MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIERINGSPRAXIS MEDBORGAR-CERTIFIKAT

För Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat på identitetskort

OID: 1.2.246.517.1.10.302.1
OID: 1.2.246.517.1.10.352.1

29.9.2022

[Yksikkö] / Kytölä Sanni

29.9.2022

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	Uppdaterade versionen och länkarna till CPS dokument	29.9.2022/SK

Innehållsförteckning

1 Definitioner och förkortningar

1.1 Definitioner

Aktiveringsuppgift: En sådan konfidentiell uppgift som behövs för aktivering av privata nycklar med chips och användning av dessa med en öppen nyckelmetod (t.ex. elektronisk signatur).

Aktiveringskod Användaren av medborgarcertifikatet för en personlig aktiveringskod för användning av kortet, varefter användaren kan aktivera och fastställa sina egna, personliga PIN-koder. Efter aktiveringsprocessen kan användaren använda sitt identitetskort vid elektronisk kommunikation.

Nyckelpar: Nycklar som används tillsammans med en öppen nyckelmetod, varav den ena är publik och den andra privat. Nycklarnas användningssyfte är fastställt i certifikatet (se certifikatinnehavarens signaturcertifikat samt verifikations- och krypteringscertifikat).

ECC-algoritm och ECC-nyckel: ECC-algoritmen omfattar olika algoritmer som anknyter till krypteringsmetoder baserade på elliptiska kurvor och som bildar ett krypteringssystem med publik nyckel. ECC-nyckeln har en publik och privat nyckeln såsom RSA-nyckelparet.

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.

Identitetskort: Identitetsbevis som beviljats av polisen och som har en teknisk del försedd med kortinnehavarens medborgarcertifikat.

Publik nyckel: Den publika delen av nyckelparet som används för icke-symmetrisk kryptering med en öppen nyckelmetod. 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: Dataskyddsinfrastruktur där dataskyddstjänster produceras med en öppen nyckelmetod.

Öppen nyckelmetod: Dataskyddstjänst, exempelvis elektronisk identifiering av personer, som produceras genom att använda publika och privata nycklar, certifikat och icke-symmetrisk kryptering.

Medborgarcertifikat: Ett signaturcertifikat som Myndigheten för digitalisering och befolkningsdata beviljat en fysisk person och vars datainnehåll fastställs i lagen om Myndigheten för digitalisering och befolkningsdata (661/2009).

Kortläsarprogrammet: Kortläsarprogrammet används i arbetsstationen som s.k. slutanvändarens applikation. Med hjälp av detta kan användaren utnyttja sitt identitetskort och de certifikat som finns på kortet i olika användnings- och applikationsmiljöer, t.ex. vid elektronisk ärendehantering, säkerhetspost och inloggning i arbetsstationen.

Signaturcertifikat: Certifikat vars innehåll motsvarar det innehåll som fastställs för signaturcertifikat i lagen och som utfärdaren som erbjuder signaturcertifikat och som uppfyller kraven i lagen har beviljat. Signaturcertifikatets datainnehåller har fastställts i lagen om stark autentisering och betrodda elektroniska tjänster.

Förlitande part: Den part som litar på uppgifterna i certifikatet och använder certifikatet för olika dataskyddstjänster, såsom elektronisk autentisering av certifikatets innehavare och konstaterande av digital signatur.

Betalkort: En allmän benämning på bank-, kredit-, kombinations-, kontant- och betaltidskort.

Chips: Ett tekniskt underlag på vilket certifikatet och de privata nycklarna finns och som finns på identitetskort, betalkort eller mobilenhetens kort.

Mobilenhet: En mobiltelefon eller en annan mobilenhet med vilken certifikatet och de privata nycklar på chipset kan användas.

PIN-kod Aktiveringsuppgift med vilken den privata nyckeln på chipset aktiveras för användning. PIN 1: baskod för verifiering och kryptering. PIN 2: signaturkod för elektronisk signatur.

Registrerare: Registreraren identifierar sökandens personlighet i enlighet med den certifikatpolicyn och certifieringspraxisen för utfärdarens del och på dennes ansvar.

RSA-algoritm och RSA-nyckel: RSA-algoritm är en allmänt använd algoritm för publik nyckel.

En del av nyckelparen för medborgarcertifikatet är RSA-nycklar.

Spärrlista: En förteckning som signeras och publiceras elektroniskt av certifikatutfärdaren över certifikat som spärrats under deras giltighetstid och tidpunkten för spärrning. Av spärrlistan framgår publiceringstidpunkt samt tidpunkten för publiceringen av nästa spärrlista. Spärrade certifikat förs in på spärrlistan.

Spärrtjänst: En teknisk leverantör som tar emot och förmedlar begäran om spärrning av certifikat till certifikatsystemet för utfärdarens del.

Elektronisk kontaktkod: En kod som består av siffror och kontrolltecken och används för att identifiera en finsk medborgare eller en utlänning som är stadigvarande bosatt i Finland och som har införts i befolkningsdatasystemet.

Certifikat: Ett elektroniskt intyg som kopplar uppgifterna om verifieringen av en signatur till den som gjort signaturen och bekräftar signeraren. Certifikatet innehåller en medföljande unik kod enligt certifieringspraxis.

Certifikatsystem: Ett datatekniskt system för att skapa certifikat och signera spärrlistor.

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

Certifikatpolicy: Ett dokument där man beskriver principerna för beviljande av certifikat samt ansvarsområdena för de förlitande parterna. Myndigheten för digitalisering och befolkningsdatas publicerade certifikatpolicyn är offentligt tillgängliga. Varje policy identifieras av en egen kod.

Certifikatregister: Ett register som en utfärdare som tillhandahåller signaturcertifikat till allmänheten har skyldighet att hålla enligt lagen om stark autentisering och betrodda elektroniska tjänster. Uppgifterna ska lagras i 10 fem år efter att certifikatets giltighetstid har upphört.

Certifikatdatasystem: Ett datatekniskt system som utgörs av certifikatsystem, datatrafik, certifikatregister och spärrlista, rådgivnings- och spärrtjänst samt hantering av certifikat och kort.

Den identifierande koden inom certifieringspraxisen är en del av certifikatets datainnehåll.

Certifieringspraxis: Beskrivning av hur certifikatutfärdaren förverkligar sin certifikatpolicy. Varje certifieringspraxis identifieras av en egen kod.

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

Certifikatutfärdarens certifikat: Innehåller utfärdarens namn, land och publika nyckel.

Utfärdarens privata nyckel: En privat nyckel som beviljas av certifikatutfärdaren för signering av utfärdarens beviljade certifikat och publicerade spärrlistor.

Certifikatsökande: En person som ansöker om ett medborgarcertifikat och pålitligt identifieras i samband med detta.

Innehavare av certifikat: En person vars data och publika nyckel har bekräftats med utfärdarens elektroniska signatur och som innehar de privata nycklarna för certifikatet.

