MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIKATPOLICY FÖR FINSKA STATENS ROTCERTIFIKATUTFÄRDARE

OID: 1.2.246.517.1.10.301
OID: 1.2.246.517.1.10.351

29.9.2022

Tel. **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi/sv**

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio
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	Tillagd information om loggdata	1.10.2021/VA
v 1.2	Uppdaterade versionen och länkarna till CPS dokument	29.9.2022/SK

Innehållsförteckning

CERTIFIKATPOLICY FÖR FINSKA STATENS ROTCERTIFIKAT-UTFÄRDARE

Definitioner och förkortningar

Definitioner

Nyckelpar: Nycklar som används tillsammans inom ett öppet nyckelssystem, varav den ena är publik 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 publik och en privat nyckel. Ett meddelande som krypterats med publik nyckel kan endast öppnas med den privata nyckeln i nyckelparet i fråga.

Publik nyckel: Den publika delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatutfärdaren bekräftar med sin digitala signatur att den publika nyckeln innehas av certifikatets innehavare. Den publika 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 enhetliga kod OID är en del av datainnehållet i varje certifikatutfärdares certifikat som beviljats av rotcertifikatutfärdaren.

Förkortningar

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy

CPS	Certification Practise Statement
CRL	Certificate Revocation List
EEC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HST	Elektronisk identifiering av en person (Henkilön sähköinen tunnistaminen)
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO IEC 27001
LDAP	Lightweight Directory Access Control
OCSP	Online Certificate Status Protocol, tjänst för verifiering av certifikatstatus i realtid
OID	Object Identifier
PDS beskrivning	PKI Disclosure Statement, certifikat-
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SIM	Subscriber Identity Module
MDB ningsdata	Myndigheten för digitalisering och befolk-

1 Inledning

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.

Den här certifikatpolicyn tillämpas då rotcertifikatutfärdarens (DVV GOV. Root CA – G3 RSA och DVV GOV. Root CA – G3 ECC) beviljar certifikatutfärdarens certifikat.

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 befolkningsdata erbjuder beträffande informationssäkerheten förstklassiga certifikat för elektroniska betrodda tjänster och elektronisk identifiering samt relaterade tjänster för den offentliga och den privata sektorn.

Myndigheten för digitalisering och befolkningsdata (MDB) hör till finansministeriets förvaltningsområde. MDB är en myndighet som upprätthåller personregisterEnligt lagen om Myndigheten för digitalisering och befolkningsdata (661/2009) har MDB till uppgift att producera tjänster inom certifierad elektronisk kommunikation. Sedan 1.12.2010 har Myndigheten för digitalisering och befolkningsdata varit lagstadgad certifikatutfärdare för hälso- och sjukvården (lag om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lag om elektroniska recept (61/2007). MDB har tillhandahållit certifikatbaserade signerings- och autentiseringsverktyg sedan år 1999 och utfärdat signeringscertifikat på europeiskt godkänd nivå sedan 31.3.2003. Myndigheten för digitalisering och befolkningsdata erbjuder även andra betrodda tjänster.

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 är finska statens rotcertifikatmyndighet och godkänner enligt sin certifikatpolicy de certifikat som beviljats och signerats av Myndigheten för digitalisering och befolkningsdata.

Myndigheten för digitalisering och befolkningsdata skapar finska statens rotcertifikat. Förtroendestrukturen som baserar sig på finska statens rotcertifikat är hierarkiskt. Myndigheten för digitalisering och befolkningsdata godkänner enligt sin certifikatpolicy de certifikat som beviljats och signerats av Myndigheten för digitalisering och befolkningsdata. Utfärdaren kan vara antingen en offentlig eller en privat organisation.

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 betrodda tjänster 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. Detta dokument beskriver de principer som rotcertifikatutfärdaren iakttar vid utfärdandet av certifikatutfärdarens certifikat antingen för Myndigheten för digitalisering och befolkningsdata eller för någon annan organisation. Rotcertifikatutfärdaren beviljar inte certifikat för slutanvändare. Certifikat för slutanvändare utfärdas av utfärdare certifierade av rotcertifikatutfärdaren. Var och en av dessa har en egen certifikatpolicy och en egen certifieringspraxis.

