätt får inga delar av denna policy, annat än enligt nedan angivna undantag, reproduceras, publiceras i ett databassystem eller skickas i någon form (elektroniskt, mekaniskt, fotokopierat, inspelat eller liknande) utan skriftligt medgivande från Västra Götalandsregionen.

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

Ansökan om tillstånd att på annat sätt reproducera och sprida delar av detta dokument kan göras hos Västra Götalands Policy Authority.

3 Identifiering och autenticering

3.1 Initial registrering

3.1.1 Namntyper

Nyckelinnehavare registreras med kontaktuppgifter samt identitetsuppgifter. Verifiering av personuppgifter genomförs vid varje ny beställning och uppdateras minst en gång årligen vid internt revisionsarbete.

3.1.1.1 VGC P Admin

Nedanstående attribut kan förekomma i ett VGC P Admin:

- Organisation
- AD Organisationsenhet
- Förnamn
- Efternamn
- HSA-ID
- Administrativ beteckning
- e-postadress (SMTP)
- UPN-namn

3.1.1.2 VGC F DC

Nedanstående attribut kan förekomma i ett VGC F DC:

- Organisation
- AD Organisationsenhet
- Administrativ beteckning
- DNS namn
- Domännamn

3.1.2 Krav på namns meningsfullhet

E-postadress kan endast utgöra SMTP-adress (RFC 822 namn).

Unik identifierare skall i de fall det är tillämpligt vara HSA-ID för aktuell identitet. Dess primära syfte är att tillhandahålla en fungerande unik identitet för informationssystem som inte kan tillämpa identiteter sammansatta av flera attribut, men det skall även säkerställa att två nyckelinnehavare inte certifieras med samma identitet.

Organisationsnamn skall alltid anges som Västra Götalandsregionen.

Organisationsenhet utgör godtycklig benämning på enhet eller gren av organisationen. Namn på organisationsenhet specificeras godtyckligt av ansvarig organisation som även ansvarar för att namnet är unikt inom organisationen.

Nyckelinnehavarens identitet kan specificeras av en godtycklig kombination av attributen i 3.1.1 så länge kombinationen innefattar obligatoriska attribut samt tillhandahåller en omisskännlig identitet. En omisskännlig identitet definieras här som en uppsättning attribut som på ett omisskännligt sätt relaterar till en specifik identitet.

3.1.3 Autenticering av organisationstillhörighet

Nyckelinnehavares organisationstillhörighet måste vara styrkt (auktoriserad) av en behörig representant för den aktuella organisationen. En auktorisation kan representera en eller flera nyckelinnehavare. Behörig representant, RA, arbetar enligt gällande RA-policy och specificerar att RA-organisationen är skyldig att rapportera relevanta förändringar i omständigheter av betydelse för beslut om spärr av certifikat.

3.1.4 Autenticering av personers identitet

Nyckelinnehavare för vilken behörig representant (arbetsgivare etc.) ansöker om certifikat identifieras vid beställningstillfället enligt 3.1.4.1 nedan.

Tjänsteman alternativt utsedd kontaktperson som godkänner ansökan gör en kontroll av att den ansökande uppfyller kraven för att kunna erhålla den typ av certifikat som ansökan avser. Godkännande av ansökan kan ske vid ansökningstillfället varvid kontrollanten anger hur beställaren identifieras och garanterar och loggar att identitetskontroll skett.

3.1.4.1 Krav på identitetskontroll

Identitetskontroll görs enligt någon av nedanstående procedurer.

a) Nyckelinnehavaren uppvisar godkänd och giltig legitimationshandling enligt definition i Västra Götalandsregionens rutinbeskrivning för utfärdande av SITHS-kort.
b) Nyckelinnehavaren uppvisar en godkänd och giltig inloggning mot en av Västra Götalandsregionen godkänd inloggningstjänst.

3.1.4.2 Procedur för autenticering

3.1.4.2.1 Procedur för autenticering mot VGR AD

Innan VGC certifikat skapas så kontrolleras samtliga nyckelinnehavarens identitetsuppgifter, som inte undantags nedan, mot VGR AD.

3.1.4.3 Krav på personlig närvaro

Elektronisk identitetskontroll vid beställning av VGC funtionsrelaterade certifikat kräver inte personlig närvaro av nyckelinnehavaren. Övrig identitetskontroll vid beställning kräver personlig närvaro.

3.1.5 Autenticering av funktioner inom organisationen

Vid beställning av VGC funtionsrelaterade certifikat, samt vid distribution av privata nycklar och koder kopplade till dessa, infordras en skriftlig beställning från en behörig representant för den aktuella organisationen. Denna beställning kan avse en eller flera nyckelinnehavare.

3.1.5.1 Autenticering av behörig representant

Vid utlämning av privata nycklar och koder sker identitetskontroll av behörig representant, motsvarande systemägare.

3.1.5.2 Krav på personlig närvaro

Elektronisk identitetskontroll vid beställning av VGC funtionsrelaterade certifikat kräver inte personlig närvaro av nyckelinnehavaren. Övrig identitetskontroll vid beställning kräver personlig närvaro.

3.1.5.3 Verifiering av rättighet till domän och certifikat

Initial beställning av organisation med dess rätt till domännamn, rätt till certifikat, rätt att beställa och mottaga certifikat skall alltid verifieras av oberoende källor. Resultat och verifieringens tillvägagångssätt skall dokumenteras och arkiveras.

3.2 Förnyad registrering vid förnyelse av nycklar

Förnyelser av VGC certifikat stöds i enlighet med stycke 1.3.4 i denna policy.

3.3 Förnyad registrering vid förnyelse av nycklar efter spärr

Vid förnyelse av nycklar efter spärr krävs alltid förnyad registrering.

