CERTIFIERINGSPRAXIS

För Myndigheten för digitalisering och befolkningsdatas rotcertifikat

OID: 1.2.246.517.1.10.301
OID: 1.2.246.517.1.10.351
OID: 1.2.246.517.1.10.201

13.9.2024

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio (VA), Jari Pirinen (JP)
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v. 1.0	Version 1.0	1.6.2021/VA
v 1.1	Uppdaterade versionen och länkarna till CPS dokument	29.9.2022/SK
v 1.3	Uppdaterade datumet och versionen till 1.3 för att vara i linje med de andra samtidigt uppdaterade rotpolicydokumenten. Specificerade spärrlistans typ till CRL och/eller ARL i styckena 1.3.1, 2.1.2 och 2.5.3. Raderade omnämnande av Medborgarcertifikat i styckena 1.1, 1.3.4 och 2.1.2. Ändrade ‘omedelbart’ till ‘utan fördröjelse’ i styckena 4.4.1 och 4.4.4.	15.9.2023/JP
v 1.4	Uppdaterade versionen och datumet. Förenade politikerna för G3- och G2-rotcertifikathierarkierna till ett och samma dokument. Lade till force majeure till stycke 2.2.5. Ändrade termen ’publik nyckel’ till ’offentlig nyckel’. Ändrade termen ’kvalitetscertifikat’ till ’kvalificerade certifikat’ i stycke 6.1.1.	13.9.2024/JP

Innehållsförteckning

1 Inledning 10
1.1 Allmänt 11
1.2 Identifikationsuppgifter 15
1.3 Rotcertifikatutfärdaren och tillämpningsområdena för certifikatutfärdarens certifikat 16
1.3.1 Rotcertifikatutfärdare 16
1.3.2 Registrerare 16
1.3.3 Registertjänst 17
1.3.4 Organisation som innehar certifikatutfärdarens certifikat 17
1.3.5 Förlitande på certifikatutfärdarens certifikat 17
1.3.6 Användning av certifikatutfärdarens certifikat 17
1.4 Kontaktuppgifter 17
1.4.1 Organisation som administrerar certifieringspraxisen 17
1.4.2 Kontaktperson 17
2 Allmänna villkor 18
2.1 Skyldigheter 18
2.1.1 Rotcertifikatutfärdarens skyldigheter 18
2.1.2 Skyldigheter som gäller den organisation som innehar certifikatutfärdarens certifikat 19
2.1.3 Skyldigheter hos den part som förlitar sig på certifikatutfärdarens certifikat 19
2.1.4 Skyldigheter som gäller publiceringen av certifikatutfärdarens certifikat 20
2.2 Ansvar 20
2.2.1 Rotcertifikatutfärdarens ansvar 20
2.2.2 Registrerarens ansvar 21
2.2.3 Ansvar för den organisation som innehar certifikatutfärdarens certifikat 21
2.2.4 Ansvaret hos den part som förlitar sig på certifikatutfärdarens certifikat 21
2.2.5 Begränsning av ansvar 21
2.3 Ekonomiskt ansvar 22
2.3.1 Rotcertifikatutfärdare 22
2.3.2 Övriga parter 22
2.3.3 Rotcertifikatutfärdarens ekonomiförvaltning 22
2.4 Tolkning och verkställighet 23
2.4.1 Lagstiftning som tillämpas 23
2.4.2 Avgörande av meningsskiljaktigheter 23
2.5 Avgifter 23

2.5.1 Utfärdande och förnyande av certifikatutfärdarens certifikat ... 23
2.5.2 Avgifter för användning av certifikatutfärdarens certifikat ... 24
2.5.3 Avgifter för registrering av certifikatutfärdarens certifikat på spärrlistan ... 24
2.6 Publikation av och tillgång till information ... 24
2.6.1 Publicering av information om certifikatutfärdarens certifikat ... 24
2.6.2 Publikationsfrekvens ... 24
2.6.3 Uppgifternas tillgänglighet ... 24
2.6.4 Dataförvaring ... 24
2.7 Dataskyddsgranskning ... 25
2.7.1 Granskningsfrekvens ... 25
2.7.2 Granskare ... 25
2.7.3 Föremål för granskningen och granskningens omfattning ... 25
2.7.4 Åtgärder vid avvikelser ... 26
2.7.5 Information om resultatet av granskningen ... 26
2.8 Publicering av information ... 27
2.8.1 Uppgifter publicerade av rotcertifikatutfärdaren ... 27
2.8.2 Offentlig information ... 27
2.8.3 Information om att giltighetstiden för certifikatutfärdarens certifikat har gått ut eller avbrutits 27
2.8.4 Information som lämnas ut till myndigheter ... 27
2.8.5 Övrig information ... 27
2.8.6 Övriga principer gällande utlämnande av information ... 27
2.9 Immaterialrättigheter ... 28
3 Identifiering av den som söker certifikatutfärdarens certifikat ... 28
3.1 Registrering ... 28
3.1.1 Benämningspraxis ... 28
3.1.2 Leverans av privata nycklar till innehavaren av certifikatutfärdarens certifikat ... 29
3.2 Förnyelse av nyckelpar ... 29
3.3 Identifiering av den som begär spärrning ... 29
4 Funktionella krav ... 29
4.1 Ansökan om certifikatutfärdarens certifikat ... 29
4.2 Utfärdande av certifikatutfärdarens certifikat ... 30
4.3 Mottagande av certifikatutfärdarens certifikat ... 30
4.4 Giltighetstiden hos certifikatutfärdarens certifikat och spärrning av det ... 30
4.4.1 Förutsättningar för spärrning av certifikatutfärdarens certifikat ... 30
4.4.2 Genomförandet av spärrningen ... 30

4.4.3 Spärrhändelsen 30
4.4.4 Tidpunkten för en spärrhändelse 31
4.4.5 Tillfälligt avbrytande av giltighetstiden för certifikatutfärdarens certifikat 31
4.4.6 Publiceringsfrekvens för spärrlista 31
4.4.7 Krav i anslutning till kontroll av spärrlistor 31
4.4.8 Kontroll av certifikatutfärdarens certifikat i realtid 32
4.4.9 Särskilda krav i en situation där den privata nyckeln för innehavaren av certifikatutfärdarens certifikat har röjts 32
4.5 Övervakningen av systemet 32
4.6 Arkivering av data i anslutning till certifikatutfärdarens certifikat 32
4.6.1 Material som arkiveras 32
4.6.2 Skydd av arkiv 33
4.6.3 Säkerhetsförfaranden för arkiverat material 33
4.6.4 Metoder för införskaffning och tryggande av arkiverat material 33
4.7 Hantering av kontinuerlig verksamhet och undantagsfall 33
4.7.1 Rotcertifikatutfärdarens privata nyckel har röjts eller rotcertifikatutfärdarens certifikatet har spärrats 33
4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof 34
4.8 Upphörande av rotcertifikatutfärdarens verksamhet 34
5 Fysiska krav, funktionella krav och krav på personalens säkerhet 34
5.1 Arrangemang i anslutning till den fysiska säkerheten 35
5.1.1 Läge och lokalernas egenskaper 35
5.1.2 Fysisk tillgång till verksamhetslokalen 35
5.1.3 Elmatning och ventilation 35
5.1.4 Brandsäkerhet 35
5.1.5 Lagring av information 35
5.1.6 Hantering av onödigt informationsmaterial 35
5.1.7 Vattenskador 36
5.2 Funktionella krav 36
5.2.1 Ansvarsfördelning 36
5.2.2 Antalet personer som krävs för olika uppgifter 36
5.2.3 Uppgiftsspecifik identifiering 36
5.3 Personsäkerhet 37
5.3.1 Utredning av personalens bakgrund 37
5.3.2 Förfarande vid utförande av bakgrundskontroll 37
5.3.3 Krav på utbildning 38
5.3.4 Underhåll av expertis och kompetens 38

5.3.5 Krav på uppgiftsrotation 38
5.3.6 Åtgärder vid avvikelser 38
5.3.7 Personal som representerar organisationen 38
5.3.8 Handlingar som tillhandahålls personalen 38
6 Tekniska säkerhetsarrangemang 38
6.1 Skapa och lagra nyckelpar 38
6.1.1 Skapa nyckelpar 38
6.1.2 Överlämnande av en privat nyckel till den som ansöker om certifikatutfärdarens certifikat 39
6.1.3 Leverans av den öppna nyckel som den som ansöker om certifikatutfärdarens certifikat skapat till rotcertifikatutfärdaren 39
6.1.4 Distribution av rotcertifikatutfärdarens öppna nyckel till innehavaren av certifikatutfärdarens certifikat 39
6.1.5 Längden på nycklar 39
6.1.6 Nycklarnas användningsändamål 39
6.2 Skydd av hemlig nyckel 40
6.2.1 Standarder som gäller säkerhetsmodulen 40
6.2.2 Personal som medverkar i behandlingen av rotcertifikatutfärdarens privata nyckel .. 40
6.2.3 Överlåtelse av hemlig nyckel till betrodd part 40
6.2.4 Säkerhetskopia av hemlig nyckel 40
6.2.5 Arkivering av privat nyckel 40
6.2.6 Administrering av privat nyckel i kryptografiska moduler 40
6.3 Övriga omständigheter i anslutning till nyckeladministration 41
6.3.1 Arkivering av öppen nyckel 41
6.3.2 Användningstiden för öppna och hemliga nycklar 41
6.4 Säkerhetskrav i anslutning till användningen av och åtkomsten till datorer 41
6.4.1 Utrustningens säkerhet 41
6.5 Hantering av certifikatsystemets livscykel 41
6.5.1 Övervakning av systemutvecklingen 41
6.5.2 Hantering av säkerhet 42
6.6 Säkerheten i datanätet 42
6.7 Övervakningen av användningen av kryptiska moduler 42
7 Utfärdarens profiler för certifikat och spärrlistor 42
7.1 Tekniska uppgifter om certifikat 42
7.2 Spärrlistprofil 42
8 Hantering av dokument innehållande bestämmelser 43
8.1 Ändring av bestämmelser 43

8.2 Publicering och information 43
8.3 Förfarande för ändring och godkännande av certifieringspraxis 43

CERTIFIERINGSPRAXIS

Definitioner och förkortningar

Definitioner

Aktiveringsuppgift: Konfidentiell uppgift som utöver RSA-nyckeln behövs för användning av kryptografiska moduler (till exempel baskod och signeringskod).

Nyckelpar: Nycklar som används tillsammans inom ett öppet nyckelssystem, varav den ena är offentlig och den andra privat. Ändamålet med nycklarna har fastställts på certifikatet (se certifikatinnehavarens signeringscertifikat samt autentiserings- och krypteringscertifikat).

Icke-symmetrisk kryptering: Vid icke-symmetrisk kryptering används ett nyckelpar med en offentlig och en privat nyckel. Ett meddelande som krypterats med offentlig nyckel kan endast öppnas med den privata nyckeln i nyckelparet i fråga.

Offentlig nyckel: Den offentliga delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatutfärdaren bekräftar med sin digitala signatur att den offentliga nyckeln innehas av certifikatets innehavare. Den offentliga nyckeln är en del av certifikatets datainnehåll.

Öppet nyckelsystem: Infrastruktur för informationssäkerheten där informationssäkerhetstjänster produceras med ett system med öppen nyckel.

Öppet nyckelsystem: Informationssäkerhetstjänst, exempelvis elektronisk identifiering av personer, som produceras med hjälp av öppna och privata nycklar, certifikat och asymmetrisk kryptering.

Rotcertifikatutfärdare: Organisation som utfärdar utfärdarens certifikat och utarbetar en certifikatpolicy och en certifieringspraxis som beskriver verksamheten. Myndigheten för digitalisering och befolkningsdata är den rotcertifikatutfärdare som avses i denna certifieringspraxis.

Förlitande part: Aktör (relying party, luottava taho) som litar på certifikatets uppgifter och som använder det för olika säkerhetstjänster såsom autentisering och för att bekräfta konfidentialiteten eller att en signatur är riktig i situationer där utfärdarens signatur i anslutning till certifikatet stämmer.

OID: Object Identifier, identifierande kod Certifieringspraxisens entydiga kod OID är en del av datainnehållet i varje certifikatutfärdares certifikat som beviljats av rotcertifikatutfärdaren.

PDS: PKI Disclosure Statement, certifikatbeskrivning I dokumentet beskrivs i stora drag de centrala delområdena av certifikatutfärdarens verksamhet.

RSA-algoritm: Algoritm för öppen nyckel, asymmetrisk algoritm.