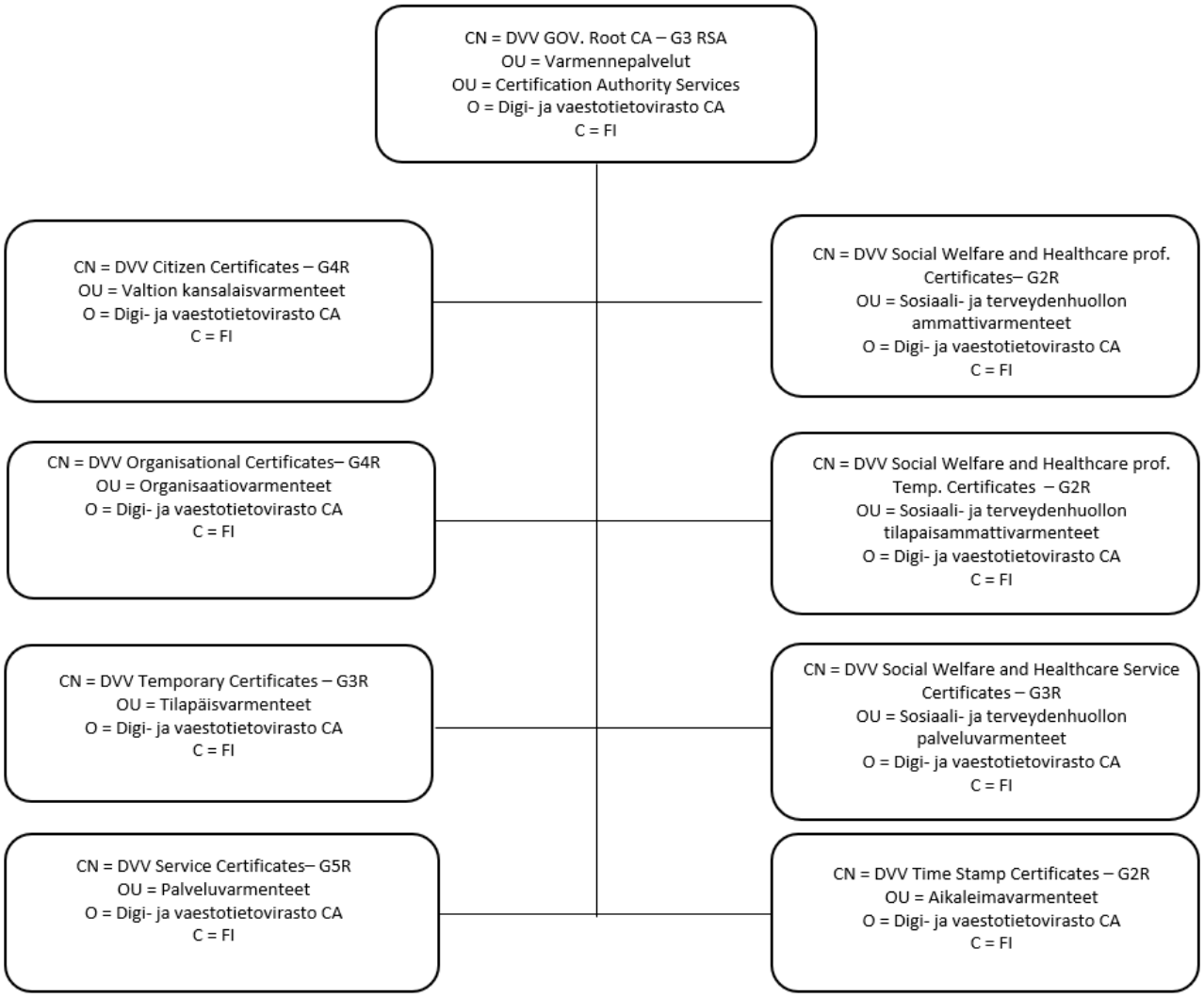

Bild 1. Certifikathierarkin RSA

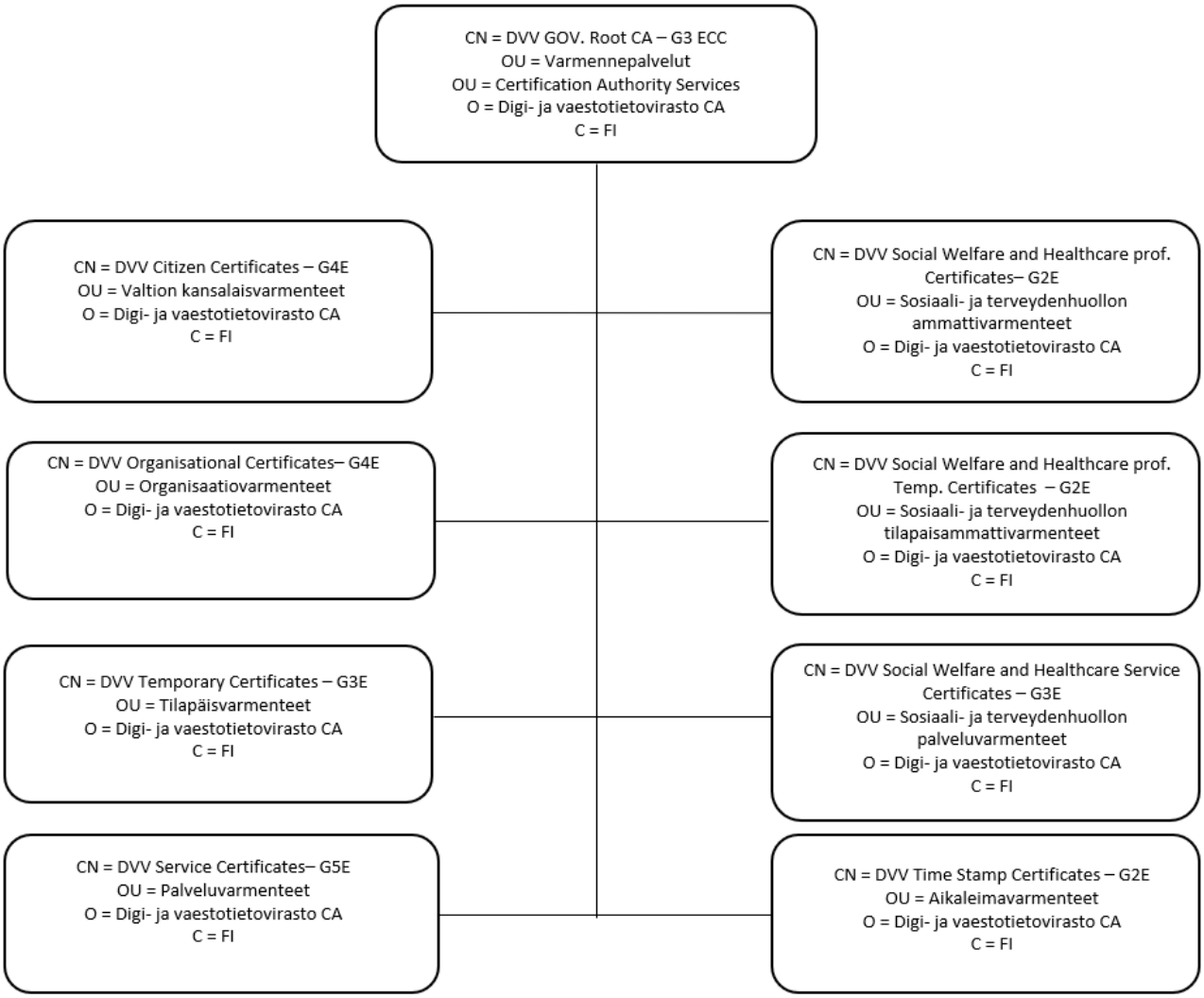

Bild 2. Certifikathierarkin ECC

Certifikathierarkin är följande

Rotcertifikatet:

Myndigheten för digitalisering och befolkningsdatas rotcertifikat

- CN = DVV Gov. Root CA – G3 RSA
- OID: 1.2.246.517.1.10.301
- CN= DVV Gov. Root CA – G3 ECC
- OID: 1.2.246.517.1.10.351

- Utfärdarens certifikat Statens medborgacertifikat

- CN = DVV Citizen Certificates - G4R
- OID: 1.2.246.517.1.10.301.1
- CN = DVV Citizen Certificates - G4E
- OID: 1.2.246.517.1.10.351.1

- Organisationscertifikat
  - CN = DVV Organisational Certificates - G4R
  - OID: 1.2.246.517.1.10.301.2
  - CN = DVV Organisational Certificates - G4E
  - OID: 1.2.246.517.1.10.351.2
- Servicecertifikat
  - CN = DVV Service Certificates - G5R
  - OID: 1.2.246.517.1.10.301.4
  - CN = DVV Service Certificates - G5E
  - OID: 1.2.246.517.1.10.351.4
- Yrkescertifikat för social- och hälsovården
  - CN = DVV Social Welfare and Healthcare Prof. Certificates - G2R
  - OID: 1.2.246.517.1.10.301.5
  - CN = DVV Social Welfare and Healthcare Prof. Certificates - G2E
  - OID: 1.2.246.517.1.10.351.5
- Servicecertifikat för social- och hälsovården
  - CN = DVV Social Welfare and Healthcare Service Certificates - G3R
  - OID: 1.2.246.517.1.10.301.7
  - CN = DVV Social Welfare and Healthcare Service Certificates - G3E
  - OID: 1.2.246.517.1.10.351.7
- Certifikat för tidsstämpel

- CN = DVV Time Stamp Certificates - G2R
- OID: 1.2.246.517.1.10.301.8
- CN = DVV Time Stamp Certificates - G2E
- OID: 1.2.246.517.1.10.351.8

- CN = VRK Gov. Root CA
  - OID: 1.2.246.517.1.10.1
  - Tillfälliga certifikat
    - CN = DVV Temporary Certificates - G3R
    - OID: 1.2.246.517.1.10.301.3
    - CN = DVV Temporary Certificates - G3E
    - OID: 1.2.246.517.1.10.351.3
  - Tillfälligt yrkescertifikat för social- och hälsovården
    - CN = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R
    - OID: 1.2.246.517.1.10.301.6
    - CN = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E
    - OID: 1.2.246.517.1.10.351.6

Certifikatutfärdarens certifikat innehåller utfärdarens öppna nyckel, namn, certifikatets användningssyfte 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 certifikatpolicyn grundar sig på systemet med öppen nyckel.

Alla certifikat som utfärdas för slutanvändarna liksom spärrlistorna signeras elektroniskt med den privata nyckel som motsvarar den öppna nyckeln. 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 eller en) för varje certifikat för utfärdare som utfärdats av rotcertifikatutfärdaren.

Certifikatpolicyerna beskriver vilka förfaranden som ska iakttas i Myndigheten för digitalisering och befolkningsdatas certifikatverksamhet, användningsvillkoren,

ansvarsfördelningen och andra aspekter på användningen av certifikat på ett allmänt plan. Certifieringspraxisen ger en detaljerad beskrivning av förfaringssätten.

Loggdata relaterat till utfärdande och spärrning av certifikat lagras minst sju (7) år efter certifikatets giltighetstid.