3.4 Spärrbegäran

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 denna policy.

4 Operationella krav

4.1 Ansökan om certifikat

Vid ansökan fullföljs följande procedurer:

Vid personcertifikat: Skall föregås av en beställning från behörig representant för verksamheten. Nyckelinnehavaren ansvarar för att upp ge relevanta personliga uppgifter. Samtliga beställningar arkiveras av RA enligt 4.6.

Vid funktionscertifikat: Skall föregås av en beställning från behörig representant för verksamheten (systemägaren eller motsvarande). Nyckelinnehavaren ansvarar för att upp ge relevanta identitetsuppgifter. Samtliga beställningar arkiveras av RA enligt 4.6.

4.2 Utfärdande av certifikat

Utfärdandet av ett certifikat innebär CA:s acceptans av nyckelinnehavarens ansökan samt av de uppgifter som nyckelinnehavaren lämnat. Hantering av elektronisk registrering hos av CA utsedd RA sker i ett system och i en miljö som är väl integritetsskyddad samt följer rutiner som är avsedda att förhindra felaktig sammanblandning av identitetsuppgifter och nycklar.

Certifikat produceras efter det att ansvarig operatör hos CA eller RA personligen konstaterat att angivna beställningsrutiner och kontrollrutiner fullföljts.

4.2.1 Metod för att bevisa innehav av privat nyckel

Nyckelinnehavarens innehav av korrekt privat nyckel säkras genom någon av följande metoder:

1. Vid PKCS#10-requests styrker nyckelinnehavaren innehavet genom att korrekt använda nyckeln i ett för syftet lämpligt kontrollförfarande (vid utfärdande av VGC Person och VGC Funktion där nyckeln skapas hos nyckelinnehavaren).

2. Vid PKCS#12-requests genom att den privata nyckeln genereras av CA samt säkert skyddas och distribueras till ansvarig nyckelinnehavare (vid utfärdande av VGC Funktion där nyckeln skapas av CA).

4.3 Accepterande av certifikat

Procedurer för nyckelinnehavarens accepterande av det utfärdade certifikatet ska framgå av den RA-policy och den RAPS som tillämpas för Västra Götalandsregionens interna PKI-hierarki.

4.4 Spärr av certifikat

CA tillhandahåller en tjänst för spärr av certifikat. Spärrtjänsten är öppen dygnet runt. CA skapar löpande signerade listor över spärrade certifikat (CRL), varav den senaste lagras publikt tillgänglig i CA:s katalog. Spärrlistorna ska vara tillgängliga i en sådan omfattning att det är möjligt för en förlitande part att på ett säkert och effektivt sätt kontrollera ett certifikats giltighet. Aktuell spärrlista omfattar information om spärr för de certifikat som är associerade med spärrlistan, i enlighet med innehållet i CRL enligt X.509, version 2. Denna innefattar information om alla spärrade certifikat vars giltighetstid inte löpt ut.

Spärrkontroll genom on-line kontroll av ett certifikats giltighet kan också göras mot en OCSP-tjänst. Aktualiteten i denna tjänst skall vara densamma som spärrlistan. Vid spärr av person certifikat informeras nyckelinnehavaren.

4.4.1 Anledning till spärr

CA spärrar utfärdade certifikat i följande fall:

a) Vid ändring av någon av de uppgifter eller förhållande som certifieras i det utfärdade certifikatet
t.ex. ändring av namn eller anställningsförhållande.

b) Efter mottagande av spärrbegäran enligt 4.4.3.

c) Vid misstanke om att den privata nyckeln används av annan än dess rättmätige nyckelinnehavare eller på något annat sätt misstänks vara kompromitterad.

d) Vid misstanke om att det EID-kort eller motsvarande lagringsmodul som innehåller korresponderande privat nyckel inte längre innehas/kontrolleras eller inte längre kan brukas av rätt nyckelinnehavare.

e) Vid skälig misstanke om att nyckelinnehavaren bryter mot villkor enligt 2.10 eller att nyckelinnehavaren i sitt nyttjande av certifikat och privata nycklar bryter mot gällande rätt.

f) Om tillämpad CA-nyckel på något sätt misstänks vara kompromitterad.

g) Om CA beslutar upphöra med sin CA-verksamhet enligt 4.9.

Om CA spärrar certifikat tillföljd av a–e ovan på felaktiga grunder avsäger sig Västra Götalandsregionens policy authority, CA samt RA allt ansvar för eventuell påverkan på nyckelinnehavare.

4.4.2 Vem kan begära spärr hos CA

Spärrbegäran enligt 3.4 kan begäras av Policy authority, RA, behörig representant för RA, Verksamhetsansvarig, systemansvarig eller av nyckelinnehavare.

CA kan dock besluta om spärr som ett resultat av uppgifter som lämnats av annan part om detta utgör skälig grund för att misstänka att något av fallen enligt 4.4.1 föreligger.

4.4.3 Procedurer för spärrningsbegäran

En till CA kopplad tjänst tar emot begäran om spärrning. Spärrbegäran ska utföras av RA, eller behörig representant för RA.

Samtliga mottagna spärrbegäran arkiveras tillsammans med information om:

a) hur begäran inkom

b) vem som begärde spärr

c) när begäran inkom

d) anledning för spärr

4.4.4 Behandlingstid vid spärrbegäran

Relevant information om spärr publiceras i spärrlistan senast en timme efter beslut om spärr av ett certifikat. Beslut om spärr fattas normalt i direkt anslutning till mottagandet av spärrbegäran. Vid tveksamma fall kan dock beslut dröja tills RA sökt särskild bekräftelse av grund för spärr. Det finns ingen maximal tid för sådant agerande, dock åtar sig RA att oupphörligen arbeta aktivt med ärendet tills det är löst.