Registrerare: Registreraren identifierar i enlighet med den certifikatsökandes certifikatpolicy och certifieringspraxis på uppdrag av rotcertifikatutfärdaren.

Spärrlista: En lista på certifikat som spärrats under deras giltighetstid. Ett certifikat som införts på en spärrlista kan inte aktiveras för användning på nytt. (Authority Revocation List, ARL eller Certificate Revocation List, CRL).

Certifikat: Ett elektroniskt intyg som kopplar uppgifterna om verifieringen av en signatur till den som gjort signaturen och bekräftar signeraren.

Certifikatsystem: Ett informationstekniskt system för att skapa certifikat och underteckna spärrlistor.

Certifikatbeskrivning: Dokumentet innehåller de centrala delarna av certifikatpolicyn och certifieringspraxisen.

Certifikatpolicy (CP): Ett dokument som beskriver hur rotcertifikatutfärdaren utfärdar utfärdarens certifikat. I dokumentet behandlas dessutom bl.a. olika parters ansvar. Certifikatpolicyn ska finnas offentligt tillgänglig.

Certifikatregister: Ett register som är förenligt med lagen om stark autentisering och betrodda elektroniska tjänster och som den certifikatutfärdare som erbjuder tjänster för allmänheten är skyldig att föra i utsatt tid.

Certifieringspraxis (CPS): En närmare beskrivning av hur rotcertifikatutfärdaren förverkligar sin certifikatpolicy.

Utfärdarens privata nyckel: En hemlig nyckel som används för signering av utfärdarens certifikat och spärrlistor.

Certifikatutfärdare: Organisationen som beviljar certifikat, som svarar för produktionen av certifikat samt utarbetar certifikatpolicy och certifieringspraxis som beskriver organisationens verksamhet.

Certifikatutfärdarens certifikat: Certifikat (CA) utfärdat av rotcertifikatutfärdaren. Certifikatet innehåller den öppna nyckeln som motsvarar utfärdarens privata nyckel. Med hjälp av detta kontrolleras att utfärdarens elektroniska signatur är äkta.

Certifikatsökande: En organisation som ansöker om certifikat och som identifieras i samband med ansökan.

Innehavare av certifikat: En organisation vars öppna nyckel har certifierats med rotcertifikatutfärdarens privata nyckel och vars identifieringsuppgifter ingår i certifikatutfärdarens certifikat.

Användning och användningssyfte för certifikat: I detta dokument avses med användning av certifikat såväl användning av själva certifikatet som användning av medföljande nycklar. Exempelvis avses med användning av certifikat vid digital signering såväl användning av den privata nyckeln vid signeringen som användning av den offentliga nyckeln och certifikatet vid autentisering av signatur.

Förkortningar

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practise Statement
CRL	Certificate Revocation List
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HST	Elektronisk identifiering av en person
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Control
OCSP	Online Certificate Status Protocol, standard för verifiering av certifikatstatus i realtid över internet
OID	Object Identifier
PDS beskrivning	PKI Disclosure Statement, certifikat-
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identity Module
MDB	Myndigheten för digitalisering och befolkningsdata

1 Inledning

Certifieringspraxisen är en beskrivning av förfaringssätt och verksamhetsprinciper som efterlevs vid beviljande av certifikat, som utarbetas av utfärdaren. Certifieringspraxis är en mer detaljerad beskrivning av utfärdarens verksamhet.

Den här certifieringspraxisen tillämpas på Myndigheten för digitalisering och befolkningsdatas certifikat för rotcertifikatutfärdaren DVV GOV. Root CA – G3 RSA, DVV Gov. Root CA – G3 ECC och VRK Gov. Root CA – G2.

Om myndighetens namnbyte har stadgats i lagen om Myndigheten för digitalisering och befolkningsdata (304/2019). Befolkningsregistercentralens namn ändrar 1.1.2020 till Myndigheten för digitalisering och befolkningsdata.

1.1 Allmänt

Myndigheten för digitalisering och befolkningsdatas datasystem för certifiering och certifikattjänsterna grundar sig på en struktur med öppen nyckel (Public Key Infrastructure, dvs. PKI). MDB:s infrastruktur för certifikat består av ett certifikatsystem, en leverantör för certifikatuppgifter som ingår i kort, en spärrlista, en rådgivningstjänst och en registertjänst. I egenskap av certifikatutfärdare har MDB till uppgift att producera certifikat-, register- och spärrtjänster, sköta registrering samt tillverka och individualisera kort som innehåller certifikat. MDB ansvarar för att hela certifikatsystemet fungerar, också när det gäller de registrerare och tekniska leverantörer som MDB anlitar.

Myndigheten för digitalisering och befolkningsdata utarbetar en separat certifikatpolicy för varje certifikattyp som utfärdas liksom en certifieringspraxis för varje tekniskt underlag. Certifikatpolicyn beskriver separat för varje certifikattyp vilka förfaranden som ska iakttas, ansvarsfördelningen och andra aspekter på användningen av certifikat på ett allmänt plan. Certifieringspraxisen ger en detaljerad beskrivning av förfaringssätten. Varje dokument har en egen individualiserande OID-kod. Dessa dokument finns elektroniskt tillgängliga på adressen https://dvv.fi/sv/certifikatpolicydokument.

Myndigheten för digitalisering och befolkningsdatas certifikatverksamhet baserar sig på Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen).

Myndigheten för digitalisering och befolkningsdatas betrodda tjänster uppfyller förutom karven i eIDAS-förordningen även kraven i standard EN 319 401 om kvalificerade tillhandahållare av betrodda tjänster och i standard EN 319 411-1 om kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller certifikat.

De certifikat som utfärdats av Myndigheten för digitalisering och befolkningsdata är elektroniska signaturer enligt lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och verktyg för stark autentisering. MDB beviljar även andra person- och programcertifikat i samma system som förlitar sig på certifikatutfärdaren.

Myndigheten för digitalisering och befolkningsdata har en hierarkisk förtroendemodell: Myndigheten för digitalisering och befolkningsdata har en rotcertifikatutfärdare som utfärdar certifikat för andra utfärdare. Utfärdaren kan antingen vara Myndigheten för digitalisering och befolkningsdata eller någon annan offentlig eller privat organisation.

Myndigheten för digitalisering och befolkningsdata övergick till ett nytt certifikatsystem 14.12.2017. Myndigheten för digitalisering och befolkningsdata har en hierarkisk förtroendemodell: Myndigheten för digitalisering och befolkningsdata har en rotcertifikatutfärdare som utfärdar certifikat för andra utfärdare. Utfärdaren kan antingen vara

Myndigheten för digitalisering och befolkningsdata eller någon annan offentlig eller privat organisation.

Det här dokumentet beskriver den praxis som rotcertifikatutfärdaren efterföljer vid utfärdandet av ett certifikat för en certifikatutfärdare som utfärdar certifikat. Rotcertifikatutfärdaren utfärdar inte slutanvändarnas certifikat: var och en av dessa har en egen certifikatpolicy och en egen certifieringspraxis.