1.2 Identifikationsuppgifter

Denna certifikatpolicy heter Certifikatpolicy för finska statens rotcertifikatutfärdare och dess entydiga kod är OID 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 certifikatpolicy och ansvarar för att de fungerar enligt rotcertifikatutfärdarens ansvar som beskrivs i kapitel 2.2.1. Rotcertifikatutfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifikatpolicy är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är finska statens rotcertifikatmyndighet. Certifikaten utfärdas av Myndigheten för digitalisering och befolkningsdata som är en myndighet som upprätthåller ett personregister samt tillhandahåller suomi.fi-tjänster och producerar certifikattjänster enligt lagen om befolkningsdatasystemet och Befolkingsregistercentralen har till uppgift att producera certifikattjänster för elektronisk kommunikation.

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 certifikat och publicering av spärrlistor

1.3.2 Registrerare

Rotcertifikatutfärdaren ansvarar för alla registreringsuppgifter för certifikatutfärdarens certifikat.

Registreraren identifierar certifikatutfärdarens certifikatsökande 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 som en offentlig tjänst tillgänglig på servern ldap.fineid.fi.

1.3.4 Organisation som innehar certifikatutfärdarens certifikat

Denna certifikatpolicy redogör för rotcertifikatutfärdarens förfarande när certifikat för certifikatutfärdare utfärdas för bruk av Myndigheten för digitalisering och befolkningsdata eller någon annan organisation.

Innehavaren av certifikatutfärdarens certifikat 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 certifikatutfärdarens certifikatuppgifter. En förlitande part ska kontrollera att det certifikat som används är i kraft och att certifikatutfärdarens certifikat inte tagits upp på spärrlistan.

1.3.6 Användning av certifikatutfärdarens certifikat

Enligt den här certifikatpolicyn beviljar rotcertifikatutfärdaren certifikatutfärdares certifikat på det sätt som föreskrivs angående certifikatutfärdarens certifikat i certifieringspraxisen. Användningssyftet för certifikatutfärdarens certifikat är till exempel att signera certifikat som beviljar medborgarcertifikat och 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 förvaltar certifikatpolicyn

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

1.4.2 Kontaktperson

Myndigheten för digitalisering och befolkningsdata

PB 123 (Fågelviksgränden 2) Tfn +358 295 535 001

00531 Helsingfors Fax +358 9 876 4369

FO-nummer: 0245437-2 kirjaamo@dvv.fi

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2 Allmänna villkor

Den här certifikatpolicyn träder i kraft 1.10.2021. Ändringsförfarandet för och publikationen av certifikatpolicyn 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 kan bevilja certifikat åt sin egen verksamhet. I så fall följer den samma förutsättningar som om certifikatet skulle beviljas åt någon annan organisation.
- 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 beskrivs i certifieringspraxisen i fråga. 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 sträva efter att förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.

Innehavarorganisationen ska omedelbart underrätta rotcertifikatutfärdaren om man känner till eller misstänker att innehavaren av certifikatutfärdarens privata nyckel har röjts. Då spärrar rotcertifikatutfärdaren det aktuella certifikatet för certifikatutfärdare och publicerar det på spärrlistan (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 certifikatutfärdarens certifikat 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 certifikat 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.

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

Rotcertifikatutfärdaren ansvarar för att certifikatutfärdarens certifikat enligt avtalet har överlämnats till en organisation som har identifierats på det sätt som certifikatutfärdarens certifikat förutsätter.

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 Rotcertifikatutfärdaren ansvarar för registreringens del för skadeståndsavtalet enligt detta kapitel.

Myndigheten för digitalisering och befolkningsdata kan även bevilja certifikatet för egna syften. Då efterföljer den samma krav som de övriga organisationerna.

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

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 eller underhåll av spärrlistan meddelas på förhand.

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

Certifikatutfärdarens certifikatinnehavares ansvar för användningen av certifikatet upphör då en representant för certifikatinnehavarens organisation har meddelat rotcertifikatutfärdaren de uppgifter som behövs för att spärra certifikatet. 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

Rotcertifikatutfärdaren har ett skadeståndsansvar gällande sin verksamhet. Detta baserar sig på samarbetsavtal samt på lagstadgade skyldigheter.