4.4.5 Utgivningsfrekvens för spärrlista

Alla spärrlistor utgivna inom ramen för denna certifikatpolicy uppdateras och publiceras så snart beslut om spärrbegäran fattats och spärr genomförts, dock minst en gång varje timme dygnet runt.

Funktionen att uppdatera och publicera spärrlistor kan vid service och systemfel vara otillgänglig under en begränsad tid, vid sådana fall har policy authority samt CA ett ansvar att lösa dessa problem enligt bästa förmåga. Vid situationer där spärrlistan ej är tillgänglig för förlitande part kan spärrcheck ej utföras, effekten av detta är beroende av hur aktuell tillämpning nyttjar spärrlistan.

4.4.6 Krav på kontroll mot spärrlista

Det är förlitande parts eget ansvar att kontrollera verifierade certifikat mot senast utgivna spärrlista.

Vid kontroll av spärrlista skall förlitande part försäkra sig om att:

a) certifikat kontrolleras mot en spärrlista som representerar den senaste aktuella spärrinformationen för certifikatet i fråga

b) spärrlistan fortfarande är giltig, dvs. att dess giltighetstid inte löpt ut

c) spärrlistans signatur är giltig

4.4.7 Möjlighet till kontroll av spärrlistor och certifikatsstatus

Som ett alternativ till spärrlistor kan on-line transaktioner för kontroll av ett certifikats giltighet och status användas. Beskrivning av procedurer för detta skall framgå av CPS:en.

4.5 Procedurer för säkerhetsrevision av CA-systemet

I detta avsnitt specificeras procedurer för loggning av händelser samt därtill relaterad revision av säkerhet i CA-systemet på systemnivå och operativsystemnivå.

4.5.1 Typ av loggade händelser

I och runt CA-systemet loggas minst följande händelser:

a) Skapande av användarkonton samt förädring av kontons behörigheter

b) Initiering av operationer på operativsystemsnivå av systemanvändare med uppgift om vem som begärde operationen, typ av operation, samt indikering av resultat av initieringen

c) Installation och uppdatering av mjukvara

d) Relevant information om säkerhetskopior

e) Start och avstängning av systemet

f) Tid och datum för alla hårdvaruuppgraderingar

g) Tid, datum och ansvarig för säkerhetskopiering och tömning av loggar

h) Tid, datum och ansvarig för säkerhetskopiering och tömning av arkivdata (enligt 4.6)

i) Tillgänglighet av spärrlista samt eventuella spärrtjänster, kontroll av tillgänglighet sker var 30:e sekund

4.5.2 Frekvens för bearbetning av logg

Loggar skall analyseras minst kvartalsvis av auktoriserad personal för upptäckt av obehöriga aktiviteter.

4.5.3 Bevaringstid för logg

Loggar enligt 4.5.1 bevaras i minst 1 år löpande.

4.5.4 Skydd av logg

Loggar skyddas mot otillbörlig förändring dels genom de logiska skyddsmekanismerna i operativsystemet samt dels genom att systemet i sig inte är fysiskt och logiskt åtkomligt annat än för behörig personal.

Alla loggposter är individuellt tidsstämplade. Loggarna verifieras och konsolideras minst en gång per kvartal under överinseende av minst två i förväg utsedda CA-operatörer med relevant kompetens.

4.5.5 Procedurer för säkerhetskopiering av logg

En kopia av CA:s konsoliderade auditlogg lagras i fysiskt säkrade utrymmen på fysiskt skild plats från CA.

Loggarna lagras på sådant sätt att de vid allvarlig misstanke om oegentligheter kan tas fram och göras läsbara för granskning under den angivna lagringstiden.

4.5.6 System för insamling av revisionsinformation

System för insamling av loggar enligt detta avsnitt hanterar enbart intern logginformation skapad i det centrala systemet för certifikatproduktion (CA).

4.6 Arkivering

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

4.6.1 Typ av arkiverad information

Följande information arkiveras löpande:

a) Transaktioner innehållande begäran om certifikatproduktion och spärr av certifikat från behörig operatör.

b) Ansökningshandlingar undertecknade av ansökande uppdragsgivare samt av personer ansvariga för att ta emot och acceptera ansökan.

c) Undertecknade mottagningskvittenser vid utlämning av nycklar och koder.

d) Utgivna certifikat samt därtill relaterade uppdateringar av katalog.

e) Historik rörande tidigare CA-nycklar, nyckelidentifierare samt korscertifikat mellan olika generationer av CA-nycklar.

f) Begäran om spärr samt därtill relaterade uppgifter inkomna till spärrtjänsten.

g) Utgivna spärrlistor samt därtill relaterade uppdateringar av CA:s katalog.

h) Resultat av revision av CA:s uppfyllelse av denna certifikatpolicy.

i) Gällande villkor och kontrakt (i alla tillämpade versioner).

j) Denna certifikatpolicy samt alla tidigare tillämpade versioner av denna certifikatpolicy.

k) Tillgänglighetsdata för spärrlista samt eventuella spärrtjänster

I de fall den arkiverade informationen utgörs av en digitalt signerad informationsmängd så arkiveras även nödvändig information som krävs för verifiering av signaturen under angiven arkiveringstid.

4.6.2 Bevaringstid för arkiv

All arkiverad information enligt 4.6.1 bevaras i minst 1 år löpande.

4.6.3 Procedurer för att nå och verifiera arkivmaterial

Arkiverat material som är klassat som konfidentiellt enligt 2.8.1 är inte tillgängligt för externa parter i sin helhet annat än vad som krävs genom lag och beslut i domstol.

Utlämning av enstaka uppgifter rörande en specifik nyckelinnehavare eller transaktion kan göras efter individuell prövning av Västra Götalandsregionens säkerhetsdirektör.