Certifikatinnehavarens signaturcertifikat: Med publik nyckel med certifikat verifieras certifikatinnehavarens elektroniska signaturcertifikat med motsvarande privat nyckel dvs. signaturnyckel. För signatur krävs en signaturkod (PIN 2).

Certifikatinnehavarens verifikations- och krypteringscertifikat Certifikatet används för elektronisk identifiering av en person och kryptering av data. Certifikatinnehavaren använder sitt privata verifikations- och krypteringscertifikat för elektronisk identifiering och upplösning av kryptering av ett meddelande. För användning av nyckeln krävs en baskod (PIN 1).

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 publika nyckeln och certifikatet vid autentisering av signatur.

Privat nyckel: Den privata delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatinnehavarens privata nycklar har lagrats på ett chips för att skydda dem mot olaglig användning.

1.2 Lista över förkortningar

CA	Certification Authority, certifikatutfärdare
CP	Certificate Policy, certifieringspolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, kryptografisk modul
HST	Elektronisk identifiering av person
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO ICE 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, onlinetjänst för återställande av certifikatets status
OID	Object Identifier, identifierande kod
PDS	PKI Disclosure Statement, certifikatbeskrivning
PIN	Personal Identification Number, PIN-kod
PKI	Public Key Infrastructure, öppet nyckelsystem
RSA	Rivest, Shamir, Adleman, en algoritm för publik nyckel, icke-symmetrisk algoritm
Elektronisk kontaktkod:	
SIM	Subscriber Identity Module
MDB	Myndigheten för digitalisering och befolkningsdata

2 Inledning

Certifikatpolicy 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.

Denna certifieringspraxis tillämpas på Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat på identitetskort som beviljas finska medborgare som registrerats i befolkningsdatasystemet och utlänningar som är stadigvarande bosatta i Finland.

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

2.1 Allmänt

Myndigheten för digitalisering och befolkningsdata erbjuder signatur- och identifieringscertifikat med hög datasäkerhetsnivå samt därtill relaterade tjänster för den offentliga och privata sektorn. Med hjälp av certifikat säkerställs certifikatinnehavarens identitet samt riktigheten, enhetligheten och ursprungligheten av de uppgifter som certifikatet innehåller. En elektronisk signatur som gjorts med signaturcertifikat samt en stark elektronisk personidentifiering med en metod för stark elektronisk autentisering ger medborgarna möjlighet till trygg och flexibel nätkommunikation, oberoende av tid och plats. Certifikatutfärdare av signaturcertifikat och leverantörer av autentiseringstjänster för stark elektronisk autentisering övervakas i Finland av Traficom.

Certifikat är ett elektroniskt intyg som kopplar uppgifterna om verifieringen av en underskrift till den som gjort underskriften och bekräftar certifikatinnehavarens identitet. Certifikatets uppgifter har signerats digitalt med certifikatutfärdarens privata nyckel. Certifikat enligt denna certifieringspraxis utgår från öppet nyckelsystem och öppen nyckelmetod. Informationsinnehållet i certifikat enligt denna certifieringspraxis har fastställts i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) och lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Myndigheten för digitalisering och befolkningsdata (MDB) lyder under finansministeriet. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) är att producera tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdata har också sedan 1.12.2010 varit lagstadgad certifikatutfärdare för hälsovården med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007). Myndigheten för digitalisering och befolkningsdatas certifikattjänster ansvarar för verkets certifikatverksamhet. MDB har utfärdat certifikatbaserade signatur- och autentiseringsmedel sedan 1999 och varit utfärdare av signaturcertifikat sedan 31.3.2003.

MDB:s certifikatdatasystem och certifikattjänster baserar sig på öppet nyckelsystem (Public Key Infrastructure, PKI). MDB:s certifikatinfrastruktur består av certifikatsystemet, leverantören av certifikatuppgifter som ingår i korten, spärrlistan,

rådgivningstjänsten och registertjänsten. I MDB:s funktioner som utfärdare ingår produktion av certifikat-, register- och spärrtjänster, registrering samt tillverkning och specificering av kort som innehåller certifikat. MDB svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Dessa funktioner beskrivs närmare i kapitel 1.3.

Myndigheten för digitalisering och befolkningsdata skapar en separat certfikatpolicy för varje typ av certifikat som den utfärdat som för varje tekniskt underlag för certifieringspraxis. Certifikatpolicy beskriver de förfaringssätt, som används per certifikattyp användarvillkor och ansvarsfördelning och övriga aspekter av användningen av certifikat på ett allmänt plan. Certifieringspraxis beskriver de förfaringssätt som tillämpas på ett detaljerat plan. Varje dokument har sin egen unik OID-kod. Dessa dokument finns elektroniskt tillgängliga på adressen https://dvv.fi/sv/certifikatpolicydokument.

Myndigheten för digitalisering och befolkningsdata, som är certifikatutfärdare, specificerar innehavaren av certifikatet med hjälp av en elektronisk kommunikationskod (SATU), som även är en del av certifikatets datainnehåll. En elektronisk kontakt kod är teknisk identifieringskod som separat skapats för elektronisk ärendehantering enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009). Den innehåller inga identifieringsuppgifter om personen.

Ett medborgar certifikat kan beviljas och sparas på olika tekniska underlag dvs. chips, såsom identitetskort, bankens betalkort med chips och en mobilenhets SIM-kort. Denna certifieringspraxis är en beskrivning av ett medborgarcertifikat på identitetskort.

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 (Förordning) tillämpas på signaturcertifikat för betrodda tjänster från och med 1.7.2016. Kraven som anknyter till regleringen i förordningen har satts i kraft i finsk lagstiftning genom ändringen i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 1.7.2016. Med lagen föreskrivs om tillhandahållandet av tjänster för elektronisk autentisering samt elektronisk signatur och deras rättsverkningar. Om identitetskortet har föreskrivits i lagen om identitetskort (829/1999) och om certifikat beviljade av Myndigheten för digitalisering och befolkningsdata har föreskrivits i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

Certifieringspraxisen som beskriver utfärdandet av detta medborgarcertifikat är registrerad av Myndigheten för digitalisering och befolkningsdata.

Medborgarcertifikatet består av tre olika certifikat med två olika användningsändamål: verifikation och kryptering samt elektronisk signatur. Verifikationscertifikatet är ett medel för elektronisk autentisering enligt ovannämnd lag. Signaturcertifikat är elektroniska signaturmedel enligt lagen om stark autentisering och betrodda elektroniska tjänster. Ett signaturcertifikat som uppfyller samma kravnivå är genomfört baserat på RSA-algoritmen och ett annat baserat på ECC-algoritmen. Certifikatinnehavaren kan använda vilket som helst av dessa certifikat för elektronisk signatur.