2.3.2 Övriga parter

En part som litar på certifikatutfärdarens certifikat kan lita på certifikatet 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 en nettobudgeterad myndighet under finansministeriet. Ungefär två tredjedelar av kostnaderna täcks med avgifter. Myndigheten för digitalisering och befolkningsdata ekonomiska förvaltning utgår från lagar och förordningar om statens ekonomi samt finansministeriets och Statskontorets bestämmelser. Statens revisionsverk granskar Myndigheten för digitalisering och befolkningsdata regelbundet. 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).

2.4.2 Avgörande av meningsskiljaktigheter

Vid utfärdandet av certifikat ansvarar rotcertifikatutfärdaren för att certifikatutfärdarnas certifikat uppfyller kraven i denna certifikatpolicy.

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 Myndigheten för digitalisering och befolkningsdata.

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 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 Myndigheten för digitalisering och befolkningsdatas giltiga 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 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 med spärrade certifikatutfärdares certifikat. Spärrlistan 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://dvv.fi/sv/certifikatpolicydokument.

2.6.4 Dataförvaring

De uppgifter som Myndigheten för digitalisering och befolkningsdata i sin egenskap som rotcertifikatutfärdare publicerar finns tillgängliga 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.

2.7 Dataskyddsgranskning

2.7.1 Granskningsfrekvens

Rotcertifikatutfärdaren Myndigheten för digitalisering och befolkningsdata dataskyddsgranskar lokalerna, maskinerna och verksamheten hos den organisation som innehar certifikatutfärdarens certifikat 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.

2.8 Publicering av information

2.8.1 Uppgifter publicerade av rotcertifikatutfärdaren

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

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

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

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

Certifikatsystemets uppgifter överlämnas endast för de syften som beskrivs i detta kapitel.

2.8.2 Övriga principer gällande utlämnande av information

Med tanke på tillförlitligheten hos certifikatutfärdaren är det av största vikt att Myndigheten för digitalisering och befolkningsdata 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 samt de certifikat som Befolkningscentralen utfärdat i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata äger samtliga ägande- och användarrättigheter för denna certifikatpolicy.

3 Identifiering av den som ansöker om certifikatutfärdarens certifikat

3.1 Registrering

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

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 den som söker certifikatutfärdarens certifikat reglerna och villkoren för användningen av certifikatet 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

Rotcertifikatutfärdaren:

Digi- ja väestötietoviraston juurivarmentajat ovat:

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

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 den som innehar 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 Begäran om spärrning

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

Representanten för den organisation som innehar certifikatutfärdarens certifikat ska meddela rotcertifikatutfärdaren omedelbart på det sätt som nämns i avtalet om man känner till eller misstänker att den privata nyckeln till certifikatutfärdarens certifikat har avslöjats. Då spärrar utfärdaren rotcertifikatutfärdaren certifikatet i fråga. Begäran om att spärra certifikatutfärdarens certifikat görs i första hand av innehavaren av 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 certifikatutfärdarens certifikat. I avtalet nämns bägge parters rättigheter och skyldigheter. Enligt ansökningshandlingen och bruksvillkoren ska den som ansöker om certifikatutfärdarens certifikat med sin underskrift intyga att de angivna uppgifterna är korrekta och godkänner att certifikatet skapas och att det publiceras i 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

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

Utfärdaren 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 utfärdaren om man känner till eller misstänker att innehavaren av certifikatutfärdarens privata nyckel har röjts. Då spärrar utfärdaren 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.

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

Rotcertifikatutfärdaren spärrar de certifikatutfärdares certifikat som utfärdats om det påträffas fel i certifikatets 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.