Arkiven lagras under sådana förhållanden att de förblir läsbara för granskning under den angivna lagringstiden.

Av den händelse att procedurer för tillgång till arkivmaterial förändras förorsakat av att CA upphör med sin verksamhet, så kommer information om procedur för fortsatt tillgång till arkivmaterial att tillhandahållas av CA genom underrättelseprocedurer enligt 4.9.

4.7 Byte av CA-nyckel

Ny CA-nyckel skapas minst sex månader före den tidpunkt då tidigare CA-nyckel upphör att användas för utfärdande av nya certifikat. Rutiner för detta skall finnas tillgängliga inom CA:s operatörsorganisation.

Vid byte av CA-nyckel sker följande:

a) nytt certifikat utfärdas för den nya publika CA-nyckeln,

b) korscertifikat utfärdas där den gamla CA-nyckeln signeras med den nya CA-nyckeln,

c) korscertifikat utfärdas där den nya CA-nyckeln signeras med den gamla CA-nyckeln och

d) certifikaten enligt a–c publiceras i relevant katalog

4.8 Planering för kompromettering och katastrof

4.8.1 Kompromettering

CA åtar sig att, vid misstanke om att CA inte längre äger fullständig och exklusiv kontroll över den privata CA-nyckeln, vidta följande åtgärder:

a) Upphöra med alla spärrkontrolltjänster rörande certifikat utgivna med den komprometterade nyckeln samt alla spärrkontrolltjänster som signeras med den komprometterade nyckeln eller av nyckel som certifierats med den komprometterade nyckeln. Detta innebär att alla associerade spärrlistor plockas bort från sina anvisade platser. Detta sker i samråd med Västra Götalandsregions IT-incidentledning, vilka har mandat att besluta huruvida upphörning av spärrkontrolltjänster skall ske eller ej.

b) Informera alla nyckelinnehavare, och alla parter som CA har en relation med, att CA-nyckeln är komprometterad och hur nytt CA-certifikat kan hämtas. Nyckelinnehavare finns i register enligt 4.6.1.

c) I det fall CA har korscertifierat den komprometterade CA-nyckeln med en annan operativ CA-nyckel, spärra sådana korscertifikat.

d) Sörja för att spärrinformation finns tillgänglig för certifikat enligt c) fram tills dess att de spärrade certifikatens giltighetstid löpt ut.

4.8.1.1 Nyckelinnehavare

Nyckelinnehavare informeras om att omedelbart upphöra med användning av privata nycklar som är associerat med certifikat utfärdade med den komprometterade CA-nyckeln.

Nyckelinnehavarna informeras om hur dessa skall förfara för att erhålla ersättningscertifikat och eventuellt även nya privata nycklar, samt under vilka förutsättningar gamla privata nycklar kan användas i samband med andra certifikat som inte är utfärdade med den kompromitterade CA-nyckeln.

4.8.1.2 Förlitande part och korscertifierande CA

Information kommer att göras tillgänglig för förlitande parter och för korscertifierande CA som klart informerar att berörda certifikat samt CA:ns utfärdarnyckel är spärrade från användning. Förlitande part och andra korscertifierande CA agerar utanför CA:s inflytande. Dessa erhåller genom CA:s hantering av spärrlistor den information som krävs för att de skall kunna agera på ett korrekt sätt.

4.8.2 Katastrofplaner

En katastrofsituation kan uppstå vid ett avbrott i verksamheten eller genom att sekretessbelagda uppgifter blir åtkomliga för obehöriga. Likaså kan brister i riktigheten i informationen medföra att felaktiga beslut tas som leder till skada för Västra Götalandsregionen.

CA ansvarar för att upprätta och förvalta processer för risk- och sårbarhetsanalyser, riskreduceringar och åtgärdsarbeten. Lämpliga områden att fokusera på kan vara: planer för katastrofhantering, tester av katastrofplaner, återstartsrutiner (gradvis, mellansnabb och omedelbar), automatisk felövervakning och genomförande av säkerhetsuppgraderingar. Test av att CA-systemet kan återstartas från säkerhetskopior ska genomföras med 1 års intervall.

Katastrof- och avbrottsplaner skall upprättas och bestå av framtagna rutiner som täcker de återstarts- och reservåtgärder för datadriften som vidtas inom ramen för ordinarie drift, så att CA-systemet ska kunna återstartas inom fastställd tid. Fokusområden bör minst vara kring risker med strömavbrott, översvämningar, brand, andra naturkatastrofer, terrorism, administrativa misstag och tekniska fel.

Datamedia och säkerhetskopior av dessa förvaras i olika brandceller eller särskilt utformade förvaringsutrymmen.

4.9 Upphörande av CA

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

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

b) Öppet informera om att verksamheten upphör minst tre månader i förväg.

c) Upphöra med alla spärrkontrolltjänster efter det att samtliga utgivna certifkats livstid har gått ut.

Detta innebär att alla associerade spärrlistor plockas bort från sina anvisade platser och att inga nya spärrlistor utfärdas som ersättning för de som plockats bort.

d) Avsluta alla rättigheter för underleverantörer att agera i den upphörande CA:s namn.

e) Sörja för att alla arkiv och loggar bevaras under angiven bevaringstid samt i enlighet med angivna föreskrifter.

Det åligger CA att inneha garantier för medel som täcker kostnaderna för åtgärderna a–e under föreskriven tid.

5 Fysisk, procedurorienterad och personalorienterad säkerhet

5.1 Fysisk säkerhet

Fysisk säkerhet syftar till att skydda CA:s lokaler, utrustning och informationskapital. Fysisk säkerhet omfattar naturkatastrofer, olyckor och fel i tekniska system samt mänskliga misstag och slarv eller kriminella handlingar. Målen med fysisk säkerhet skall vara att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information. Målen skall sättas i rimlig proportion till förekommande risker. Fysiskt tillträde inkluderar även fjärransluten konsolåtkomst till CA-servrar utan certifikatinloggning.