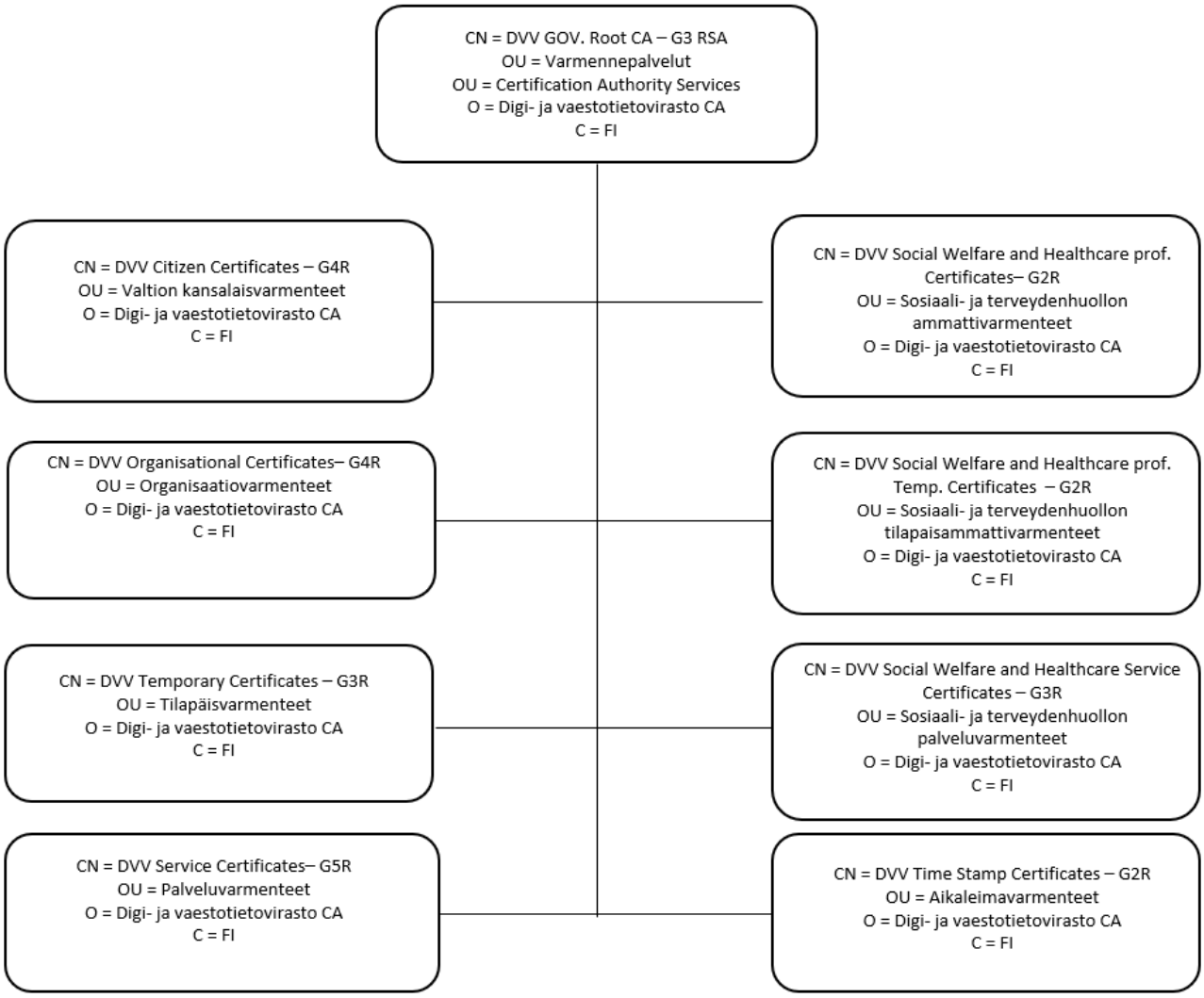

Bild 1: Certifikathierarkin DVV Gov. Root CA – G3 RSA

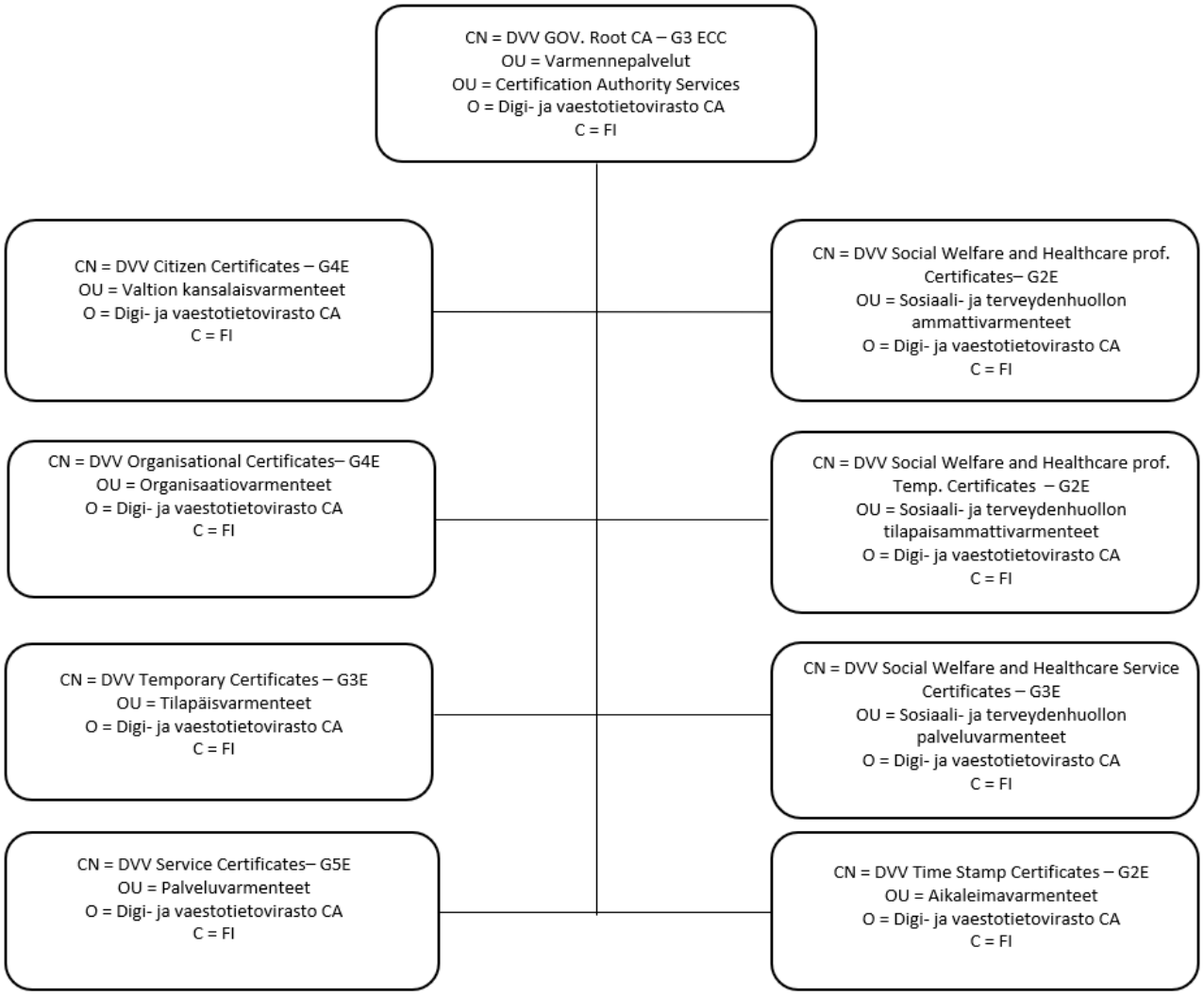

Bild 2: Certifikathierarkin DVV Gov. Root CA – G3 ECC

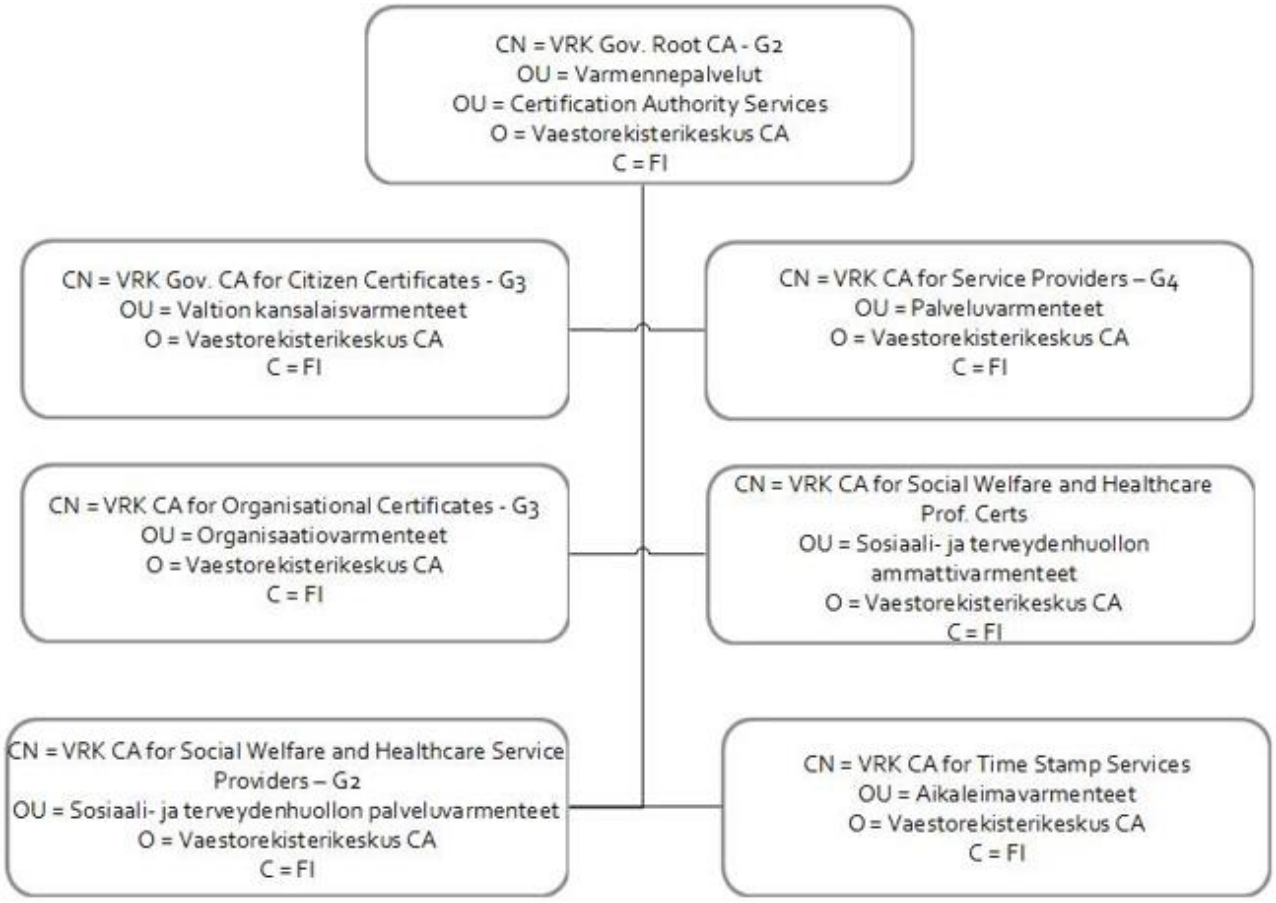

Bild 3: Certifikathierarkin VRK Gov. Root CA – G2

Certifikatutfärdarens certifikat innehåller utfärdarens öppna nyckel, namn, certifikatets användningssyfte , giltighetstid samt de övriga uppgifter som behövs för användningen av certifikatet. Certifikatets uppgifter har signeras digitalt med rotcertifikatutfärdarens privata nyckel. Certifikatutfärdarens certifikat som är förenligt med denna certifieringspraxisen grundar sig på systemet med öppen nyckel.

Alla certifikat liksom spärrlistorna signeras elektroniskt med den privata nyckel som motsvarar den öppna nyckeln i certifikatutfärdarens certifikat. Med hjälp av rotcertifikatet kan den förlitande parten verifiera äktheten och integriteten hos ett certifikat.

Myndigheten för digitalisering och befolkningsdatas dokument över certifikatpolicyer och certifieringspraxis identifieras med specifika koder (OID).

Myndigheten för digitalisering och befolkningsdata gör upp en separat certifikatpolicy för rotcertifikatutfärdare samt separat certifieringspraxis för varje certifikat för utfärdare som utfärdats av rotcertifikatutfärdaren. Certifikatpolicyerna beskriver separat för varje certifikattyp vilka förfaranden som ska iakttas i utfärdarens certifikatverksamhet, användningsvillkoren, ansvarsfördelningen och andra aspekter på användningen av certifikat på ett allmänt plan. Certifieringspraxisen ger en detaljerad beskrivning av förfaringssätten.

1.2 Identifikationsuppgifter

Namnet på den här certifieringspraxisen är certifieringspraxis för Myndigheten för digitalisering och befolkningsdatas rotcertifikat

och det hänvisar till certifieringspraxisen för följande undercertifikat:

DVV Citizen Certificates - G4R, OID: 1.2.246.517.1.10.301.1

DVV Citizen Certificates - G4E, OID: 1.2.246.517.1.10.351.1

DVV Organisational Certificates - G4R, OID: 1.2.246.517.1.10.301.2

DVV Organisational Certificates - G4E, OID: 1.2.246.517.1.10.351.2

DVV Temporary Certificates - G3R, OID: 1.2.246.517.1.10.301.3

DVV Temporary Certificates - G3E, OID: 1.2.246.517.1.10.351.3

DVV Service Certificates - G5R, OID: 1.2.246.517.1.10.301.4

DVV Service Certificates - G5E, OID: 1.2.246.517.1.10.351.4

DVV Social Welfare and Healthcare Prof. Certificates - G2R, OID: 1.2.246.517.1.10.301.5

DVV Social Welfare and Healthcare Prof. Certificates - G2E, OID: 1.2.246.517.1.10.351.8

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R, OID: 1.2.246.517.1.10.301.6

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E, OID: 1.2.246.517.1.10.351.6

DVV Social Welfare and Healthcare Service Certificates - G3R, OID: 1.2.246.517.1.10.301.7

DVV Social Welfare and Healthcare Service Certificates - G3E, OID: 1.2.246.517.1.10.351.7

DVV Time Stamp Certificates - G2R, OID: 1.2.246.517.1.10.301.8

DVV Time Stamp Certificates - G2E, OID: 1.2.246.517.1.10.351.8

VRK Gov. CA for Citizen Certificates - G3, OID: 1.2.246.517.1.10.201.1

VRK CA for Organisational Certificates - G3, OID: 1.2.246.517.1.10.201.2

VRK CA for Temporary Certificates - G2, OID: 1.2.246.517.1.10.201.3

VRK CA for Service Providers - G4, OID: 1.2.246.517.1.10.201.4

VRK CA for Social Welfare and Healthcare Prof. Certs, OID: 1.2.246.517.1.10.201.5

VRK CA for Social Welfare and Healthcare Prof. Temp. Certs, OID: 1.2.246.517.1.10.201.6

VRK CA for Social Welfare and Healthcare Service Providers – G2, OID: 1.2.246.517.1.10.201.7

VRK CA for Time Stamp Services, OID: 1.2.246.517.1.10.201.8

Denna certifieringspraxis hänvisar till Myndigheten för digitalisering och befolkningsdatas policy för rotcertifikatutfärdare, OID 1.2.246.517.1.10.301, 1.2.246.517.1.10.351 och 1.2.246.517.1.10.201.

Såväl certifikatpolicyn som certifieringspraxisen finns på https://dvv.fi/sv/certifikatpolicydokument.

1.3 Rotcertifikatutfärdaren och tillämpningsområdena för certifikatutfärdarens certifikat

Rotcertifikatutfärdaren tillhandahåller certifikattjänster på villkor som föreskrivs i denna certifieringspraxis och ansvarar för att de fungerar enligt rotcertifikatutfärdarens ansvar som beskrivs i kapitel 2.2.1. Rotcertifikatutfärdaren ansvarar för att hela certifikatsystemet fungerar, också när det gäller de registrerare och tekniska leverantörer som den anlitar. Denna certifieringspraxis har registrerats av Myndigheten för digitalisering och befolkningsdata som även är innehavaren av certifikatutfärdarens certifikat enligt denna certifieringspraxis.

Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralen till uppgift att producera certifikattjänster för elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdatas certifikattjänst indelas i följande delfunktioner:

1.3.1 Rotcertifikatutfärdare

Rotcertifikatutfärdarens uppgift är:

- att utfärda certifikatutfärdarens certifikat.
- att se till att datainnehållet i certifikaten är felfria
- att tillhandahålla certifikat- och registertjänster och spärrtjänster i enlighet med certifikatpolicyn och certifieringspraxisen
- att sörja för spärrning av certifikatutfärdarens certifikat och publicering av spärrlistor för certifikatutfärdarens certifikat (CRL och/eller ARL).

1.3.2 Registrerare

Rotcertifikatutfärdaren ansvarar för alla registreringsuppgifter för certifikatutfärdarens certifikat.

- Registreraren identifierar certifikatsökanden på det sätt som beskrivs i certifieringspraxisen.

1.3.3 Registertjänst

Registertjänsten är en offentlig webbtjänst som innehåller samtliga utfärdarcertifikat som rotcertifikatutfärdaren utfärdat samt den senaste spärrlistan. Registertjänsten finns på ldap://ldap.fineid.fi.

1.3.4 Organisation som innehar certifikatutfärdarens certifikat

Certifikatutfärdarens certifikat enligt denna certifieringspraxis har beviljats till Myndigheten för digitalisering och befolkningsdata för beviljande av certifikat.

Certifikatinnehavarens organisation bör iaktta rotcertifikatutfärdarens certifikatpolicy och certifieringspraxis.