Denna certifieringspraxis beskriver de detaljerade krav som gäller utfärdande, produktion och ansvarsfördelning gällande signaturcertifikat för elektronisk signatur

enligt Förordningen och lagen om stark autentisering och betrodda elektroniska tjänster. Signaturcertifikat som beviljas enligt denna certifieringspraxis kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de krav som förutsätts för godkända elektroniska signaturer och medel för skapande enligt artikel 28 och artikel 29 i Förordningen. Nivån av identifieringscertifikatet uppfyller kravnivån ”hög” enligt Förordningen och Säkerhetsnivåförordningen som utfärdats med stöd av den.

Detta dokument beskriver också lösningar och förfaringssätt med beaktande av kraven i produktionsmiljön gällande utfärdande och produktion av och lagring av uppgifter om identifikationscertifikat som utfärdas som ett medel för stark elektronisk autentisering enligt lagen om stark elektronisk autentisering och elektroniska signaturer och som ingår i medborgarcertifikatet.

2.2 Identifikationsuppgifter

Denna certifieringspraxis heter Certifieringspraxis för Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat vars OID är 1.2.246.517.1.10.302.1 och 1.2.246.517.1.10.351.1..

Denna certifieringspraxis syftar till Certifikatpolicyn för Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat, OID 1.2.246.517.1.10.302 och 1.2.246.517.1.10.352.

Myndigheten för digitalisering och befolkningsdata följer certifikatpolicyn som gäller signaturcertifikat som beviljas allmänheten enligt betrodda tjänster i EU-förordningen nr (EU) 910/2014. Dokumentets referensuppgifter är SÖK EN 319 411-1 [2], punkt QCP-n-qscd; OID: 0.4.0.194112.1.2. Signaturcertifikat som beviljas enligt denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de godkända certifikat och medel för skapande som beskrivs i Förordningen.

Både certifikatpolicyn och certifieringspraxisen finns på adressen https://dvv.fi/sv/certifikatpolicydokument.

2.3 Certifikatutfärdare och tillämpningsområden för certifikat

Utfärdaren producerar certifikattjänster enligt villkoren i denna certifieringspraxis och ansvarar för att de fungerar i innehavarens användning enligt 2.2.1 som beskriver utfärdarens ansvar. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifieringspraxis är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) är att producera tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdatas certifikattjänst indelas operativt i följande delområden:

2.3.1 Certifikatutfärdare

Utfärdarens uppgift är att:

- utfärda certifikat- och registertjänster samt spärrtjänster enligt certifikatpolicyn och certifieringspraxisen
- personligen identifiera certifikatsökanden
- se till att datainnehållet i certifikaten är felfritt
- se till att certifikaten spärrs och att statusuppgifterna är riktiga samt att spärrlistorna för certifikat publiceras
- följa god dataskyddsnivå och god datahanteringssed vid hantering av certifikatinnehavarnas personuppgifter

2.3.2 Registrerare

Registreraren för ett medborgarcertifikat på identitetskort är polisen.

- Registreraren agerar på certifikatutfärdarens uppdrag och ansvar.
- Registreraren följer certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Registreraren identifierar certifikatsökanden enligt certifieringspraxisen.
- Kortunderlaget för medborgarcertifikatet på identitetskortet har skapats av polisen.
- Polisen som är registrerare levererar de uppgifter som anknyter till identifiering av personen och till ansökan av medborgarcertifikatet på identitetskort, enligt vilka medborgarcertifikatet skapas.

2.3.3 Tillverkare och specificerare av aktivkort

- Tillverkaren agerar på certifikatutfärdarens uppdrag och ansvar och enligt samarbetsavtalet vad gäller nyckelparen och aktiveringsuppgifterna.
- Tillverkaren följer certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Aktivkorten specificeras enligt de uppgifter som registreraren lämnat.

2.3.4 Spärrtjänst

Utfärdarens spärrtjänst spärrar certifikat på innehavarens eller utfärdarens önskemål innan certifikatets giltighetstid har löpt ut. De spärrade certifikaten införs i spärrlistan. Orsaken till spärrning av medborgarcertifikat på identitetskort kan vara till exempel att identitetskortet försvunnit.

2.3.5 Registertjänst

Registertjänsten är en offentlig webbtjänst som innehåller samtliga medborgarcertifikat beviljade av utfärdaren samt utfärdarens certifikat och spärrlistan. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

2.3.6 Innehavare av certifikat

Ett medborgarcertifikat enligt denna certifieringspraxis kan beviljas en finsk medborgare eller en utlänning som enligt lagen om hemkommun (201/1994) stadigvarande är bosatt i Finland och vars personuppgifter är registrerade i befolkningsdatasystemet

Certifikatinnehavaren ska följa certifikatutfärdarens certifikatpolicy och certifieringspraxis.

2.3.7 Part som litar på certifikatet

Part som litar på certifikatet är en person eller en organisation som litar på certifikatuppgifterna och som använder certifikatet för verifiering, kryptering av data och elektronisk signatur. Parten som litar på certifikatet ska se till att certifikatet är giltigt och att det inte finns på spärrlistan.

2.3.8 Användning av certifikatet

Ett medborgarcertifikat enligt denna certifieringspraxis kan användas för att verifiera en person, kryptera data och för elektronisk signatur. Medborgarcertifikatet kan användas i enlighet med användningssyftet utan begränsningar inom administration samt i applikationer och tjänster som erbjuds av en privat organisation.

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

2.4 Kontaktuppgifter

2.4.1 Organisation som administrerar certifieringspraxisen

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

Upphovsrätten enligt denna certifieringspraxis tillfaller Myndigheten för digitalisering och befolkningsdata.

2.4.2 Kontaktperson

På frågor som gäller certifieringspraxisen svarar och för kommunikation som gäller dessa dokument ansvarar Myndigheten för digitalisering och befolkningsdatas certifikattjänster.

Frågor som gäller denna certifieringspraxis skickas till följande adress:

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

3 Allmänna villkor

Denna certifieringspraxis träder i kraft 1.10.2021. Ändringsförfarandet för och publiceringen av certifieringspraxisen har beskrivits i punkt 8 i detta dokument.

3.1 Skyldigheter

3.1.1 Certifikatutfärdarens skyldigheter

- Myndigheten för digitalisering och befolkningsdata har ett lagstadgat uppdrag att fungera som certifikatutfärdare.
- Utfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt hantera eventuella krav på skadeersättning.
- Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer och personer som man anlitar, t.ex. registrerare och korttillverkare.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning för beviljande av medborgarcertifikat samt övriga aspekter av användningen av medborgarcertifikatet på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren uppfyller kraven enligt certifikatpolicyn och certifieringspraxisen.
- Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen och gör dem allmänt tillgängliga.

- Utfärdaren anställer tillräckligt med personal med den expertis, erfarenhet och kompetens som fordras för produktionen av certifikattjänster.
- Utfärdaren använder pålitliga system och produkter som är skyddade från otillbörlig användning.
- Utfärdaren tillhandahåller offentligt information om certifikat och certifikatverksamheten, utgående från vilken utfärdarens verksamhet och pålitlighet kan bedömas.
- Utfärdaren säkerställer att uppgifterna för skapande av signatur är tillförlitliga.
- Utfärdaren sparar eller kopierar inte uppgifter för skapande av signatur som lämnats till undertecknaren.