CA ansvarar för skydd av säkrade utrymmen som skalskydd, brand- och vattenskydd, lokaler med tillträdeskontroll och rutiner för arbetet i säkrade utrymmen.

CA ansvarar för skydd av utrustning, tekniska försörjningssystem, t ex elförsörjning och UPS. CA ansvarar för skydd kring avveckling och återanvändning av utrustning, t ex lagringsmedia som innehåller känslig information.

5.1.1 Anläggningens läge 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

Detaljerad information av säkerhetsprocedurer för fysiskt tillträde är av säkerhetsskäl inte publikt tillgänglig. Lokalernas externa skydd så som lås och larmanordningar kontrolleras regelbundet av datahallsansvariga inom Västra Götalandsregionen.

5.1.3 Lagring av media

Frånsett datorhall enligt 5.1.1 finns en annan, fristående skyddad, lokal för lagring av säkerhetskopior och viktiga handlingar. I denna lokal finns särskilda individuellt låsbara skåp för förvaring av olika typer av loggar och arkiv. Säkerhetsklassning för säkerhetskopior följer säkerhetsklassificeringen som gäller för originalinformationen.

5.1.4 Fysisk säkerhet för RA

Några RA funktioner som innefattar roller enligt 5.2.1 kan förekomma utanför den skyddade centrala fysiska miljön enligt 5.1.1. De är:

1. Identifiering av nyckelinnehavare vid ansökan med personlig närvaro.

2. Utlämning av nycklar och koder för VGC Person.

3. Elektronisk registrering av nyckelinnehavare.

Funktion enligt punkt 1 och 2 innebär ingen åtkomst till CA-systemet. Dessa funktioner har därför inga särskilda säkerhetsföreskrifter vad avser fysisk säkerhet.

Funktioner enligt punkt 3 utförs i låsbart utrymme i kontorsmiljö. Inga nycklar eller koder lämnas utan tillsyn. Operatörskort som ger åtkomst till operativa roller i CA-systemet är personliga och lämnas inte kvar då operatören lämnar lokalen. Lokalen innefattar även låsbara skåp för förvaring av arkivmaterial.

5.2 Procedurorienterad säkerhet

CA ansvarar i enlighet med 2.1.1. för alla procedurer och förhållanden som definieras i detta avsnitt. Detta innefattar allt från certifikatproduktion och logistik till administration av hela processen.

5.2.1 Betrodda roller

5.2.1.1 Betrodda roller inom CA

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

Certification Authority Administrator (CAA) Administrativ produktions-/driftspersonal för CA:n.

Typiska uppgifter som kan administreras av CAA är:

- Skapa certifikat
- Generera nycklar
- Generera spärrlista
- Kontroll av certifikatutfärdarloggen
- Ändra konfiguration av aktuell CA

System Administrator (SA) Teknisk produktions-/driftspersonal för CA:n.

Typiska uppgifter som kan administreras av SA är:

- Installationer
- Systemunderhåll
- Byte av media med säkerhetskopior

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

Information Systems Security Officer (ISSO) Säkerhetsansvarig för CA-tjänsten.

ISSO är inte själva direkt involverade i processen att generera certifikat, kort och spärrlistor, men ansvarar för att alla operativa roller agerar inom ramen för sina befogenheter.

5.2.1.2 Betrodda roller inom RA

Operatörer inom en RA-organisation besitter enbart roller anpassade efter RA:s arbetsuppgifter. Dessa roller specificeras i gällande RA-policy.

5.2.2 Krav på antal personer per uppgift

Rollerna enligt 5.2.1.1 tillsätts av minst en person vardera. Person som innehar roll som ISSO eller CAA innehar inte samtidigt någon annan av dessa roller.

Initiering av CA-systemet samt generering och initiering av CA-nycklar kräver närvaro av minst en person som innehar ISSO samt en person som innehar CAA roll.

Övriga krav på närvaro av personer vid utförande av olika arbetsuppgifter redovisas under berörda avsnitt.

5.2.3 Identifiering och autenticering av varje roll

Identifiering av roller i CA-systemet sker enligt följande:

- Identifiering av rollerna SA sker i operativsystemet i CA-systemets enheter.
- Identifiering av rollerna CAA (där så är tillämpligt) sker i CA-systemets applikationer och baseras på stark autenticering med hjälp av personliga operatörskort. Det enda undantaget mot det är vid installation av CA-systemet då då identifiering av CAA sker i operativsystemet.

5.3 Personalorienterad säkerhet

5.3.1 Bakgrund, kvalifikationer, erfarenhet och tillståndskrav

Roller enligt 5.2.1.1 tilldelas endast särskilt utvalda och pålitliga personer som uppvisat lämplighet för en sådan befattning. Dessa personer får inte inneha annan roll som kan bedömas stå i konflikt med den tilldelade rollen.

Identifiering och bakgrundskontroll av ansvarig personal är betydande. Personal skall kontinuerligt uppvisa tillräckliga kunskaper i grundläggande PKI-teknik. Kunskaperna skall kunna omsättas i såväl praktik som teori och genomföras på en tillräckligt hög nivå.

En bakgrundskontroll av tilltänkt CA personal skall genomföras innan CA roll får tilldelas. Kontroll skall ske gentemot säkerhetsskyddslagen enligt säkerhetsklass 3. Övriga lämpliga kontroller kan vara: tidigare anställningar samt högsta och adekvata utbildningsreferenser som anges i rollansökan.

5.3.2 Krav på utbildning

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.