1.3.5 Förlitande på certifikatutfärdarens certifikat

En förlitande part är en person eller en organisation som litar på innehållet i certifikatutfärdarens certifikat och som använder rotcertifikatutfärdarens certifikat för autentisering, kryptering av information och för elektroniska signaturer i certifikatutfärdarens certifikat. En förlitande part ska kontrollera att det certifikat som används är i kraft och att det inte tagits upp på spärrlistan.

1.3.6 Användning av certifikatutfärdarens certifikat

Användningssyften för certifikatutfärdarens certifikat enligt denna certifieringspraxis är: signering av certifikatutfärdarens certifikat och signering av spärrlistan.

Certifikatpolicyn och certifieringspraxisen innehåller krav som gäller skyldigheterna för rotcertifikatutfärdaren, registreraren, innehavaren av utfärdarcertifikatet och den förlitande parten samt frågor som gäller lagstiftning och lösning av eventuella konflikter.

1.4 Kontaktuppgifter

1.4.1 Organisation som administrerar certifieringspraxisen

Denna certifieringspraxis är registrerad av Myndigheten för digitalisering och befolkningsdata. Den svarar för administrationen och uppdateringen av denna certifieringspraxis.

Upphovsrätterna i enlighet med denna certifieringspraxis tillhör Myndigheten för digitalisering och befolkningsdata.

1.4.2 Kontaktperson

Förfrågningar om certifieringspraxisen kan riktas till följande adress:

Myndigheten för digitalisering och befolkningsdata

PB 123 (Fågelviksgränden 2)
00531 Helsingfors
FO-nummer: 0245437-2

Tfn +358 295 535 001
Fax +358 9 876 4369
kirjaamo@dvv.fi

Myndigheten för digitalisering och befolkningsdatas registratorskontor svarar på frågor om certifikatpolicyn på e-postadressen kirjaamo@dvv.fi.

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2 Allmänna villkor

Certifieringspraxisen träder i kraft vid datumet som nämns på framsidan. Förfaringssättet för att göra ändringar i och publicera certifieringspraxisen beskrivs i kapitel 8 i detta dokument.

2.1 Skyldigheter

2.1.1 Rotcertifikatutfärdarens skyldigheter

- Rotcertifikatutfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Rotcertifikatutfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Rotcertifikatutfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser samt möjlighet att täcka eventuella krav på skadestånd.
- Rotcertifikatutfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer och personer som rotcertifikatutfärdaren anlitar.
- Rotcertifikatutfärdaren utarbetar och upprätthåller en certifikatpolicy som beskriver förfaringssätt, användarvillkor och ansvarsfördelning vid utfärdandet, underhållet och administrationen av certifikatutfärdarens certifikat samt övriga aspekter på användningen av certifikatutfärdarens certifikat på ett allmänt plan.
- Rotcertifikatutfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur rotcertifikatutfärdaren tillämpar certifikatpolicyn.
- Rotcertifikatutfärdaren uppfyller kraven enligt certifikatpolicyn och certifieringspraxisen.

- Rotcertifikatutfärdaren publicerar certifikatpolicyn och certifieringspraxisen och gör dem allmänt tillgängliga.
- Rotcertifikatutfärdaren anställer tillräckligt med personal med den expertis, erfarenhet och kompetens som fordras för produktionen av certifikattjänster.
- Rotcertifikatutfärdaren använder pålitliga system och produkter som är skyddade från otillbörlig användning.
- Rotcertifikatutfärdaren tillhandahåller offentligt information om rotcertifikat och certifikatverksamheten, utgående från vilken rotcertifikatutfärdarens verksamhet och pålitlighet kan bedömas.
- Rotcertifikatutfärdaren efterföljer certifikatpolicyn och certifieringspraxisen i registreringen.
- Rotcertifikatutfärdaren identifierar tillförlitligt den organisation som ansöker om certifikatutfärdarens certifikat på det sätt som beskrivs i certifieringspraxis så att den sökandes uppgifter noggrant granskas.
- Rotcertifikatutfärdaren ser till att uppgifterna hanteras omsorgsfullt och konfidentiellt.

2.1.2 Skyldigheter som gäller den organisation som innehar certifikatutfärdarens certifikat

- Användningssyftet för certifikatutfärdarens certifikat är: att signera certifikat och att signera spärrlistan. Ett certifikat får användas enbart i avsett syfte.
- Den organisation som är innehavare av certifikatutfärdarens certifikat ansvarar för att de uppgifter som uppges i ansökan är korrekta.
- Den organisation som är innehavare av certifikatutfärdarens certifikat ska förvara sin privata nyckel i en säker miljö och förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.
- Innehavarorganisationen av certifikatutfärdarens certifikat ska omedelbart underrätta rotcertifikatutfärdaren om man känner till eller misstänker att certifikatutfärdarens privata nyckel har röjts. Då spärrar rotcertifikatutfärdaren det aktuella certifikatet för certifikatutfärdare och publicerar det på spärrlistan (CRL och/eller ARL).

2.1.3 Skyldigheter hos den part som förlitar sig på certifikatutfärdarens certifikat

Rotcertifikatutfärdaren efterföljer certifikatpolicyn och certifieringspraxisen i beviljandet av certifikatutfärdarens certifikat.

En förlitande part kan i god tro lita på certifikatet efter att ha kontrollerat att det är i kraft och inte tagits upp på spärrlistan. Förlitande parter är innan de godkänner ett certifikat skyldiga att kontrollera dem från spärrlistan. För att säkerställa att det går att

lita på att certifikatutfärdarens certifikat är giltigt ska den förlitande parten utföra alla nedan nämnda kontrollåtgärder på spärrlistan.

Förlitande parter som hämtar spärrlistan i registret ska kontrollera spärrlistans integritet och autenticitet med stöd av utfärdarens digitala signatur. Dessutom ska förlitande parter kontrollera spärrlistans giltighetstid.

Om det på grund av störningar i systemet eller tjänsten inte går att få tillgång till en giltig spärrlista, får certifikatutfärdarens certifikat eller ett certifikat utfärdat med det enligt denna certifieringspraxis inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Alla godkännanden av certifikatutfärdarens certifikat och slutanvändarens certifikat efter att giltighetstiden har gått ut sker på den förlitande partens egen risk.

2.1.4 Skyldigheter som gäller publiceringen av certifikatutfärdarens certifikat

Certifikatutfärdarens certifikat publiceras i ett offentligt register som är allmänt tillgänglig. Spärrade certifikatutfärdares certifikat publiceras på en spärrlista. De förlitande parterna ska kontrollera mot spärrlistan att ett certifikat är giltigt.

2.2 Ansvar

2.2.1 Rotcertifikatutfärdarens ansvar

Myndigheten för digitalisering och befolkningsdata svarar som rotcertifikatutfärdare för säkerheten för hela certifikatsystemet. Rotcertifikatutfärdaren svarar för införskaffade tjänster på samma sätt som om utfärdaren själv hade producerat tjänsten.

Myndigheten för digitalisering och befolkningsdata ansvarar för att certifikatutfärdarens certifikat har skapats enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralen samt lagen om stark autentisering och betrodda elektroniska tjänster och att det uppfyller certifikatutfärdarens fastställda skadeståndsansvar. Myndigheten för digitalisering och befolkningsdata ansvarar endast för de uppgifter som den har lagrat på certifikatet.

Myndigheten för digitalisering och befolkningsdata svarar för att certifikatutfärdarens certifikat är tillgängligt för användning från att det överlåts under hela giltighetstiden för certifikatutfärdarens certifikat, förutsatt att certifikatet inte spärras.

Myndigheten för digitalisering och befolkningsdata ansvarar för att certifikatutfärdarens certifikat enligt avtalet har överlämnats till en organisation som har identifierats på det sätt som certifikatutfärdarens certifikat förutsätter.

Vid signering av certifikatutfärdarens certifikat med sin privata nyckel intygar rotcertifikatutfärdaren att utfärdaren har kontrollerat uppgifterna i certifikatet med de metoder som beskrivs i rotcertifikatutfärdarens certifikatpolicy och certifieringspraxis.

Rotcertifikatutfärdaren ansvarar för att rätt certifikat för certifikatutfärdare förs in på spärrlistan och att det förs in på spärrlistan inom den tid som fastställs i certifieringspraxisen.

2.2.2 Registrerarens ansvar

Rotcertifikatutfärdaren är registrerare av certifikatutfärdarens certifikat Certifikatutfärdarens certifikat ansöks hos rotcertifikatutfärdaren med en ansökan om detta.

Rotcertifikatutfärdaren efterföljer i all sin verksamhet certifikatutfärdarens ansvar som nämns i detta kapitel.

Rotcertifikatutfärdaren ansvarar för registreringens del för skadeståndsavtalet enligt detta kapitel.

2.2.3 Ansvar för den organisation som innehar certifikatutfärdarens certifikat

Innehavarorganisationen av certifikatutfärdarens certifikat ansvarar för användningen av certifikatet, för de rättshandlingar som innehavaren gör med det och för de ekonomiska följderna av rättshandlingarna.

Ansvaret som innehavarorganisationen av certifikatutfärdarens certifikat bär upphör efter att organisationen har meddelat rotcertifikatutfärdaren de uppgifter som enligt avtalet om utfärdandet av certifikatet behövs för att spärra certifikatet. För att ansvaret som innehavarorganisationen av certifikatutfärdarens certifikat bär ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

2.2.4 Ansvaret hos den part som förlitar sig på certifikatutfärdarens certifikat

Den part som litar på certifikatutfärdarens certifikat kan inte uppriktigt lita på certifikatet om den förlitande parten inte kontrollerat certifikatets giltighet på spärrlistan. Om certifikatutfärdarens certifikat godkänns i en sådan situation frias rotcertifikatutfärdaren från ansvar.

Den part som litar på certifikatutfärdarens certifikat ska kontrollera att det utfärdade certifikatet motsvarar användningssyftet.

2.2.5 Begränsning av ansvar

Rotcertifikatutfärdaren svarar inte för eventuella skador eller kostnader som orsakas av att certifikatinnehavarens privata nycklar röjs, om inte röjningen direkt har orsakats av rotcertifikatutfärdaren omedelbara åtgärder.

Rotcertifikatutfärdaren svarar inte för indirekta skador eller följdskador som har orsakats den organisation som innehar certifikatutfärdarens certifikat. Myndigheten för digitalisering och befolkningsdata svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till den organisation som innehar certifikatutfärdarens certifikat.

Rotcertifikatutfärdaren svarar inte för skador som orsakas av force majeure, till exempel: strejk, eldsvåda, krig, uppror, konfiskering, valutarestriktioner, myndighetsåtgärder, lagstiftning och myndighetsbestämmelser, störningar i telekommunikation, eller dylika signifikanta och ovanliga orsaker oberoende av certifikatutfärdaren.

Rotcertifikatutfärdaren ansvarar inte för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel Internet, eller för att en rättshandling inte kan utföras på grund av att certifikatutfärdarens certifikatinnehavares utrustning eller kortläsare inte fungerar eller för att certifikatutfärdarens certifikat används i strid med sitt syfte.

Rotcertifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Rotcertifikatutfärdaren är inte skyldig att ersätta kostnader som orsakats den organisation som innehar certifikatutfärdarens certifikat eller den part som förlitar sig på certifikatet på grund av rotcertifikatutfärdarens utvecklingsarbete.

Rotcertifikatutfärdaren har rätt att avbryta tjänsten för den tid ändringar eller underhåll av systemet utförs. Om ändringar i eller underhållsarbeten på spärrlistan meddelas på förhand.

Vid fel i en nättjänst eller applikation som baserar sig på certifikatet svarar rotcertifikatutfärdaren inte för användningen av certifikatet eller för de kostnader som det orsakar användaren.

Det ansvar organisationen som innehar certifikatutfärdarens certifikat har för användningen av certifikatet upphör då organisationens representant har meddelat rotcertifikatutfärdaren de uppgifter som behövs för att spärra certifikatet och dessutom meddelat sina viktigaste samarbetspartners och intressentgrupper i certifikatärenden om saken. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

2.3 Ekonomiskt ansvar

2.3.1 Rotcertifikatutfärdare

På Myndigheten för digitalisering och befolkningsdata tillämpas bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Även vissa bestämmelser i skadeståndslagen (412/1974) tillämpas.