3.1.2 Registrerarens **skyldigheter**

- Registreraren efterlever certifikatpolicyn och certifieringspraxisen i samband med registreringen.
- Registreraren identifierar servercertifikatsökanden personligen på det sätt som beskrivs i certifieringspraxisen, på så sätt att sökandens identitet och övriga uppgifter om sökandens person som fordras för beviljande av certifikat noga kontrolleras.
- Registreraren ser till att personuppgifterna hanteras omsorgsfullt och konfidentiellt.
- Registreraren ger certifikatsökanden uppgifter om användarvillkoren för certifikatet.
- Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med utfärdaren.

3.1.3 Certifikatinnehavarens skyldigheter

- Användningsändamålet för certifikatet har fastställs i varje certifikats certifikatpolicy, certifieringspraxis och certifikatinnehavarens användningsvillkor. Certifikatet får endast användas enligt dess användningsändamål för elektronisk signatur, verifiering eller kryptering av data.
- Innehavaren av medborgarcertifikatet ansvarar för att de uppgifter som uppges då man ansöker om medborgarcertifikatet är riktiga.
- Certifikatinnehavaren ansvarar för användningen av identitetskortet och medborgarcertifikatet som ingår i detta, de rättshandlingar som denne gör med dessa och deras ekonomiska följder. Vad gäller signaturcertifikatet följs bestämmelserna i Förordningen.

- Innehavaren av medborgarcertifikatet förvarar de privata nycklar och de koder som behövs för att använda dessa separat samt strävar efter att förhindra att de privata nycklarna försvinner, hamnar i utomståendes händer, ändras eller används olovligt. Att lämna identitetskortet eller avslöja aktiveringskoden för en annan person, t.ex. genom att låna, frigör utfärdaren och parten som litar på medborgarcertifikatet från eventuellt ansvar som orsakas av användningen kortet.

- Medborgarcertifikatet hanteras och skyddas med samma noggrannhet som andra motsvarande kort eller dokument, såsom kreditkort, körkort och pass. Personliga aktiveringskoder ska förvaras fysiskt på ett annat ställe än identitetskortet.

- Om medborgarcertifikatet och identitetskortet försvinner eller om det finns möjlighet till missbruk, ska man omedelbart meddela Utfärdaren om detta genom att ringa den avgiftsfria spärrtjänsten +358 800 162 622. Det finns ett eget texttelefonnummer för döva och hörselskadade.

3.1.4 Den förlitande partens skyldigheter

Den förlitande parten är skyldig att säkerställa att certifikatet används enligt användningssyftet. Användningsändamålet för medborgarcertifikatet på identitetskort är elektronisk signatur. Användningsändamålet för verifierings- och krypteringscertifikatet är verifiering av person och kryptering av data.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan uppriktigt lita på medborgarcertifikatet då denne kontrollerat att **organisationscertifikatet är giltigt.** Den förlitande parten är skyldig att kontrollera certifikaten på spärrlistan. För att säkerställa att medborgarcertifikatets giltighet är tillförlitlig, ska den förlitande parten kontrollera nedannämnda kontrollåtgärder för spärrlistan.

Om den förlitande parten kopierar spärrlistan från registret, ska denne säkerställa spärrlistans autenticitet genom att kontrollera utfärdarens elektroniska signatur. Dessutom ska spärrlistans giltighetstid kontrolleras.

Om det på grund av störningar i systemet eller tjänsten inte går att få tillgång till en giltig spärrlista, får medborgarcertifikatet inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Om ett medborgarcertifikat godkänns efter denna giltighetstid, sker det på den förlitande partens eget ansvar.

3.1.5 Skyldigheter vid publicering av medborgarcertifikat

Medborgarcertifikaten identifikationscertifikat publiceras i det allmänt tillgängliga offentliga registret och de spärrade medborgarcertifikaten på spärrlistan och den förlitande parten ska kontrollera att listan är giltig.

3.2 Ansvar

3.2.1 Certifikatutfärdarens ansvar

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

Myndigheten för digitalisering och befolkningsdata svarar för att medborgarcertifikaten har skapats enligt de förfaranden som beskrivs i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009), lagen om stark autentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet och certifikatpolicyn samt certifieringspraxisen och utgående från de uppgifter som certifikatsökanden lämnat. Myndigheten för digitalisering och befolkningsdata ansvarar endast för den information som man sparat i medborgarcertifikatet.

Myndigheten för digitalisering och befolkningsdata svarar för att medborgarcertifikatet används sakligt, och att det är tillgängligt för för användning från att det överlåts under hela dess giltighetstid, förutsatt att certifikatet inte spärras. Medborgarcertifikat har överlåtits till en person som har identifierats på det sätt som förutsätts för medborgarcertifikatet. Certifikatinnehavaren har före undertecknandet av avtalet fått anvisningar för användning av medborgarcertifikatet.

Vid undertecknande av medborgarcertifikatet med sin privata nyckel intygar certifikatutfärdaren att utfärdaren har kontrollerat personuppgifterna i medborgarcertifikatet med de metoder som beskrivs i certifikatpolicyn och certifieringspraxisen.

Utfärdaren ansvarar för att medborgarcertifikat för rätt person förs in på spärrlistan och att det förs in på spärrlistan inom den tid som fastställs i denna certifieringspraxis.

3.2.2 Registrerarens ansvar

Registreraren för identitetskortet är polisen, som registrerar certifikatsökanden för på Myndigheten för digitalisering och befolkningsdata som är utfärdare. Om polisens åtgärder i samband med registreringen har föreskrivits närmare i lagen om identitetskort.

3.2.3 Medborgarcertifikatinnehavarens ansvar

Medborgarcertifikatet är sin innehavares elektroniska identitet och därför får det inte överlåtas till en annan person för användning.

Innehavaren av medborgarcertifikatet ansvarar för användningen av certifikatet, de rättshandlingar som denne gör med certifikatet och deras ekonomiska följder.

Om identitetskortet lämnas i kortläsaren, kan det finnas risk för missbruk av kortet. Efter att innehavaren av medborgarcertifikatet slutar använda enheten eller inte övervakar enheten ansvarar innehavaren för att avlägsna identitetskortet från kortläsaren och stänga de använda applikationerna på ett behörigt sätt.