5.3.3 Personalorienterad säkerhet för RA

Ansvarig personal hos RA utses inom den organisation som är utsedd att utföra tilldelade arbetsuppgifter. Om sådan roll utses av underleverantör till CA så ansvarar denna även för att lämplig personalkontroll utförs.

RA personal som tilldelats roll i CA-systemet uppfyller samma krav som för motsvarande CA-personal vad avser lämplighet och utbildning.

6 Teknikorienterad säkerhet

6.1 Generering och installation av nyckelpar

6.1.1 Generering av nyckelpar

Nedan angivna krav för generering av nycklar avser endast de nycklar som skapas av CA. Nycklar som skapas av CA genereras utifrån ett slumptal. Processen att generera slumptal, som bas för nyckelgenerering, är slumpmässig på så sätt att det är beräkningsmässigt ogörligt att återskapa ett genererat slumptal, oavsett mängden kunskap om genereringsprocessens beskaffenhet eller vid vilken tidpunkt eller med hjälp av vilken utrustning slumptalet skapades.

Nyckelgenereringsprocessen är så beskaffad att ingen information om nycklarna hanteras utanför nyckelgeneringssystemet annat än genom säker överföring till avsedd förvaringsplats.

Nycklarnas unicitet uppnås genom att nycklarna är slumpmässigt genererade och av sådan längd att sannolikheten för att två identiska nycklar genereras är försumbar.

6.1.1.1 Specifika krav rörande CA:s utfärdarnycklar

Generering av CA:s privata utfärdarnycklar sker i den datorenhet där nycklarna sedan används. De privata nycklarna skyddas i mjukvara som minst motsvarar säkerhetskraven enligt Västra Götalandsregionens säkerhetspolicy. Denna datorenhet skyddas fysiskt enligt avsnitt 5.1.

6.1.1.2 Specifika krav rörande privata nycklar för nyckelinnehavare

Centralt genererade nycklar genereras i en fristående arbetsstation och lagras på lämplig lagringsmodul och raderas därefter från arbetsstationens arbetsminne.

6.1.2 Leverans av centralt genererade privata nycklar till nyckelinnehavare

Efter produktion levereras nycklar på portabelt media via personlig närvaro till aktuell nyckelinnehavare. PIN-kod för att låsa upp innehållet på det portabla mediat skickas via krypterad e-post i Västra Götalandsregionens e-postsystem till aktuell nyckelinnehavare.

Mottagande av nycklar kvitteras. Kvittensen arkiveras i minst certifikatets giltighetstid plus 5 år.

6.1.3 Leverans av publik nyckel till CA

Överföring av publika nycklar från nyckelinnehavare till CA sker endast vid begäran om sekundärcertifikat, dvs. då ett VGC Person ska utfärdas eller då nyckelpar på annat sätt genereras av nyckelinnehavaren. Den publika nyckeln verifieras oberoende av hur den levereras genom ett för ändamålet särskilt protokoll, eller mot uppvisandet av ett certifikat som minst motsvarar säkerhetsnivån enligt denna policy, som intygar nyckelinnehavarens association med nyckeln. Vid automatiskt utfärdade certfikat agerar giltig inloggning mot VGR AD som intyg för identitet samt nyckelinnehavares association med aktuell nyckel.

6.1.4 Leverans av CA:s publika nycklar till nyckelinnehavare och förlitande parter

Förlitande part ansvarar för att hämta korrekta och gällande versioner av CA:s publika nycklar. CA-certifikat kan hämtas från CA:s katalog (VGR AD).

6.1.5 Nyckelstorlekar

CA:s nycklar genereras med minst 2048 (Subordinate CA) respektive 4096 (root CA) bitars längd. Övriga nycklar genereras med minst 1024 bitars längd.

6.1.6 Generering av publika nyckelparametrar

Nyckelinnehavares nycklar som i certifikaten markeras med användningsområdena kryptering och autenticering ges publika exponenter som förhindrar kända attacker.

Nyckelinnehavares nycklar som i certifikaten markeras med användningsområdet avsett för verifiering av oavvisliga digitala dokument ges publika exponenter som förhindrar kända attacker.

CA:s nycklar ges publika exponenter som förhindrar kända attacker.

Det förutsätts att CA håller sig ajour med teknikutvecklingen inom kryptoteknikområdet och anpassar sina kryptoalgoritmer i enlighet de senaste rönen.

6.1.7 Kontroll av kvalitet på nyckelparametrar

Nycklarnas kvalitet säkras dels genom krav på slumptalsgenerering enligt 6.1.1.

6.1.8 Generering av nycklar i hårdvara/mjukvara

Nycklar genereras med mjukvara.

6.1.9 Användningsområde för nycklar

Utgivna certifikat innehåller information som definierar tillämpligt användningsområde för certifikatet och dess associerade nycklar. Markering av användningsområde sker i enlighet med X.509 version 3.

Certifikat utgivna i enlighet med denna certifikatpolicy kan omfatta följande användningsområden:

a) Identifiering och Autenticering

b) Konfidentialitetskryptering

c) Verifiering av elektroniska signaturer i samband med oavvislighetstjänster

Användningsområde a) och b) representeras av samma certifikat. Användningsområde c) representeras av ett särskilt certifikat som inte kan användas för a) eller b).

Om användningsområdet c) finns markerat i ett certifikat så har detta innebörden att certifikatet och dess associerade nycklar endast får användas i oavvislighetstjänster.

För personliga inloggning/autentisering skall endast certifikat lagrade på smarta kort användas, certifikat lagrade i mjukvara accepteras ej för personliga inloggningar.