2.3.2 Övriga parter

En part som litar på certifikatutfärdarens certifikat kan lita på certifikatutfärdarens certifikat och de åtgärder som utförs med det om parten har kontrollerat att certifikatet inte finns på spärrlistan och att certifikatets giltighetstid inte gått ut och har kontrollerat certifikatets signering. Rotcertifikatutfärdaren ansvarar för certifikatutfärdarens certifikat innan det anmäls till spärrlistan enligt förbindelsen i denna certifikatpolicy och i certifieringspraxisen som gäller certifikatutfärdarens certifikat.

2.3.3 Rotcertifikatutfärdarens ekonomiförvaltning

Myndigheten för digitalisering och befolkningsdata är rotcertifikatutfärdare och dess certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Myndigheten för digitalisering och befolkningsdata är ett ämbetsverk underställt finansministeriet. Myndigheten för digitalisering och befolkningsdata ekonomiska förvaltning utgår från lagar och förordningar om statens ekonomi samt finansministeriets och Statskontorets bestämmelser. Statens revisionsverk sköter

granskningen av ekonomin. Utöver detta beskrivs verksamhetens resultat med fokus på effekter, ekonomi och lönsamhet.

2.4 Tolkning och verkställighet

2.4.1 Lagstiftning som tillämpas

Rotcertifikatutfärdaren iakttar gällande finsk lagstiftning i verksamheten med certifikattjänster.

Om Myndigheten för digitalisering och befolkningsdatas ställning föreskrivs i lagen om Myndigheten för digitalisering och befolkningsdata (304/2019).

Rotcertifikatutfärdaren iakttar god informationshantering enligt personuppgiftslagen (523/1999) och lagen om offentlighet i myndigheternas verksamhet (621/1999).

Myndigheten för digitalisering och befolkningsdatas certifikatverksamhet baserar sig på Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen).

Myndigheten för digitalisering och befolkningsdatas betrodda tjänster uppfyller förutom karven i eIDAS-förordningen även kraven i standard EN 319 401 om kvalificerade tillhandahållare av betrodda tjänster och i standard EN 319 411-1 om kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller certifikat.

På Myndigheten för digitalisering och befolkningsdata tillämpas bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Även vissa bestämmelser i skadeståndslagen (412/1974) tillämpas.

2.4.2 Avgörande av meningsskiljaktigheter

Vid utfärdandet av certifikat ansvarar rotcertifikatutfärdaren för att certifikatutfärdarnas certifikat uppfyller kraven i denna certifieringspraxis samt i certifikatpolicyn för certifikatutfärdarens certifikat.

Eventuella tvister löses enligt rättssystemet i Finland. Vid lösningen av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning.

2.5 Avgifter

I detta stycke fastställs avgifterna för användningen av det certifikat för certifikatutfärdare som utfärdats av rotcertifikatutfärdaren.

2.5.1 Utfärdande och förnyande av certifikatutfärdarens certifikat

Certifikatutfärdarens certifikat ansöks hos Myndigheten för digitalisering och befolkningsdata. Ett certifikat utfärdas alltid utifrån en ny ansökan med beaktande av det identifieringsförfarande som fastställts i den här certifieringspraxisen. Avgiften för certifikatutfärdarens certifikat utgår från en årlig avgift enligt Myndigheten för digitalisering och befolkningsdatas serviceprislista.

2.5.2 Avgifter för användning av certifikatutfärdarens certifikat

Rotcertifikatutfärdaren kan inte debitera certifikatutfärdarens certifikatinnehavare separat för användningen av certifikaten, spärrlistan eller det offentliga registret. Avgiften för certifikatutfärdarens certifikat utgår från en årlig avgift enligt rotcertifikatutfärdarens serviceprislista.

Enskilda tillhandahållare av e-tjänster kan debitera separat för användningen av sin egen tjänst.

2.5.3 Avgifter för registrering av certifikatutfärdarens certifikat på spärrlistan

Det kostar ingenting att anmäla certifikatutfärdarens certifikat till spärrlistan. Att hämta spärrlistor (CRL och/eller ARL) från registret och kontrollera att certifikatutfärdarens certifikat är i kraft är också gratis.

2.6 Publikation av och tillgång till information

2.6.1 Publicering av information om certifikatutfärdarens certifikat

Rotcertifikatutfärdaren publicerar alla certifikatutfärdares certifikat och spärrlistor i ett avgiftsfritt och allmänt tillgängligt offentligt register. Myndigheten för digitalisering och befolkningsdata publicerar certifikatpolicyn, certifieringspraxisen, certifikatbeskrivningen samt övriga offentliga handlingar med anknytning till produktionen av certifikattjänster på sin webbplats.

2.6.2 Publikationsfrekvens

Certifikatutfärdarens certifikat publiceras i det offentliga registret och finns i registret under hela dess giltighetstid. Rotcertifikatutfärdaren publicerar en spärrlista som gäller i ett år från publikation. Spärrlistan uppdateras en gång i året eller vid behov med en ny spärrlista.

2.6.3 Uppgifternas tillgänglighet

Uppgifterna i registret och spärrlistan är offentligt tillgängliga. Myndigheten för digitalisering och befolkningsdatas FINeID-specifikationer och dokument över certifikatpolicyer och certifieringspraxis finns på webbplatsen https://www.eevertti.vrk.fi.

2.6.4 Dataförvaring

Offentlig information som publiceras av Myndigheten för digitalisering och befolkningsdata finns på MDB:s webbplats. Uppgifter i certifikatsystemet som inte är offentliga har registrerats i Myndigheten för digitalisering och befolkningsdatas datalager. Certifikatutfärdarens information arkiveras i enlighet med rotcertifikatutfärdarens gällande arkivstadga. Personuppgifter behandlas särskilt omsorgsfullt och

Myndigheten för digitalisering och befolkningsdata har publicerat särskilda uppförandekoder enligt personuppgiftslagen som gäller produktionen av certifikattjänster. Myndigheten för digitalisering och befolkningsdata har även berett en

registerbeskrivning för hanteringen av personuppgifter inom varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen.

2.7 Dataskyddsgranskning

2.7.1 Granskningsfrekvens

Myndigheten för digitalisering och befolkningsdata utför i sin egenskap av rotcertifikatutfärdare en dataskyddsgranskning för de tekniska leverantöreras lokaler, utrustning och verksamhet på ett ändamålsenligt sätt. Granskningar utförs minst en gång om året och alltid när en ny avtalsperiod inleds. Vid granskningsförfarandet iakttar Myndigheten för digitalisering och befolkningsdata förfaringssätten enligt informationssäkerhetsstandarden ISO 27001.

Med hjälp av granskningarna klarläggs om utfärdarens verksamhet uppfyller kraven i informationssäkerhetsstandarderna. I regel utvärderas utfärdare i enlighet med standarden ISO 27001.

Traficom, som är kvalitetssäkrare, har rätt att granska utfärdarens verksamhet på villkor som bestämts i lagen om stark autentisering och betrodda elektroniska tjänster.

2.7.2 Granskare

Informationssäkerheten på Myndigheten för digitalisering och befolkningsdata granskas av chefen för informationssäkerheten eller av en utomstående granskare som är specialiserad på granskning av tekniska leverantörer av certifikattjänster.

2.7.3 Föremål för granskningen och granskningens omfattning

Målen för granskningen fastställs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller, om Myndigheten för digitalisering och befolkningsdata utför granskningen i enlighet med dataskyddsstandarden ISO 27001, i enlighet med Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy eller tekniska leveransavtal.

Granskningen utförs med beaktande av genomförandet av åtta delområden inom informationssäkerhet. Egenskaper som granskas är konfidentialitet, integritet och tillgänglighet.

I granskningen jämförs certifikatpolicyn, certifieringspraxisen och de tekniska leverantörernas verksamhetsanvisningar med hela certifikatorganisationens och -systemets verksamhet. Myndigheten för digitalisering och befolkningsdata övervakar att verksamhetsanvisningarna stämmer överens med certifikatpolicyn.

I granskningarna beaktas inte bara den administrativa informationssäkerheten utan även olika serviceleverantörer bl.a. enligt följande indelning:

Spärrtjänst:

- informationssäkerhet
- personalsäkerhet

- fysisk säkerhet

Certifikatproduktion:

- arbetsfördelningar och var och ens uppgifter, personalsäkerhet
- fysisk säkerhet
- säkerhet som gäller certifikatutfärdarens privata nyckel
- certifikatutfärdarens produktionssystem och reservsystem
- informationssäkerhet

Kortproduktion:

- produktionslinjen som helhet från ända till ända
- kvalitetsövervakningen i kortproduktionen
- informationssäkerhet
- personalsäkerhet
- fysisk säkerhet

Registertjänst:

- de komponenter som används
- administrationsförbindelser
- underhåll av registret och verksamhet vid felsituationer
- personalsäkerhet
- informationssäkerhet
- fysisk säkerhet

2.7.4 Åtgärder vid avvikelser

Upptäckta avvikelser antecknas i granskningsrapporten och man reagerar på dessa enligt lagen, dataskyddsstandarden ISO 27001 och gällande leveransavtal.

2.7.5 Information om resultatet av granskningen

Man informerar om resultatet av granskningen i enlighet med lagen, dataskyddsstandarden ISO 27001, Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och gällande leveransavtal. Det detaljerade och standardiserade granskningsresultatet avsett för intern användning är konfidentiellt och offentliggörs inte.

Rapporter med på förhand bestämd utformning utarbetas separat för användning utanför organisationen.

2.8 Publicering av information

2.8.1 Uppgifter publicerade av rotcertifikatutfärdaren

Uppgifterna i certifikatsystemet publiceras eller överlämnas inte vidare, såvida detta inte grundar sig på bestämmelserna om utlämnande av uppgifter i personuppgiftslagen, lagen om offentlighet i myndigheternas verksamhet, lagen om befolkningsdatasystemet och Befolkningsregistercentralen eller lagen om stark autentisering och betrodda elektroniska tjänster eller på ändamål som fastställts i certifikatpolicyn eller certifieringspraxisen.

2.8.2 Offentlig information

Uppgifterna i det offentliga registret och spärrlistan är offentliga, likaså certifieringspraxisen och de i certifieringspolicyn fastställda uppgifterna samt de publicerade FI-NEID-specifikationerna.

2.8.3 Information om att giltighetstiden för certifikatutfärdarens certifikat har gått ut eller avbrutits

Start- och slutdatum för giltighetstiden för certifikatutfärdarens certifikat anges på certifikatet. Certifikatutfärdares certifikat som spärrats under giltighetstiden publiceras på en allmänt tillgänglig spärrlista.

2.8.4 Information som lämnas ut till myndigheter

Vilka uppgifter som ska lämnas ut till myndigheter bestäms enligt gällande lagstiftning.

2.8.5 Övrig information

Uppgifterna i certifikatutfärdarens certifikatsystem lämnas inte ut för andra ändamål än de som nämns i detta avsnitt.

2.8.6 Övriga principer gällande utlämnande av information

Med tanke på tillförlitligheten hos certifikatutfärdaren är det av största vikt att rotcertifikatutfärdaren på alla vis sörjer för att hemlighålla konfidentiellt material som erhålls i samband med certifikatverksamheten och iakttar god informationsförvaltningssed, om inte annat föranleds av myndigheternas rätt att få uppgifter ur certifikatsystemet.

Vid behandlingen av personuppgifter iakttar Myndigheten för digitalisering och befolkningsdata personuppgiftslagen och speciallagstiftning. Myndigheten för digitalisering och befolkningsdata har berett uppförandekoder både för utlämning av uppgifter och för den behandling av personuppgifter som sker inom certifikatverksamheten. Vid behandlingen av personuppgifter iakttas särskild omsorgsfullhet.

2.9 Immaterialrättigheter

Myndigheten för digitalisering och befolkningsdata äger samtliga uppgifter som anknyter till certifikaten och dokumentationen i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata äger samtliga ägande- och användarrättigheter för denna certifieringspraxis och certifikatpolicyn för certifikatutfärdaren.

3 Identifiering av den som söker certifikatutfärdarens certifikat

3.1 Registrering

I kapitlen 4.1 – 4.3 behandlas den praxis och de processer som iakttas vid identifiering och verifiering av de som söker certifikatutfärdarens certifikat.

Rättigheterna och skyldigheterna hos den som ansöker om certifikatutfärdarens certifikat nämns i avtalet om produktionen av certifikatutfärdarens certifikat som ingåtts mellan rotcertifikatutfärdaren och den som söker certifikatutfärdarens certifikat.

I avtalet sägs tydligt att den som söker certifikatutfärdarens certifikat godkänner att certifikatutfärdarens certifikat skapas och publiceras i ett offentligt register. På samma gång godkänner certifikatsökanden reglerna och villkoren för användningen av certifikatutfärdarens certifikat samt sin skyldighet att göra en anmälan om det föreligger risk för att den privata nyckeln har missbrukats eller röjts.