Medborgarcertifikatinnehavarens ansvar för användningen av ett certifikat upphör när certifikatinnehavaren har anmält till spärrtjänsten de uppgifter som är nödvändiga för spärrningen av medborgarcertifikatet och efter att ha fått ett meddelande av den tjänsteman som mottagit samtalet om spärrningen. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

3.2.4 Den förlitande partens ansvar

Den förlitande parten kan inte uppriktigt lita på medborgarcertifikatet och den elektroniska signaturen, om denne inte kontrollerat medborgarcertifikatets giltighet på spärrlistan. Om medborgarcertifikatet trots detta godkänns frias Myndigheten för digitalisering och befolkningsdata från ansvar. Den förlitande parten ska kontrollera att det beviljade certifikatet motsvarar användningssyftet i den rättshandling det används för.

3.2.5 Begränsning av ansvar

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Myndigheten för digitalisering och befolkningsdata tillämpas utfärdarens skadeståndsansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och lagen om elektronisk kommunikation i myndigheternas verksamhet. I tillämpliga delar tillämpas också skadeståndslagen (412/1974).

Om ett elektroniskt identitetskort har föreskrivits i lagen om identitetskort (829/1999). Om kommunikationen i förvaltningen har föreskrivits i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Myndigheten för digitalisering och befolkningsdata svarar inte för eventuella skador som orsakas av att aktiveringsuppgifterna och medborgarcertifikatinnehavarens privata nycklar röjs, om inte röjningen direkt har orsakats av Befolkningregistercentralens omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdatas ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdata svarar inte för indirekta skador eller följdskador som har orsakats certifikatinnehavaren. Myndigheten för digitalisering och befolkningsdata svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter för kortinnehavaren.

Myndigheten för digitalisering och befolkningsdata är inte ansvarig för funktionen i de allmänna teleförbindelserna, t.ex. internet, eller för att en rättshandling inte kan utföras på grund av att certifikatinnehavarens utrustning eller program inte fungerar eller för att medborgarcertifikatet används i strid med sitt syfte.

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

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Medborgarcertifikatinnehavare eller förlitande parter ska i sådana fall svara för egna kostnader som följer av detta och utfärdaren är inte skyldig att ersätta medborgarcertifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

Vid fel i en nättjänst eller applikation som hänför sig till ett certifikat avsett för medborgare eller organisation svarar utfärdaren inte för användningen av certifikatet eller för de kostnader som detta orsakar.

Medborgarcertifikatinnehavarens ansvar för användningen av ett certifikat upphör när certifikatinnehavaren har anmält till spärrtjänsten de uppgifter som är nödvändiga för spärrningen av medborgarcertifikatet och efter att ha fått ett meddelande av den tjänsteman som mottagit samtalet om att medborgarcertifikatet har införts i spärrlistan. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

3.3 Ekonomiskt ansvar

3.3.1 Certifikatutfärdare

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Myndigheten för digitalisering och befolkningsdata tillämpas utfärdarens skadeståndsansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och lagen om elektronisk kommunikation i myndigheternas verksamhet. I tillämpliga delar tillämpas också skadeståndslagen (412/1974).

Myndigheten för digitalisering och befolkningsdatas ansvar gentemot förlitande parter omfattar högst direkta skador, om skadan beror på Myndigheten för digitalisering och befolkningsdatas åtgärder.

3.3.2 Andra parter

En part som litar på medborgarcertifikatet kan lita på riktigheten av medborgarcertifikatet och den elektroniska signaturen, om denne har kontrollerat att medborgarcertifikatet inte finns på spärrlistan och att certifikatets giltighetstid inte har upphört och denne inte har andra grundade orsaker att misstänka riktigheten av användningen av certifikatet.

Utfärdaren ansvarar för medborgarcertifikatet i enlighet med vad utfärdaren har förbundit sig till i denna certifieringspraxis och certifikatpolicy som gäller medborgarcertifikatet.

3.3.3 Utfärdarens ekonomiförvaltning

Myndigheten för digitalisering och befolkningsdatas 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.

3.4 Tolkning och verkställighet

3.4.1 Lagstiftning som tillämpas

Ett signaturcertifikat som beviljats enligt denna certifieringspraxis uppfyller de krav som ställts för ett signaturcertifikat i 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.

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som gjorts med signaturcertifikat. Om identitetskortet har föreskrivits i lagen om identitetskort (829/1999) och om certifikat beviljade av Myndigheten för digitalisering och befolkningsdata har föreskrivits i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (611/2009).

Vid produktion av certifikattjänster fastställs Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar enligt bestämmelserna i skadeståndslagen (412/1974). På Myndigheten för digitalisering och befolkningsdata tillämpas också lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet kan man alltid uträtta ärenden med signaturcertifikatet i myndighetsförvaltningen.

Myndigheten för digitalisering och befolkningsdata följer principer för god informationshantering enligt personuppgiftslagen (523/1999) och god informationshantering enligt lagen om offentlighet i myndigheternas verksamhet (621/1999). I Myndigheten för digitalisering och befolkningsdata säkerställs dataskyddet bland annat genom kontinuerlig utbildning. Myndigheten för digitalisering och befolkningsdata har också berett uppförandekoder för både informationstjänster och certifikattjänster.

Myndigheten för digitalisering och befolkningsdata skaffar de uppgifter som krävs för registrering och identifiering av person från Polisen. I denna verksamhet följer Myndigheten för digitalisering och befolkningsdata bestämmelserna i lagen om samservice inom den offentliga förvaltningen (2007/223).

Om Myndigheten för digitalisering och befolkningsdatas ställning föreskrivs i lagen (166/1996) och förordningen om registerförvaltningen (248/1996). Signaturutfärdare övervakas i Finland av Traficom.

Myndigheten för digitalisering och befolkningsdata svarar för att medborgarcertifikaten på identitetskort har skapats enligt de förfaranden som beskrivs i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009), lagen om elektroniska signaturer, lagen om elektronisk kommunikation i myndigheternas verksamhet och certifikatpolicyn och utgående från de uppgifter som identitetskortsökanden lämnat.

Myndigheten för digitalisering och befolkningsdatas certifikattjänster övervakas av Traficom som är ett tillsynsorgan enligt lagen om stark autentisering och betrodda elektroniska tjänster och som ger bestämmelser och rekommendationer om signaturcertifikatverksamheten. Därför deltar Myndigheten för digitalisering och befolkningsdata inte i frivilliga ackrediteringssystem. Myndigheten för digitalisering och befolkningsdatas certifikatverksamhet övervakas av Traficom och i fråga om personuppgifter följer Myndigheten för digitalisering och befolkningsdata personuppgiftslagen. Myndigheten för digitalisering och befolkningsdata samarbetar också kontinuerligt med Dataombudsmannen i fråga om hanteringen av personuppgifter.

Vid lösningen av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning. Vid produktionen av signaturcertifikat ska man särskilt beakta lagen om stark autentisering och betrodda elektroniska tjänster.

3.4.2 Avgörande av meningsskiljaktigheter

Vid beviljandet av medborgarcertifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att certifikaten uppfyller de krav som ställs i denna certifieringspraxis och i certifikatpolicyn som gäller medborgarcertifikat.