6.2 Skydd av privat nyckel

Procedurerna enligt denna certifikatpolicy vad avser generering, förvaring och distribution av privata nycklar har som syfte att till största möjliga grad borga för att privata nycklar skyddas på ett sådant sätt att de inte kan falla i orätta händer samt, vad avser nyckelinnehavares privata nycklar, att de inte i något fall exponeras eller brukas på otillbörligt sätt, innan de nått rätt mottagare.

6.2.1 Standard för kryptografisk modul

CA:s signeringsnyckel används och skyddas i en särskild datorenhet och skyddas i mjukvara som minst motsvarar säkerhetskraven enligt FIPS 140-2, nivå 1, som är inlåst i ett säkerhetsskåp och i sin tur förvaras inom det skalskyddade område som definieras i 5.1.

Nyckelinnehavares privata nycklar kan inneslutas och skyddas på två olika sätt.

1. Hårdvaruskyddade nycklar som nyckelinnehavaren erhållit i samband med ansökan om andra certifikat, och som minst motsvarar säkerhetsnivån i denna policy, skall skyddas i hårdvara som minst motsvarar säkerhetskrav enligt FIPS 140-2, nivå 3.

2. Mjukvaruskyddade privata nycklar som genererats av CA eller av ansökande part enligt denna policy skall skyddas lägst motsvarande säkerhetskrav enligt FIPS 140-2, nivå 1.

Mjukvaruskyddade nycklar skall lagras i krypterad form med säkerhetsnivå som gör det beräkningsmässigt ogörligt att forcera kryptoskyddet genom logiska attacker. Nycklar för dekryptering av skyddade privata nycklar skall skyddas mot obehörig åtkomst på ett sätt som skapar ett skydd mot missbruk som motsvarar hårdvaruskyddade nycklar. Nyckelinnehavare skall för detta ändamål använda av CA godkända metoder och verktyg. Dock gäller för lokalt genererade mjukvaruskyddade nycklar att det är nyckelinnehavaren som helt på egen hand ansvarar för att tillfredsställande säkerhet uppnås i användarens lokala miljö.

6.2.2 Säkerhetskopiering av privata nycklar

Säkerhetskopia skall tas av CA:s privata nyckel. Hantering av säkerhetskopian omgärdas av motsvarande regler för åtkomstskydd som gäller för originalet. Säkerhetskopian får ej arkiveras för annat syfte än som backuprutin ur ett driftperspektiv. Arkivering av säkerhetskopia för CA:s privata nyckel hos extern tredjepart är ej tillåten.

6.2.3 Arkivering av privata nycklar

Inga centralt genererade nycklar för nyckelinnehavare eller för RA får arkiveras av CA. CA:s privata nycklar får ej arkiveras.

6.2.4 Metod för förstörande av privat nyckel

CA:s privata utfärdarnycklar förstörs då deras användningstid löpt ut. Säkerhetskopior förstörs genom att använt lagringsmedium raderas. För operativa nycklar som lagras i utfärdarsystemets hårddisk i krypterad form, gäller följande:

1. Om utrustningen skall användas vidare i samma skyddade miljö sker överskrivning på sådant sätt att dessa nycklar ej kan återvinnas.

2. Om utrustningen skall användas utanför den skyddade zonen eller säljas skall det säkerställas att ingen information kan återskapas eller läsas ut från aktuella hårddiskar.

6.3 Andra aspekter på hantering av nyckelpar

Inga privata nycklar eller annan konfidentiell information inom CA och RA får lämna sin föreskrivna skyddsmiljö. Vid service och liknande situationer då föreskrivna skyddsmetoder inte kan upprätthållas avlägsnas alternativt förstörs alla lagringsmedia som innehåller känslig information eller känsliga privata utfärdarnycklar.

6.3.1 Användningsområde för publika och privata nycklar

Certifikat utfärdade enligt denna certifikatpolicy utfärdas dels för nya nycklar och dels för befintliga nycklar som certifierats tidigare i samband med att nycklarna genererades. Certifikat för nyproducerade nycklar ges maximalt en giltighetstid på fem år. Certifikat för existerande nycklar ges maximalt en giltighetstid fram till dess att ursprungscertifikatets giltighetstid löper ut.

Certifikat som används av personal vid drift av CA-systemet ges maximalt en giltighetstid på 12 månader.

Självsignerade CA-certifikat ges en giltighetstid som maximalt täcker tiden från genereringstillfället fram till och med den tidpunkt som associerad privat nyckel upphör att användas för signering av certifikat och spärrlistor.

Korscertifikat mellan olika generationer av CA nycklar ges maximalt en giltighetstid på fem år plus en överlappningstid på maximalt sex månader (Den tid innan nyckelbytet som den nya nyckeln samt korscertifikat för gamla nyckeln finns tillgänglig för uppdatering).

6.4 Säkerhet i datorsystem

Hela CA-systemet skall vara uppbyggt på ett sådant sätt att individuella roller enligt 5.2 kan separeras.

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

6.5 Säkring av levnadscykel

6.5.1 Säkring av systemutveckling

CA-systemets mjukvara skall utvecklas/uppdateras av tillverkare som använder en kontrollerad utvecklingsmiljö med ett väl dokumenterat kvalitetssäkringssystem.

6.5.2 Säkring av säkerhetsadministration

Driftsdokumentation som i detalj dokumenterar hur roller och behörigheter skall tillämpas och vidmakthållas, skall finnas.

6.6 Säkring av nätverk

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

Informationsutväxling mellan RA och CA skall vara krypterad och transaktioner som påverkar användningen av CA:s privata utfärdarnycklar skall vara individuellt signerade.

Alla kommunikationsportar i CA-systemet som inte behövs skall vara deaktiverade och tillhörande mjukvarurutiner som inte används skall vara blockerade.