Sökanden av certifikatutfärdarens certifikat svarar för att samtliga uppgifter som är väsentliga för certifikatet och som sökanden uppgett till utfärdaren eller registreraren är riktiga.

3.1.1 Benämningspraxis

Myndigheten för digitalisering och befolkningsdatas rotcertifikat är:

CN (Common name) = DVV Gov. Root CA – G3 RSA
OU (Organizational unit) = Varmennepalvelut
OU (Organizational unit) = Certification Authority Services
O (Organization) = Digi- ja vaestotietovirasto CA
C (Country) = FI

och

CN (Common name) = DVV Gov. Root CA – G3 ECC
OU (Organizational unit) = Varmennepalvelut
OU (Organizational unit) = Certification Authority Services
O (Organization) = Digi- ja vaestotietovirasto CA
C (Country) = FI

och

CN (Common name) = VRK Gov. Root CA – G2
OU (Organizational unit) = Varmennepalvelut
OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA
C (Country) = FI

Utfärdaren av rotcertifikatet signerar utfärdarens certifikat och det förs in i det offentliga registret.

Uppgifterna om innehavaren av utfärdarens certifikat anger entydigt certifikatets innehavarorganisation.

3.1.2 Leverans av privata nycklar till innehavaren av certifikatutfärdarens certifikat

Den som ansöker om certifikatutfärdarens certifikat skapar en hemlig och en öppen nyckel. Den organisation som är innehavare av certifikatutfärdarens certifikat ska förvara sin privata nyckel i en säker miljö och förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.

3.2 Förnyelse av nyckelpar

Vid förnyelse av certifikatutfärdarens certifikat iakttas samma rutiner som vid första ansökan om certifikatutfärdarens certifikat. Då innehavaren av certifikatutfärdarens certifikat förnyar sin privata nyckel fordrar detta alltid ny registrering, nytt avtal och nytt certifikatutfärdarens certifikat.

3.3 Identifiering av den som begär spärrning

Innehavaren av certifikatutfärdarens certifikat kan begära att certifikatutfärdarens certifikat spärras innan dess giltighetstid löpt ut.

Förfarande vid begäran om spärrning

Representanten för den organisation som innehar certifikatutfärdarens certifikat ska omedelbart underrätta rotcertifikatutfärdaren om man känner till eller misstänker att innehavaren av certifikatutfärdarens privata nyckel har röjts. Då spärrar rotcertifikatutfärdaren certifikatet i fråga. Begäran om att spärra certifikatutfärdarens certifikat görs i första hand av den organisation som innehar certifikatutfärdarens certifikat om missbruk av certifikatet blivit möjlig. En begäran om spärrning kan också göras av registreraren eller rotcertifikatutfärdaren.

4 Funktionella krav

4.1 Ansökan om certifikatutfärdarens certifikat

Rättigheterna och skyldigheterna för den som ansöker om certifikatutfärdarens certifikat nämns i ansökningshandlingen och i det avtal som ingås med den organisation som söker certifikatutfärdarens certifikat. Avtalet undertecknas av en behörig representant för den organisation som innehar certifikatet. I avtalet nämns bägge parters rättigheter och skyldigheter. I ansökningshandlingen och i användningsvillkoren nämns tydligt att den som ansöker om certifikatutfärdarens certifikat intygar riktigheten hos uppgifterna med sin signatur samt godkänner att certifikatet framställs och att det publiceras i det offentliga registret. På samma gång godkänner certifikatsökanden att certifikatet införs på spärrlistan ifall det finns risk för missbruk av certifikatet.

4.2 Utfärdande av certifikatutfärdarens certifikat

Rotcertifikatutfärdaren beviljar certifikatutfärdarens certifikat genom att godkänna ansökan om certifikatutfärdarens certifikat och underteckna leveransavtalet om certifikatutfärdarens certifikat.

Rotcertifikatutfärdaren ansvarar vid beviljandet av certifikatet för att datainnehållet i certifikatet är riktigt vid överlåtelsen av certifikatet.

4.3 Mottagande av certifikatutfärdarens certifikat

Då certifikatutfärdarens certifikat har beviljats levereras det till kunden enligt avtal.

4.4 Giltighetstiden hos certifikatutfärdarens certifikat och spärrning av det

4.4.1 Förutsättningar för spärrning av certifikatutfärdarens certifikat

Den som innehar certifikatutfärdarens certifikat ska omedelbart underrätta rotcertifikatutfärdaren om man känner till eller misstänker att innehavaren av certifikatutfärdarens privata nyckel har röjts. Då spärrar rotcertifikatutfärdaren certifikatet i fråga. Den behöriga representanten för den organisation som innehar certifikatutfärdarens certifikat har definierats i avtalet mellan rotcertifikatutfärdaren och den organisation som innehar certifikatutfärdarens certifikat.

Spärrandet av certifikatutfärdarens certifikat utförs utan fördröjelse efter att begäran om spärrning har anlänt och då spärrningen av certifikatutfärdarens certifikat har bekräftats.

4.4.2 Genomförandet av spärrningen

Begäran om att spärra certifikatutfärdarens certifikat görs i första hand av innehavaren av certifikatutfärdarens certifikat om missbruk av certifikatet blivit möjlig. Certifikatutfärdarens certifikat kan även spärras av registreraren eller rotcertifikatutfärdaren.

4.4.3 Spärrhändelsen

Den organisation som innehar certifikatutfärdarens certifikat ansvar för spärrandet av certifikatutfärdarens certifikat. Certifikatutfärdarens certifikat kan på anmälan av den organisation som innehar certifikatet registreras på spärrlistan och då förhindras användningen av det certifikatutfärdarens certifikat som rotcertifikatutfärdaren beviljat.

Certfikatutfärdarens certifikat spärras genom att enligt leveransavtalet som ingåtts med den organisation som innehar certifikatutfärdarens certifikat meddela detta till Myndigheten för digitalisering och befolkningsdata på adressen kirjaamo@dvv.fi. Ansvaret enligt avtalet med den organisation som innehar certifikatutfärdarens certifikat upphör då en preciserad anmälan som möjliggör spärrandet har tagits emot. Samtidigt upphör det ansvar innehavaren av certifikatutfärdarens certifikat bär för användningen av certifikatutfärdarens certifikat.

Då certifikatutfärdarens certifikat har spärrats kan det inte tas i bruk på nytt.

Myndigheten för digitalisering och befolkningsdata spärrar de certifikatutfärdares certifikat som utfärdats om det påträffas fel i certifikatutfärdarens certifikats datainnehåll eller om man känner till att den privata nyckeln till certifikatutfärdarens certifikat har avslöjats eller det föreligger ett motiverat hot om detta eller om avtalet som ingåtts med den organisation som innehar certifikatutfärdarens certifikat inte har efterföljts eller avtalstiden har gått ut.

Myndigheten för digitalisering och befolkningsdata kan i egenskap av rotcertifikatutfärdare spärra certifikatutfärdarens certifikat som signerats med rotcertifikatutfärdarens privata nyckel om det finns anledning att misstänka att Myndigheten för digitalisering och befolkningsdatas privata nycklar har röjts eller råkat i fel händer.

Samtliga giltiga certifikatutfärdarens certifikat som utfärdats med den röjda nyckeln ska spärras på en eller flera spärrlistor vilkas giltighetstid inte upphör innan det senast spärrade certifikatutfärdarens certifikats giltighetstid har löpt ut.

Om den privata nyckeln eller annan teknisk metod som använts vid skapandet av rotcertifikatutfärdarens certifikat för certifikatutfärdaren har röjts eller på annat vis blivit oanvändbar ska rotcertifikatutfärdaren meddela det inträffade till samtliga innehavarorganisationer av certifikatutfärdarens certifikat och slutanvändarna på ändamålsenligt sätt.

Rotcertifikatutfärdaren kan spärra ett certifikat av särskild anledning.

4.4.4 Tidpunkten för en spärrhändelse

Spärrningen av certifikatutfärdarens certifikat genomförs omedelbart i samband med begäran om spärrning.

4.4.5 Tillfälligt avbrytande av giltighetstiden för certifikatutfärdarens certifikat

Giltighetstiden för ett certifikatutfärdarens certifikat kan inte avbrytas tillfälligt.

4.4.6 Publiceringsfrekvens för spärrlista

Certifikatutfärdarens certifikat publiceras i det offentliga registret och finns i registret under hela dess giltighetstid. Rotcertifikatutfärdaren publicerar en spärrlista som gäller i ett år från publikation. Spärrlistan uppdateras med en ny spärrlista en gång i året.

Spärrlistan innehåller en uppgift om tidpunkten för publiceringen av nästa spärrlista.

Den nya spärrlistan publiceras senast när det föregående upphör att gälla.

Vid systemuppdateringar och andra exceptionella situationer kan MDB publicera spärrlistor enligt andra intervaller och med förlängd giltighetstid.

4.4.7 Krav i anslutning till kontroll av spärrlistor

Skyldigheterna hos den part som förlitar sig på certifikatutfärdarens certifikat beskrivs i avsnitt 2.

4.4.8 Kontroll av certifikatutfärdarens certifikat i realtid

Certifikatutfärdarens certifikat kan endast spärras på det sätt som nämns i avtalet eller denna certifieringspraxis hos registreraren. Rotcertifikatutfärdaren tillhandahåller ingen tjänst för kontroll av certifikatens status i realtid, dvs. en OCSP-tjänst. Certifikatutfärdaren publicerar en spärrlista över spärrade certifikat.

4.4.9 Särskilda krav i en situation där den privata nyckeln för innehavaren av certifikatutfärdarens certifikat har röjts

Innehavaren av certifikatutfärdarens certifikat ansvarar för en skyddad användning av de privata nycklarna genom att på alla sätt bära omsorg för sin privata nyckel på det sätt som beskrivs i bruksvillkoren. En organisation som innehar certifikatutfärdarens certifikat som misstänker att det blivit möjligt att använda certifikatet i strid med avtalsvillkoren ska genast kontakta rotcertifikatutfärdaren.

4.5 Övervakningen av systemet

För övervakningen av systemet sparar rotcertifikatutfärdaren loggar över händelserna i certifikatutfärdarens certifikatproduktion, hanteringen av användarrättigheterna till certifikatutfärdarens certifikatsystem, utrustningen i sin helhet, systemprogrammen och tillämpningarna jämte ändringar, säkerhetskopieringen och återställande av säkerhetskopior. Rotcertifikatutfärdaren övervakar även de dokument som gäller verksamheten. Iakttagna avvikelser rapporteras på det sätt som överenskommits med avtalspartnern.

4.6 Arkivering av data i anslutning till certifikatutfärdarens certifikat

4.6.1 Material som arkiveras

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid arkiveringen av certifikatutfärdarens certifikat tillämpas dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

Om rotcertifikatutfärdarens verksamhet avbryts eller upphör ska rotcertifikatutfärdaren meddela samtliga kunder att arkivet fortfarande är tillgängligt. Samtliga förfrågningar om arkiverade uppgifter skickas till utfärdaren eller den instans som rotcertifikatutfärdaren uppgett innan rotcertifikatutfärdaren verksamhet har upphört.

Rotcertifikatutfärdaren ser till att arkiven är tillgängliga och läsbara även om rotcertifikatutfärdarens verksamhet avbryts eller upphör.

Uppgifterna i ett certifikatregister som baserar sig på lagen om starkautentisering och betrodda elektroniska tjänster förfaras i 10 år efter att certifikatutfärdarens certifikat har gått ut.

Det arkiverade materialet förvaras enligt bestämmelserna för myndighet som fungerar som utfärdare av kvalificerade certifikat.

4.6.2 Skydd av arkiv

Rotcertifikatutfärdaren förvarar handlingar med anknytning till ansökning om certifikatutfärdarens certifikat, autentisering av personer och överlåtelse av certifikatutfärdarens certifikat som arkiveras i ändamålsenliga lokaler.

Materialet som arkiveras förvaras i säkra lokaler med passagekontroll.

4.6.3 Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

4.6.4 Metoder för införskaffning och tryggande av arkiverat material

Om rotcertifikatutfärdarens verksamhet avbryts eller upphör ska rotcertifikatutfärdaren meddela samtliga kunder att arkivet fortfarande är tillgängligt. Samtliga förfrågningar om arkiverade uppgifter skickas till utfärdaren eller den instans som rotcertifikatutfärdaren uppgett innan rotcertifikatutfärdaren verksamhet har upphört.