Eventuella tvister löses enligt rättssystemet i Finland. Vid lösningen av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning. Vid produktionen av signaturcertifikat ska man särskilt beakta lagen om stark autentisering och betrodda elektroniska tjänster.

3.5 Avgifter

I detta kapitel fastställs de avgifter som hänför sig till användningen av medborgarcertifikat på identitetskort.

3.5.1 Beviljande och förnyelse av medborgarcertifikat

Medborgarcertifikat på identitetskort ansökas hos polisen. Ett medborgarcertifikat på identitetskort beviljas alltid utgående från en ny ansökan genom att följa den identifieringsmetod som fastställs i lagen om identitetskort. Priset på identitetskortet fastställs enligt finansministeriets vid var tid gällande förordning om avgifterna för Myndigheten för digitalisering och befolkningsdatas prestationer.

3.5.2 Avgifter som hänför sig till användningen av medborgarcertifikat

Utfärdaren debiterar inte innehavaren av medborgarcertifikat separat för användningen av medborgarcertifikatet, spärrtjänsten eller det offentliga registret. Enskilda nättjänstleverantörer kan debitera för användningen av sina egna tjänster. Användningen av medborgarcertifikat förutsätter inget separat meddelande eller tillstånd av utfärdaren.

3.5.3 Avgifter som hänför sig till markering av medborgarcertifikat på spärrlistan

Det är avgiftsfritt att anmäla att ett medborgarcertifikat ska införas på spärrlistan. Även avhämtning av spärrlistor från registret och kontroll av medborgarcertifikatets giltighet är avgiftsfritt.

3.5.4 Övriga avgifter

En separat avgift för användning av rådgivningstjänsten tas ut enligt giltig prislista.

Om tjänsteleverantören vill ordna en informationsförsörjningstjänst mellan en kod som specificerar medborgarcertifikat och koduppgifter i sitt eget bakgrundssystem eller andra uppdateringsuppgifter, kan tjänsteleverantören ansöka om tillstånd till överlåtelse av uppgifter i informationstjänsten hos Myndigheten för digitalisering och befolkningsdata. Denna tjänst prissätts enligt den giltiga lagen om grunderna för avgifter till staten och finansministeriets förordning om avgifterna för Myndigheten för digitalisering och befolkningsdatas prestationer.

3.6 Publicering och tillgänglighet av uppgifter

3.6.1 Publicering av utfärdarens uppgifter

Utfärdaren publicerar medborgarcertifikats identifikationscertifikat och spärrlistor i ett offentligt register som kan användas utan avgift. Utfärdaren publicerar certifikatpolicy, certifieringspraxis, certifikatbeskrivning (PDS) samt övriga offentliga handlingar med anknytning till produktionen av certifikattjänster på sin webbplats.

3.6.2 Publiceringsfrekvens

Medborgarcertifikatet identifikationscertifikat publiceras i det offentliga registret genast då det skapats och finns i registret under hela dess giltighetstid. Utfärdaren publicerar en spärrlista som är giltig åtta timmar efter publikationen. Denna spärrlista uppdateras en gång per timme med en ny spärrlista.

3.6.3 Uppgifternas tillgänglighet

Offentiliga uppgifterna i registret och spärrlistan är offentligt tillgängliga. Offentliga FI-NEID-bestämmelser som publicerats av utfärdaren finns på utfärdarens webbplats. Certifikatpolicyn och certifieringspraxisen finns även tillgängliga på certifikatutfärdarens webbplats.

3.6.4 Dataförvaring

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats. De konfidentiella uppgifterna i certifikatsystemet är sparade i utfärdarens egna, konfidentiella dataförråd. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Man fäster särskild uppmärksamhet vid hanteringen av personuppgifter och Myndigheten för digitalisering och befolkningsdata har publicerat särskilda regler för produktionen av certifikattjänster i enlighet med personuppgiftslagen. Utfärdaren har även berett en registerbeskrivning för hanteringen av personuppgifter inom varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen.

3.7 Dataskyddsinspektion

Traficom som övervakar signaturutfärdare kan inspektera utfärdarens verksamhet under de förutsättningar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster.

3.7.1 Frekvens av inspektioner

Myndigheten för digitalisering och befolkningsdata utför en dataskyddsgranskning för de tekniska leverantörernas lokaler, utrustning och verksamhet på ett ändamålsenligt sätt. Inspektionen görs minst en gång om året och alltid när en ny avtalsperiod börjar. Vid inspektionsförfarandet följer Myndigheten för digitalisering och befolkningsdata de förfaranden som fastställs i dataskyddsstandarden ISO/IEC 27001.

Med hjälp av inspektionen utreder man om den tekniska leverantörens verksamhet motsvarar avtalet med hänsyn till kraven i dataskyddsstandarderna. I regel bedöms en teknisk leverantör enligt standarden ISO/IEC 27001 och Traficoms bestämmelser.

3.7.2 Inspektör

Myndigheten för digitalisering och befolkningsdatas dataskyddsinspektion görs av Myndigheten för digitalisering och befolkningsdatas dataskyddschef eller en utomstående inspektör som är specialiserad på auditering av tekniska leverantörer av certifikattjänster.

3.7.3 Målen för och omfattningen av inspektionen

Målen för granskningen fastställs i lagen om stark autentisering och betrodda elektroniska tjänster eller om Myndigheten för digitalisering och befolkningsdata utför granskningen i enlighet med dataskyddsstandarden ISO/IEC 27001 i enlighet med Myndigheten för digitalisering och befolkningsdatas dataskyddspolitik eller tekniska leveransavtal.

Inspektionen görs genom att beakta genomförandet av dataskyddets åtta delområden. Dataskyddsegenskaper som inspekteras är bl.a. konfidentialitet, integritet och användbarhet.

Inspektionen omfattar Traficoms bestämmelser om datasäkerhet vid utfärdarens verskamhet.

I inspektionen jämförs policyn, certifieringspraxisen och tillämpningsanvisningar med hela certifikatorganisationens och -systemets verksamhet. Myndigheten för digitalisering och befolkningsdata kontrollerar att tillämpningsanvisningarna är enhetliga med certifikatpolicyn.