7 Certifikat och CRL-profiler

7.1 Formatversioner och profiler för certifikat

VGC certifikat utformas i enlighet med standarder för VGC som administreras av Västra Götalandsregionens ”Policy Authority”. Detta dokument benäms som Västra Götalandsregionens certifikatprofil.

8 Specifikationsadministration

8.1 Procedurer för specifikationsförändringar

Västra Götalandsregionens ”Policy Authority” kan ändra i denna publikation under iakttagande av följande grundprinciper:

Ändring som kan ske utan underrättelse:

- De ändringar som kan företas i denna CA-policy utan underrättelse är språkliga justeringar och omdisponeringar som inte påverkar säkerhetsnivån i beskrivna procedurer och regelverk.

Ändring som skall ske med underrättelse:

- Förändring som bedöms innebära en märkbar försämring av säkerhetsnivå skall resultera i en ny publikation som ges en ny identitet (Policyobjektidentifierare enligt 1.2). På så vis kan certifikat utfärdade efter nya regler särskiljas från certifikat utfärdade efter tidigare gällande regler.

9 Refererande dokument

Västra Götalandsregionens Certifikatprofil

Västra Götalandsregionens Certificate Practise Statment

Västra Götalandsregionens RA Policy för intern PKI

Västra Götalandsregionens RAPS för intern PKI

BILAGA A - Definitioner

Applikation: IT-tjänst eller IT-tillämpning.

Asymmetrisk krypteringsalgoritm: En krypteringsteknik som utnyttjar två relaterade transformeringsalgoritmer, en publik transformering, med användande av en publik nyckel, och en privat transformering med användande av en privat nyckel. De två transformeringarna har den egenskapen att om man känner den publika transformeringen är det matematiskt omöjligt att ur denna härleda den privata transformeringen.

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

Bascertifikat: Se primärcertifikat.

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

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

CA: Organisation 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.

CA-certifikat: Certifikat som certifierar att en viss publik nyckel är publik nyckel för en specifik CA.

Certification Authority: Se CA.

Certification Practice Statement: Se CPS.

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

Certifikatextensioner: Del av certifikatinnehåll specificerat av standarden X.509 version 3.

Certifikatskedja: Kedja med certifikat där delarna i kedjan är CA-certifikat för CA som korscertifierat

varandra. Vid verifiering av ett certifikat, följs kedjan tills en betrodd CA hittats.

Certifikatsnivå: Det finns certifikat på två nivåer, primärcertifikat och sekundärcertifikat.

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

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.

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

Elektronisk identitetskontroll: Identitetskontroll som kan göras utan att den, vars identitet kontrolleras, är personligen närvarande.

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

Förlitande part: En mottagare av ett certifikat som förlitar sig på detta certifikat vid autenticering, verifiering av digitala signaturer och/eller kryptering av information.

Katalogtjänst: Databastjänst som i detta dokument avser en databas som struktureras enligt standarden X.500.

Korscertifiering: Processen där en CA utfärdar ett certifikat för en annan CA:s publika CA-nyckel.

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.

Kryptografisk modul: En enhet i vilken krypteringsnycklar lagras tillsammans med en processor som kan utföra kritiska kryptografiska algoritmer. Exempel på kryptografisk modul är EID-kort och diskett.

Lagringsmodul: I detta dokument avses kryptografisk modul.

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.

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

Oavvislighetstjänster: Tjänster vars syfte är att binda en nyckelinnehavare vid ansvar för signerade meddelanden på ett sådant sätt att det kan verifieras av en tredje part vid senare tidpunkt.

Omisskännlig identitet: En identitet bestående av en uppsättning attribut som på ett omisskännligt sätt relaterar till en specifik person. Den omisskännliga kopplingen mellan identiteten och personen kan vara beroende på sammanhang inom vilka identitetsbegreppen hanteras. Vissa av dessa sammanhang kan kräva hjälp från aktuell registerhållare av olika attribut.

Operatör: Anställd hos CA.

Policy: I detta dokument synonymt med certifikatpolicy.

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 privata 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.

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

RA-policy: En namngiven uppsättning regler för RA:s roll i framställning, utgivning och spärr 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.

RSA: Namn på en specifik asymmetrisk krypteringsalgoritm för kryptering med publika och privata nycklar, uppkallad efter matematikerna Rivest, Shamir och Adleman.

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.

Spärr: 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 använder samma hemliga nyckel både för kryptering och dekryptering.

Tillförlitlig tredje part: Se TTP.

TTP: En part som två eller flera samverkande parter litar på. En TTP utför tjänster åt de samverkande parterna, såsom t ex tidsstämpling, certifikatsutgivning.

Uppdragsgivare: Den organisation inom hälso- och sjukvården som genom avtal ger i uppdrag till en CA att utfärda certifikat för organisationens anställda, vårdgivare som arbetar på organisationens uppdrag samt 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.

BILAGA B - Förkortningar

CA Certification Authority*
CAA Certification Authority Administrator
CPS Certification Practice Statement*
CRL Certificate Revocation List, på svenska spärrlista*
EID Elektroniskt ID-kort*
VGC Västragötalandscertifikat
IETF Internet Engineering Task Force
ISO International Organization for Standardization
ISSO Information Systems Security Officer
OID Object Identifier
PIN Personal Identification Number
PKI Public Key Infrastructure
PKCS Public Key Cryptography Standards
PKIX Public Key Infrastructure (x.509) (IETF Working Group)

RA Registration Authority*
RAPS Registration Authority Practice Statement*
RFC Request For Comments
RSA Rivest – Shamir – Adleman, asymmetrisk krypteringsalgoritm*
SA System Administrator
SMTP Simple Mail Transfer Protocol
SO Security Officer
TTP Tillförlitlig tredje part eller Trusted Third Party*
*se också definitionerna ovan