Rotcertifikatutfärdaren ser till att arkiven är tillgängliga och läsbara även om rotcertifikatutfärdarens verksamhet avbryts eller upphör.

Uppgifter kan överlåtas ur arkivet i den mån detta är motiverat med tanke på innehavaren av certifikatutfärdarens certifikat eller den förlitande parten.

4.7 Hantering av kontinuerlig verksamhet och undantagsfall

Rotcertifikatutfärdaren har en kontinuitets- och beredskapsplan som gör att rotcertifikatutfärdarens verksamhet kan fortsätta i exceptionella situationer.

4.7.1 Rotcertifikatutfärdarens privata nyckel har röjts eller rotcertifikatutfärdarens certifikatet har spärrats

Utfärdaren av rotcertifikatet uppger i varje certifieringspraxis de åtgärder som utfärdaren, innehavarna av utfärdarens certifikat, parterna som litar på utfärdarens certifikat, registrerarna och utfärdarens personer ska vidta om utfärdarens privata nyckel har röjts eller blivit oanvändbar på annat vis.

I detta fall ska utfärdaren av rotcertifikatet antingen upphöra med sin verksamhet på det sätt som beskrivs i kapitel 4.8 eller utföra följande åtgärder:

a) Utfärdaren av rotcertifikatet meddelar det inträffade till samtliga innehavare, förlitade parter och avtalskunder eller i övrigt har ett sådant förhållande till utfärdaren på grund av avtalsförhållande eller myndighetsverksamhet att utfärdaren måste informera om det inträffade.

b) Rotcertifikatutfärdaren av rotcertifikatet skapar en ny nyckel i enlighet med kapitel 6.

c) Samtliga gällande utfärdarens certifikat och certifikat för slutanvändare om beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars

giltighetstid inte upphör innan det senast spärrade utfärdarens certifikatets giltighetstid har löpt ut.

4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas, som är rotcertifikatutfärdare, säkerhetspolicy beaktas åtgärder som förorsakas av problem med den externa säkerheten. Myndigheten för digitalisering och befolkningsdata har fått informationssäkerhetscertifikatet ISO 27001, som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även vid en eventuell katastrof. Myndigheten för digitalisering och befolkningsdata efterföljer i utfärdandet och underhållet av certifikat de förfaringssätt som fastställts för datasäkerheten.

4.8 Upphörande av rotcertifikatutfärdarens verksamhet

Rotcertifikatutfärdarens verksamhet anses upphöra i en situation när alla tjänster som knyter an till rotcertifikatutfärdaren och upprätthållande och administration av certifikatutfärdarens certifikat läggs ned permanent. Rotcertifikatutfärdarens verksamhet anses inte upphöra om certifieringstjänsten överförs från en organisation till en annan.

Rotcertifikat utfärdaren meddelar om en nedläggning av certifikattjänsterna till de aktörer som nämns i avsnitt 4.7.1 a så snart som möjligt, dock minst en månad före tidpunkten för nedläggningen.

Innan rotcertifikatutfärdarens verksamhet upphör utförs minst följande åtgärder:

a) Samtliga utfärdade och giltiga certifikatutfärdarens certifikat spärras på en eller flera spärrlistor, vilkas giltighetstid inte upphör förrän giltighetstiden för de sista spärrade certifikatutfärdarens certifikat har löpt ut.

b) Rotcertifikatutfärdaren upphäver samtliga avtalspartners befogenheter för att utföra åtgärder med anknytning till processen för beviljande av rotcertifikat för rotcertifikatutfärdarens del.

c) c) Rotcertifikatutfärdaren säkerställer att tillgången till rotcertifikatutfärdarens arkiv som nämns i punkt 4.6 bevaras även efter att rotcertifikatutfärdarens verksamhet upphört.

5 Fysiska krav, funktionella krav och krav på personalens säkerhet

Myndigheten för digitalisering och befolkningsdata har i egenskap av rotcertifikatutfärdare beviljats ett informationssäkerhetscertifikat. MDB:s informationssäkerhetslösningar fyller kraven i standarden ISO 27001.

Rotcertifikatutfärdaren kan anlita tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatutfärdarens certifikatverksamhet. Rotcertifikatutfärdaren ansvarar i egenskap av certifikatutfärdare för säkerheten och funktionerna inom samtliga delområden av certifikatproduktionen.

Rotcertifikatutfärdaren efterföljer god informationshanteringssed. De tjänster som gäller erbjudandet av certifikat har organiserats som Myndigheten för digitalisering och befolkningsdatas certifikattjänstsfunktioner enligt husets organisationsstruktur.

5.1 Arrangemang i anslutning till den fysiska säkerheten

5.1.1 Läge och lokalernas egenskaper

Rotcertifikatutfärdarens system finns i säkra maskinsalar och uppfyller anvisningarna och bestämmelserna för säkerheten i maskinsalar.

Säkerheten hos rotcertifikatutfärdarens lokaler har skapats genom att hindra obehörigas tillträde genom att låsa lokalerna och använda lokaler av stabil struktur och tillräcklig styrka. Maskinsalarna saknar onödiga fönster och de har byggts upp med hållbara byggnadsmaterial i konstruktionen.

5.1.2 Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässiga uppgifter inom rotcertifikatsystemet utförs är försedda med passagekontroll. Passerkontrollsystemet upptäcker både tillåtet och otillåtet tillträde. Tillträde till maskinsal fordrar autentisering av personen, varvid personen identifieras och hans eller hennes passagerättigheter kontrolleras och händelsen registreras. Maskinsalarna övervakas dygnet runt.

5.1.3 Elmatning och ventilation

Rotcertifikatutfärdarens maskinsalar för certifikatsystemet har ändamålsenlig ventilation. Lokalerna är försedda med reservkraftslösningar i fastigheterna som förberedelser inför okontrollerade elavbrott.

5.1.4 Brandsäkerhet

Rotcertifikatutfärdarens maskinsalar för certifikatsystemet har behövliga larmmekanismer för eldsvådor, den första släckningsutrustning som behövs samt automatiska släckningssystem.

5.1.5 Lagring av information

Den information som rotcertifikatutfärdaren arkiverar och säkerhetskopiorna bevaras i andra lokaler än rotcertifikatutfärdarens maskiner.

Rotcertifikatutfärdarens information har skyddats från förstörelse, ändring och otillåten användning.

5.1.6 Hantering av onödigt informationsmaterial

Rotcertifikatutfärdarens säkerhetsklassade informationsmaterial förstörs på ett tillförlitligt sätt.

5.1.7 Vattenskador

Maskinsalarna för rotcertifikatutfärdarens certifikatsystem har ändamålsenliga fuktsensorer.

5.2 Funktionella krav

5.2.1 Ansvarsfördelning

Rotcertifikatutfärdaren anlitar tekniska leverantörer för registrering och datatekniska uppdrag inom produktionen av certifikat.

Rotcertifikatutfärdarens uppgifter delas in i följande ansvarsområden:

- Datasäkerhetsansvarig
- Registreringsansvarig
- Administratör för systemet
- Användare av systemet
- Övervakare av systemet

Rotcertifikatutfärdaren och den tekniska leverantören för rotcertifikatutfärdarens certifikatsystem har ingått ett leveransavtal, där leverantörens uppgifter, metoder och ansvarsområden samt anordnandet av datasäkerheten beskrivs detaljerat.

5.2.2 Antalet personer som krävs för olika uppgifter

Skapande, aktivering, säkerhetskopiering och returnering av rotcertifikatutfärdarens privata nyckel är åtgärder som utförs med två personer som fungerar som administratörer för systemet närvarande. Det är möjligt att återkalla rotcertifikatutfärdarens privata nyckel bara om två behöriga personer övervakar åtgärden. Vid formateringen av den kryptografiska modulen närvarar minst två personer som fungerar som administratörer för systemet.

5.2.3 Uppgiftsspecifik identifiering

Registreraren av certifikatutfärdarens certifikat: Registrerare är registreringsenheten för certifikatverksamheten vid Myndigheten för digitalisering och befolkningsdata.

Administratören för rotcertifikatutfärdarens certifikatsystem: Systemets administratör autentiseras med ett personligt kontrollkort för administration av rotcertifikatutfärdarens system. Administratörer för rotcertifikatutfärdarens certifikatsystem är certifikatsystemleverantörens systemexperter samt personer som befullmäktigats för uppdraget av Myndigheten för digitalisering och befolkningsdata.

Användaren av rotcertifikatutfärdarens certifikatsystem: Systemanvändaren autentiseras med ett personligt personkort för användning av systemet. Användare av rotcertifikatutfärdarens certifikatsystem är maskinsalsverksamheten, initiativtagare till tekniska certifikatbegäranden och spärrtjänsten.

5.3 Personsäkerhet

Myndigheten för digitalisering och befolkningsdata fungerar som rotcertifikatutfärdare och svarar för rotcertifikatverksamheten. De tekniska underleverantörerna har anlitats genom upphandling och agerar för Myndigheten för digitalisering och befolkningsdatas räkning och på Myndigheten för digitalisering och befolkningsdatas ansvar.

Personalen vid Myndigheten för digitalisering och befolkningsdatas certifikattjänster förutsätts ha den utbildning och kännedom om certifikatverksamheten som arbetsuppgifterna förutsätter. Experterna följer hela tiden med branschutvecklingen i Finland och Europa samt är sakkunniga inom branschen.

I samband med upphandlingen har rotcertifikatutfärdaren utvärderat kompetensen hos de nyckelsakkunniga hos de tekniska leverantörerna vad gäller deras förmåga att verkställa rotcertifikatutfärdarens certifikattjänst. De datatekniska underleverantörerna upprätthåller personalens kompetens vad gäller utrustning, program, metoder och informationssäkerhet som tillämpas i serviceproduktionen. Dessutom ser de tekniska leverantörerna till att personalen känner till databehandlingsuppgifterna i certifikattjänsten på det sätt som tjänsten förutsätter.

5.3.1 Utredning av personalens bakgrund

Myndigheten för digitalisering och befolkningsdata utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar i de tekniska leverantörernas certifikatutfärdarnas certifikatmiljö. Säkerhetskontrollen görs av skyddspolisen. Myndigheten för digitalisering och befolkningsdata förbehåller sig rätten att inte godkänna en anställd hos den tekniska leverantören för uppdrag som gäller arbete med rotcertifikatutfärdarens certifikatsystem.

5.3.2 Förfarande vid utförande av bakgrundskontroll

Personalens arbetserfarenhet kartläggs vid rekryteringen. Ett tillförlitlighetsförfarande utförs för varje person utifrån de uppgifter han eller hon uppger på ett standardformulär.

Samtliga personer som arbetar med centrala uppgifter hos rotcertifikatutfärdaren, certifikattjänsterna, producenterna av registertjänster och spärrtjänsten ska:

- fylla i den blankett som behövs för tillförlitlighetsförfarandet som skickas in till skyddspolisen. Blanketten används för att utföra ett tillförlitlighetsförfarande för personen,
- avstå från uppgifter som strider mot deras skyldigheter och ansvarsområden,
- vara personer som inte tidigare har avfärdats på grund av att de försummat eller misskött sina uppgifter,
- ha lämplig utbildning för att utföra sina uppgifter.

5.3.3 Krav på utbildning

Personalen hos rotcertifikatutfärdaren ska ha sådan utbildning att de kan utföra sina uppgifter på bästa möjliga sätt. Vid Myndigheten för digitalisering och befolkningsdata finns en utbildningsplan. För förverkligandet av planen svarar Myndigheten för digitalisering och befolkningsdatas administrativa enhet.

5.3.4 Underhåll av expertis och kompetens

Utbildningen för Myndigheten för digitalisering och befolkningsdatas personal planeras och underhålls på så vis att de anställda alltid besitter den kompetens som fordras för att utföra uppgifterna på bästa möjliga sätt.

5.3.5 Krav på uppgiftsrotation

Då rotcertifikatutfärdaren planerar arbetsrotation inom sin verksamhet ska uppgifterna organiseras på så vis att den anställda kan utföra sina nya uppgifter på bästa möjliga sätt. I planeringen av personalrotationen beaktas bl.a. de krav som informationssäkerheten ställer, skyddet av förtroligheten och principerna för god hantering av personuppgifter som beskrivs i praxisen för behandling av personuppgifter. Även inom arbetsrotationen efterlevs rotcertifikatutfärdarens dataskyddspolicy och dataskyddsplan samt rotcertifikatutfärdarens övriga allmänna anvisningar.