Vid inspektionerna beaktas förutom administrativ datasäkerhet också olika tjänsteleverantörer bland annat enligt följande indelning:

Spärrtjänst:

- Datakommunikationssäkerhet
- Personalsäkerhet
- Fysisk säkerhet

Certifikatproduktion:

- arbetsfördelning och varje persons uppgifter – personalsäkerhet
- fysisk säkerhet
- Säkerhet i anknytning till utfärdarens nycklar
- Produktionssystemet för certifikat och reservsystemet
- datakommunikationssäkerhet

Kortproduktion:

- produktionslinjen som helhet i hela dess sträckning
- kvalitetskontroll vid kortproduktion
- datakommunikationssäkerhet
- personalsäkerhet
- fysisk säkerhet

Registertjänst:

- använda komponenter
- administrationsförbindelser
- uppdatering av register och registrets funktion i felsituationer
- personalsäkerhet
- datakommunikationssäkerhet
- fysisk säkerhet

HelpDesk-verksamhet:

- datakommunikationssäkerhet
- personalens yrkeskompetens och utbildning
- förfarandeprocess i olika hjälpfunktioner

3.7.4 Åtgärder vid avvikelser

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

3.7.5 Information om resultatet av inspektionen

Man informerar om resultatet av inspektionen i enlighet med lagen, dataskyddsstandarden ISO/IEC 27001, Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och gällande leveransavtal. Det detaljerade och standardiserade inspektionsresultatet avsett för intern användning är konfidentiellt och offentliggörs inte. Rapporter med på förhand bestämd utformning utarbetas separat för användning utanför organisationen.

Myndigheten för digitalisering och befolkningsdata informerar Traficom om inspektionens resultat enligt lagen om stark autentisering och betrodda elektroniska tjänster samt Traficoms bestämmelser och rekommendationer.

3.8 Publicering av uppgifter

3.8.1 Uppgifter som publiceras av utfärdaren

Uppgifterna i certifikatsystemet är konfidentiella, om de inte grundar sig på bestämmelser om överlåtelse av uppgifter enligt personuppgiftslagen, lagen om elektronisk kommunikation i myndigheternas verksamhet och lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) eller lagen om stark autentisering och betrodda elektroniska tjänster eller de ändamål som fastställs i utfärdarens certifikatpolicy eller certifieringspraxis.

3.8.2 Offentliga uppgifter

Uppgifterna i det offentliga registret och spärrlistan är offentliga, likaså de uppgifter som fastställs i certifieringspraxisen och certifikatpolicyn, samt de publicerade FI-NEID-specificeringarna.

3.8.3 Uppgifter som anknyter till upphörande eller avbrott av medborgarcertifikatets giltighet

Medborgarcertifikatets giltighet har antecknats i medborgarcertifikatet. Certifikat som spärrats under giltighetstiden publiceras på spärrlistan som är allmänt tillgänglig.

3.8.4 Uppgifter som lämnas ut till myndigheter

Uppgifter som lämnas ut till myndigheter fastställs enligt gällande lagstiftning.

3.8.5 Övriga uppgifter

Uppgifter i certifikatsystemet överlåts endast för de ändamål som nämns ovan i detta kapitel.

3.8.6 Överlåtelse av uppgifter på certifikatinnehavarens begäran

Certifikatinnehavaren har rätt att få uppgifter som gäller honom eller henne, till exempel personuppgifter, enligt gällande lagstiftning.

3.8.7 Övriga principer för överlåtelse av uppgifter

För utfärdarens pålitlighet är det viktigt att Myndigheten för digitalisering och befolkningsdata på alla sätt sörjer för sekretessen av sådant konfidentiellt material som den får tillgång till i samband med certifikatverksamheten och för god informationshantering, om inte myndighetens rätt att få information om certifikatsystemet ger anledning till annat.

I hanteringen av personuppgifter följer Myndigheten för digitalisering och befolkningsdata personuppgiftslagen samt speciallagstiftningen. Myndigheten för digitalisering och befolkningsdata har berett uppförandekoder för överlåtelse av uppgifter samt hantering av personuppgifter i samband med certifikatverksamheten. Särskild noggrannhet iakttas i hanteringen av personuppgifter.

3.9 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.

4 Identifiering av certifikatsökande

4.1 Registrering

I kapitlen 4.1–4.3 framställs den praxis och de verksamhetsprocesser som följs vid identifiering och verifiering av certifikatsökande.

Rättigheterna och skyldigheterna för certifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden. Ansökningsdokumentet innehåller information om varje parts rättigheter och skyldigheter.

I ansökningsdokumentet och användarvillkoren nämns tydligt att sökanden av medborgarcertifikat intygar riktigheten hos uppgifterna med sin signatur samt godkänner att medborgarcertifikatet skapas och kan publiceras i det offentliga registret. Samtidigt godkänner sökanden reglerna och villkoren för användning av medborgarcertifikatet samt sörjer för förvaringen av medborgarcertifikatet och aktiveringskoderna samt för att anmäla om eventuellt missbruk eller försvunnet kort.

Utfärdaren och registreraren, korttillverkaren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheter för samtliga parter.

Sökanden av medborgarcertifikat svarar för att samtliga uppgifter som är väsentliga för medborgarcertifikatet och som sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren av medborgarcertifikatet ska endast använda sitt medborgarcertifikat i enlighet med dess användningssyfte.

Då Utfärdaren beviljar medborgarcertifikatet, godkänner utfärdaren samtidigt certifikatansökan.

Sökanden av medborgarcertifikatet kan, om han eller hon vill, spara sin e-postadress både i certifikatet och befolkningsdatasystemet. E-postadressen antecknas både i certifikatet och befolkningsdatasystemet i den form som sökanden uppgett. E-postadressen som antecknats i medborgarcertifikatet sparas i det offentliga registret såsom också det övriga datainnehållet i medborgarcertifikatet. E-postadressen kan inte ändras under medborgarcertifikatets giltighetstid.

För innehavaren av medborgarcertifikatet klargörs att han eller hon har möjlighet att byta de ursprungliga aktiveringskoderna till nya koder. Användningen av medborgarcertifikatet i elektroniska webbtjänster förutsätter att man skaffar ett nödvändigt kortläsarprogram. På Myndigheten för digitalisering och befolkningsdatas webbplats https://dvv.fi/sv/ kan certifikatinnehavaren ladda ner det kortläsarprogram som han eller hon behöver för att använda certifikatet. Med hjälp av programmet är det också möjligt att byta PIN-koderna på identitetskortet.

Innehavaren av medborgarcertifikatet ansvarar för att förhindra att de privata nycklar som denne har och aktiveringskoderna används i strid mot användningsvillkoren genom att sörja för kortet och koderna på det sätt som nämns i användningsvillkoren.

Certifikatinnehavaren ska omedelbart anmäla medborgarcertifikatet till spärrlistan om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

4.1.1 Namngivningspraxis

Myndigheten för digitalisering och befolkningsdatas rotutfärdare är:

CN = DVV Gov. Root CA – G3 RSA

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

och

CN = DVV Gov. Root CA – G3 ECC

OU = Varmennepalvelut

OU = Certification Authority Services

O = Digi- ja vaestotietovirasto CA

C = FI

Utfärdaren för Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat är:

CN (Common name) = DVV Citizen Certificates - G4R

OU (Organizational unit) = Valtion kansalaisvarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

och

Digi- ja väestötietoviraston kansalaisvarmenteiden varmentaja on:

CN (Common name) = DVV Citizen Certificates - G4E

OU (Organizational unit) = Valtion kansalaisvarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Certifikatinnehavarens namngivningspraxis för medborgarcertifikat:

2.5.4.5 (Serial Number) = Elektronisk kontaktkod (SATU)

SN (Surname) = Efternamn

G (Given name) = Förnamn

CN (Common name) = Efternamn Förnamn SATU

C (Country) = FI

E (EmailAddress) = e-postadress (valfri)

Utfärdarens publika nyckel placeras i utfärdarens certifikat, det offentliga registret och på medborgarcertifikatinnehavarens aktivkort. För identitetskortet som innehåller medborgarcertifikatet har för visuell identifiering av personen specificerats kortinnehavarens foto och underskriftsprov. Uppgifterna i medborgarcertifikatet fastställer innehavaren av medborgarcertifikatet entydigt. Utfärdaren utreder vid behov certifikatsökandens officiella identitet.