Rotutfärdaren kan 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 Myndigheten för digitalisering och befolkningsdatas certifikat för certifikatutfärdaren har röjts eller på annat vis blivit oanvändbar ska Myndigheten för digitalisering och befolkningsdata meddela det inträffade till samtliga innehavarorganisationer av certifikatutfärdarens certifikat och slutanvändarna på ändamålsenligt sätt.

Rotcertifikatutfärdaren kan spärra ett certifikat av särskild anledning.

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

4.4.2 Publiceringsfrekvens för spärrlista

Certifikatutfärdarens certifikat publiceras i det offentliga registret och finns i registret under hela dess giltighetstid. Utfärdaren publicerar en spärrlista som är i kraft i 72 timmar efter publiceringen. 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.

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

4.4.3 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 certifikatutfärdaren 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 rotcertifikatutfärdarens 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.

4.7 Hantering av kontinuerlig verksamhet och undantagsfall

Rotcertifikatutfärdaren har en kontinuitets- och beredskapsplan som gör att rotcertifikatutfärdarens verksamhet kan fortsätta i exceptionella situationer. Rotcertifikatutfärdarens åtgärder vid exceptionella situationer beskrivs i certifieringspraxisen.

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. Rotcertifikatutfärdarens åtgärder vid exceptionella situationer beskrivs i certifieringspraxisen.

5 Fysiska krav, funktionella krav och krav på personalens säkerhet

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

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom rotcertifikatverksamheten. Rotcertifikatutfärdaren ansvarar i egenskap av certifikatutfärdare för säkerheten och funktionerna inom samtliga delområden av certifikatproduktionen. Rotcertifikatutfärdarens åtgärder vid exceptionella situationer beskrivs i detalj i certifieringspraxisen.

Om någon annan organisation än rotcertifikatutfärdaren utfärdar certifikat för slutanvändare med utgångspunkt i certifikatutfärdarens certifikat ska organisationen dessutom iaktta de egna riktlinjerna för informationssäkerheten.

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.

Rotcertifikatutfärdaren skapar privata nycklar för signering och publika nycklar som motsvarar de privata nycklarna för signering. Nycklarna förvaras i de nyckelförvaringsapparater (HSM) som administreras av rotcertifikatutfärdaren.

6.1.2 Längden på nycklar

Rotcertifikatutfärdarens privata nyckel som använts för signering av rotcertifikatutfärdarens certifikat och den motsvarande öppna nyckeln är 4 096 bitars RSA-nycklar.

Längderna på den privata och öppna nyckel som innehas av innehavaren av rotcertifikatutfärdarens certifikat beskrivs i certifieringspraxisen.

6.1.3 Nycklarnas användningsändamål

Fältet som gäller nyckelanvändningen (key usage) på certifikaten anger användningsändamålet för den privata och öppna nyckeln som är kopplad till rotcertifikatutfärdarens certifikat.

6.2 Skydd av privat nyckel

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.

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

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.

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

Certifikatutfärdarens 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.

6.3 Övriga omständigheter i anslutning till nyckeladministration

Rotcertifikatutfärdaren arkiverar alla certifierade öppna 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

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.

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.

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 certifikatutfärdarens certifikatsystem. Nätet har indelats i logiska delar mellan vilka förbindelserna är begränsade.

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.

En modul samlar logguppgifter om transaktionerna.

7 Utfärdarens profiler för certifikatutfärdarens certifikat och spärrlistor

7.1 Tekniska uppgifter om certifikatutfärdarens certifikat

Datainnehållet rotcertifikatet och certifikatutfärdarens certifikat 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/certifikatpolicydokument.

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 specifikationerna ska föras in i certifikatpolicy- och certifieringspraxisdokumenten på det sätt som beskrivs i det följande.

8.2 Publicering och information

Rotcertifikatutfärdaren publicerar certifikatpolicyn och certifieringspraxisen som finns tillgängliga på webbplatsen 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 certifikatpolicyn

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 dokumentversionerna och arkiverar samtliga certifikatpolicy- och certifieringspraxisdokument. 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.

[Yksikkö] / Aarnio Ville 1.6.2021