5.3.6 Åtgärder vid avvikelser

Myndigheten för digitalisering och befolkningsdatas personal agerar i sitt uppdrag med ämbetsmannaansvar och i enlighet med Myndigheten för digitalisering och befolkningsdatas interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

5.3.7 Personal som representerar organisationen

Vid rekryteringen av personal ska man se till att personalen innehar den kompetens som fordras för uppgifterna och att inget sådant framgår vid utredningen av personens bakgrund som står i konflikt med produktionen av certifikatutfärdarens certifikattjänster.

5.3.8 Handlingar som tillhandahålls personalen

Personalen har alltid tillgång till Myndigheten för digitalisering och befolkningsdatas kvalitets- och säkerhetsdokument.

6 Tekniska säkerhetsarrangemang

6.1 Skapa och lagra nyckelpar

6.1.1 Skapa nyckelpar

Rotcertifikatutfärdaren skapar nycklar baserat på ett inmatat slumptal som är tillräckligt långt och som har spakats så att det kalkylmässigt är omöjligt att spåra även om man vet när och med vilken maskin det har skapats. Dessutom uppfyller den algoritm

och det genereringssätt som används för att generera slumptalet de kvalitetskrav som ställs. Kraven gäller bl.a. tillförlitligheten hos algoritmen, att genereringsmetoden inte kan upprepas och att slumptalet de facto är slumpmässigt. Rotcertifikatutfärdaren publicerar inte den exakthet och metod som använts för sannolikheten.

Rotcertifikatutfärdare:

Rotcertifikatutfärdaren skapar privata nycklar för signering och offentliga nycklar som motsvarar de privata nycklarna för signering. Nycklarna förvaras i de nyckelförvaringsapparater (HSM) som administreras av rotcertifikatutfärdaren. Den utrustning som används för att administrera nycklarna har den säkerhetsnivå som behövs för att producera kvalificerade certifikatet.

6.1.2 Överlämnande av en privat nyckel till den som ansöker om certifikatutfärdarens certifikat

Den som ansöker om certifikatutfärdarens certifikat skapar själv en hemlig och en öppen nyckel.

6.1.3 Leverans av den öppna nyckel som den som ansöker om certifikatutfärdarens certifikat skapat till rotcertifikatutfärdaren

Den som ansöker om certifikatutfärdarens certifikat skickar den certifikatbegäran som skapats till registreraren och utifrån detta skapas certifikatutfärdarens certifikat.

6.1.4 Distribution av rotcertifikatutfärdarens öppna nyckel till innehavaren av certifikatutfärdarens certifikat

Rotcertifikatutfärdarens öppna nyckel finns i certifikatutfärdarens certifikat som även fritt kan distribueras och finns tillgänglig i det allmänna registret samt på rotcertifikatutfärdarens webbtjänst.

6.1.5 Längden på nycklar

Rotcertifikatutfärdarens privata nyckel som använts för signering av ett certifikat och certifikatutfärdarens motsvarande öppna nyckel är 4 096 bitars RSA-nycklar och 384 bitars ECC-nycklar.

De privata och öppna nycklar som innehavaren av certifikatutfärdarens certifikat har är 4096-bitars RSA-nycklar och 384 bitars ECC-nycklar.

6.1.6 Nycklarnas användningsändamål

Fältet som gäller nyckelanvändningen (key usage) på certifikaten anger användningsändamålet för den privata och öppna nyckeln som är kopplad till utfärdarens certifikat och beskrivs för respektive certifikattyp i certifikatpolicyerna (till exempel signering av certifikaten eller signering av spärrlistorna).

Rotcertifikatutfärdarens certifikat:

Ändamål: Signering av certifikatutfärdarnas certifikat och spärrlistor.

6.2 Skydd av hemlig nyckel

6.2.1 Standarder som gäller säkerhetsmodulen

Rotcertifikatutfärdarens privata nycklar förvaras i kryptografiska moduler som administreras av rotcertifikatutfärdaren och som är förenliga med kraven i tillämpliga säkerhetsstandarder.

Rotcertifikatutfärdaren ser till att rotcertifikatutfärdarens privata nycklar är skyddade så att de inte kan röjas eller missbrukas. Säkerhetskopior tas på rotcertifikatutfärdarens privata nycklar på det sätt som fordras för den kritiska datasäkerheten.

6.2.2 Personal som medverkar i behandlingen av rotcertifikatutfärdarens privata nyckel

För att skapa en privat nyckel för rotcertifikatutfärdaren fordras att minst två personer samtidigt är närvarande eller aktiverar funktionen.

6.2.3 Överlåtelse av hemlig nyckel till betrodd part

Den organisation som är innehavare av certifikatutfärdarens certifikat ska förvara sin privata nyckel i en säker miljö och förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.

6.2.4 Säkerhetskopia av hemlig nyckel

Rotcertifikatutfärdarens privata nycklar och deras säkerhetskopior förvaras starkt krypterade på utrustning som uppfyller kraven på säkring av kritisk information.

6.2.5 Arkivering av privat nyckel

Rotcertifikatutfärdarens privata nycklar förvaras i kryptografiska moduler som administreras av utfärdaren.

Den organisation som är innehavare av certifikatutfärdarens certifikat ska förvara sin privata nyckel i en säker miljö och sträva efter att förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.

6.2.6 Administrering av privat nyckel i kryptografiska moduler

Rotcertifikatutfärdarens privata signeringsnycklar skyddas med fysiska och logiska säkerhetsåtgärder av hög tillitsnivå. De används bara i system som förlagts till en säker miljö. Användningen av nycklarna övervakas med hjälp av speciella administrationskort som skyddats mot obehörig användning.

De personer som arbetar med rotcertifikatutfärdarens betrodda uppgifter besitter administrationskort som är skyddade med PIN-kod. Personens rätt att använda certifikatsystemet eller andra system som gäller certifieringen konstaters med hjälp av dessa administrationskort.

Då användningen av rotcertifikatutfärdarens nyckel avslutas förstörs nyckeln så att den inte längre kan användas eller skapas på nytt. Samtidigt förstörs nyckelns säkerhetskopior. Metoderna för att förstöra maskiner som gått sönder har ordnat så att

man kan förstöra både privata nycklar som sparats på maskinen och i programmen på ett tillförlitligt sätt (t.ex. genom att tillräckligt många gånger skriva över dem).

6.3 Övriga omständigheter i anslutning till nyckeladministration

6.3.1 Arkivering av öppen nyckel

Rotcertifikatutfärdaren arkiverar alla certifierade öppna nycklar.

6.3.2 Användningstiden för öppna och hemliga nycklar

Användningstiden för certifikatutfärdarens certifikat bestäms i avtalet om leveransen av certifikatet. Certifikatutfärdarens certifikat kan spärras under sin giltighetstid om avtalsvillkoren inte iakttas eller om det framkommer andra, i certifieringspraxisen nämnda anledningar att spärra certifikatet.

6.4 Säkerhetskrav i anslutning till användningen av och åtkomsten till datorer

6.4.1 Utrustningens säkerhet

För rotcertifikatutfärdarens certifikatsystem används bara ändamålsenlig utrustning.

Hårdvarusäkerheten har förverkligats i enlighet med god informationsförvaltningssed så att man vid problem med systemet kan övergå till att använda ett reservsystem utan att riskera konfidentialiteten, integriteten och användbarheten hos systemet. Tillgången till reservdelar för utrustning som är oumbärlig för verksamheten har säkrats.

Vid serviceförfaringssättet har utomstående personals tillträde till system som serviceproduktionen ansvarar för förhindrats. Endast en teknisk leverantör som ingått ett tekniskt leveransavtal och ett sekretessavtal kan utföra servicebesöket. Listan med godkända tekniska leverantörer hålls uppdaterad.

Servicebesöken är möjliga endast under övervakning av systemets administratör eller en person med fullmakt av denna.

Den hårdvara som ingår i rotcertifikatutfärdarens certifikatsystem övervakas dygnet runt.

6.5 Hantering av certifikatsystemets livscykel

Myndigheten för digitalisering och befolkningsdata upprätthåller i egenskap av rotcertifikatutfärdare en klassificering av mål och system för certifikattjänsterna, deras tryggande, prioritering och minimiunderhåll.

6.5.1 Övervakning av systemutvecklingen

Rotcertifikatutfärdarens certifikatsystem utvecklas och testas i en separat testmiljö. Endast testade, fungerande och godkända lösningar överförs till produktionssystemet.

6.5.2 Hantering av säkerhet

Informationssäkerheten på Myndigheten för digitalisering och befolkningsdata som är rotcertifikatutfärdare hanteras i enlighet med Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy och standarden ISO 27001.

6.6 Säkerheten i datanätet

Säkerheten i rotcertifikatutfärdarens datakommunikation har garanterats så att datanätet för certifikatsystemet utgör en helhet som separerats från andra datanät och vars kritiska delar finns i dubbla uppsättning. Varken meddelanden som förmedlas i nätet eller deras avsändare eller mottagare röjs för obehöriga utan särskilda åtgärder. Nätet används bara för uppgifter med anknytning till rotcertifikatutfärdarens certifikatsystem. Onödiga webbtjänster har tagits ur bruk. Nätet har indelats i logiska delar mellan vilka förbindelserna är begränsade. Det finns tillräckliga metoder för autentisering, passagekontroll och oavsiktlighet.

6.7 Övervakningen av användningen av kryptiska moduler

Rotcertifikatutfärdaren ser till att rotcertifikatutfärdarens privata nycklar är skyddade så att de inte kan röjas eller missbrukas. Säkerhetskopior tas på rotcertifikatutfärdarens privata nycklar på det sätt som fordras för den kritiska datasäkerheten.

Användningen av den kryptografiska modulen kräver alltid ett kort för att identifiera personen och konstatera användarrättigheten. Modulen kan ställas in i aktivt läge endast med systemanvändarens personliga administrationskort.

För att skapa ny användarrättighet på användarnivå krävs samtidig närvaro av två personer med administrationsrättigheter för systemet och deras motsvarande personliga administrationskort. En modul samlar logguppgifter om transaktionerna.

7 Utfärdarens profiler för certifikat och spärrlistor

7.1 Tekniska uppgifter om certifikat

Rotcertifikatets datainnehåll beskrivs i dokumentet FINEID S2. Dokumentet finns på rotcertifikatutfärdarens webbplats https://dvv.fi/sv/.

7.2 Spärrlistprofil

Datainnehållet i de spärrlistor som rotcertifikatutfärdaren publicerar beskrivs i dokumentet FINEID S2. Dokumentet finns på rotcertifikatutfärdarens webbplats, https://dvv.fi/sv/.

8 Hantering av dokument innehållande bestämmelser

8.1 Ändring av bestämmelser

Rotcertifikatutfärdaren kan ändra specifikationerna med anledning av krav i lagstiftningen eller funktionella krav. Ändringar i bestämmelserna ska föras in i certifikatpolicy- och certifieringspraxishandlingarna på det sätt som beskrivs här näst.

8.2 Publicering och information

Rotcertifikatutfärdaren publicerar certifikatpolicyn och certifieringspraxisen på sin webbplats och på https://dvv.fi/sv/certifikatpolicydokument.

Offentliga bestämmelser relaterade till rotutfärdarens produktion av certifikat är tillgängliga på samma webbplats.

Avtal som ingåtts med datatekniska leverantörer om leverans av certifikat samt beskrivningar av produktionssystem och bestämmelser om produkter är konfidentiella.

8.3 Förfarande för ändring och godkännande av certifieringspraxis

Myndigheten för digitalisering och befolkningsdata godkänner rotcertifikatutfärdaren samt såväl certifikatpolicyn som certifieringspraxisen för certifikat. Rotcertifikatutfärdarens dokument kan ändras genom Myndigheten för digitalisering och befolkningsdatas interna ändringsförfarande.

Myndigheten för digitalisering och befolkningsdata informerar om ändringar på sin webbplats i god tid innan de träder i kraft.

Myndigheten för digitalisering och befolkningsdata förvaltar de olika versionerna av dokument och arkiverar samtliga certifikatpolicy- och certifieringspraxishandlingar. Typografiska korrigeringar och ändringar av kontaktuppgifter kan göras omedelbart.

1. Samtliga punkter i certifikatpolicyn och certifieringspraxisen kan ändras genom att anmäla kommande väsentliga ändringar 30 dagar innan de träder i kraft.

2. Punkter som inte enligt Myndigheten för digitalisering och befolkningsdata märkbart påverkar certifikatinnehavare och förlitande parter kan ändras genom att meddela om ändringarna 14 dagar innan de träder i kraft.