4.1.2 Leverans av privata nycklar till innehavaren av medborgarcertifikat

De privata nycklar som skapats i kortets tekniska del i medborgarcertifikatet levereras till sökanden av medborgarcertifikatet i samband med överlåtelsen av koret. Av

privata signaturnycklar som skapats i den tekniska delen finns inte kopior och sådana kan inte heller senare tillverkas.

Identitetskortet som innehåller medborgarcertifikatet överlåts till sökanden av medborgarcertifikatet i enlighet med det förfarande som överenskommits med registreraren som representerar utfärdaren.

Användning av identitetskort vid elektronisk kommunikation förutsätter aktivering med hjälp av en aktiveringskod. Med hjälp av aktiveringskoden kan användaren aktivera sitt identitetskort. När identitetskortet används för första gången vid elektronisk kommunikation till exempel via hemdatorn, startar kortläsarprogrammet automatiskt aktiveringsprocessen för identitetskortet. Under denna process ombeds användare först ange aktiveringskoden, varefter användaren kan aktivera och ställa in sin egen, personliga PIN-kod. Efter aktiveringsprocessen kan användaren använda sitt identitetskort vid elektronisk kommunikation.

Det finns två aktiverade koder. En baskod med vilken användaren kontrollerar identitetskortets underhåll och elektronisk identifiering. En signaturkod med vilken användaren kan göra en elektronisk signatur.

Om användaren anger fel kod fem gånger, låses kortet och funktioner som skyddats med PIN-koden kan inte längre användas. Låsning av baskoden hindrar användning av alla applikationer som skyddas med koden. Låsning av signaturkoden hindrar användning av elektronisk signatur. Låsta koder låses upp med aktiveringskoden.

4.2 Förnyelse av nyckelpar

Publika nycklar i medborgarcertifikatet och privata nycklar på chips kan inte förnyas. För att skapa nya nyckelpar krävs ett nytt medborgarcertifikat.

Vid förnyelse av medborgarcertifikat iakttas samma rutiner som vid första ansökan om certifikat.

4.3 Förnyelse av nyckelpar efter införande av certifikat på spärrlista

Publika nycklar i medborgarcertifikatet och privata nycklar på chips kan inte förnyas. För att skapa nya nyckelpar krävs ett nytt medborgarcertifikat.

Vid förnyelse av medborgarcertifikat iakttas samma rutiner som vid första ansökan om certifikat.

4.4 Identifiering av den person som gjort begäran om spärrning

Innehavaren av medborgarcertifikatet kan begära att certifikatet spärras innan dess giltighetstid löpt ut.

4.5 Förfarande vid begäran om spärrning

Begäran om spärrning görs i första hand av certifikatinnehavaren när denne märker att certifikatet har försvunnit eller om missbruk av certifikatet har varit möjligt. Begäran om spärrning kan dock göras av till exempel korttillverkaren eller registreraren.

Begäran om spärrning ska göras omedelbart när det finns anledning att misstänka missbruk av medborgarcertifikatet på grund av att det har försvunnit eller stulits. Medborgarcertifikat kan spärras genom att ringa det avgiftsfria allmänna spärrtjänstnumret 800 162 622.

Varje begäran om spärrning, grunderna för spärrning, identifieringssättet för den person som gjort begäran om spärrning och de åtgärder som utfärdaren gjort till följd av begäran arkiveras. Samtal om begäran om spärrning inspelas.

4.6 Identifiering av den person som gjort begäran om spärrning av medborgarcertifikat

Identifiering av den person som gjort begäran om spärrning sker genom att kontrollera uppringarens personuppgifter. Om uppringaren är någon annan som innehavaren av det medborgarcertifikat som ska spärras, identifieras förutom uppringaren också innehavaren av medborgarcertifikatet.

Utifrån medborgarcertifikatinnehavarens identifieringsuppgifter får man reda på certifikatets specificerande uppgift som möjliggör begäran om spärrning.

Om begäran om spärrning görs av registreraren eller korttillverkaren, identifieras personen som gjort begäran på det sätt som beskrivs i kapitel 4.4.3.

5 Funktionella krav

5.1 Ansökan om medborgarcertifikat

Rättigheterna och skyldigheterna för sökanden av medborgarcertifikat ingår i ansökningsdokumentet och i de allmänna användningsanvisningarna som ges innan ansökan om medborgarcertifikat undertecknas. Tillsammans med dessa bildar dessa ett avtal som ingås med sökanden av medborgarcertifikatet. Ansökningsdokumentet innehåller information om varje parts rättigheter och skyldigheter. När sökanden av medborgarcertifikatet söker certifikat, godkänner denne samtidigt de allmänna användningsvillkoren.

I ansökningsdokumentet och användningsanvisningarna nämns tydligt att sökanden av medborgarcertifikat intygar riktigheten hos uppgifterna med sin signatur samt godkänner att certifikatet skapas och kan publiceras i det offentliga registret. Samtidigt godkänner sökanden reglerna och villkoren för användning av medborgarcertifikatet samt sörjer för förvaringen av medborgarcertifikatet och aktiveringskoderna samt för att anmäla om eventuellt missbruk eller försvunnet certifikat/identitetskort.

Utfärdaren och registreraren, korttillverkaren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheter för båda parterna.

Man ansöker om ett medborgarcertifikat genom att personligen besöka ett den polismyndighet som är registrerar eller ett annat registreringsställe. Vid ansökan om medborgarcertifikat kontrolleras identiteten mot ett giltigt dokument som utfärdats av polisen och som styrker personens identitet, till exempel ett ID-kort och pass.

Godtagbara identifieringshandlingar är ett giltigt pass eller identitetskort som beviljats av myndighet i en medlemsstat inom EES och ett giltigt pass som beviljats av myndighet i något annat land. Om sökanden inte har ovannämnda dokument, identifierar polisen sökandens identitet på något annat sätt. Uppgiften om identifieringssättet antecknas på ansökningsblanketten och tjänstemannen vid registreringsstället bekräftar med sin underskrift att en verifiering av identiteten har ägt rum.

Uppgifter som personen uppgett jämförs med uppgifterna i Befolkningsdatasystemet.

5.2 Beviljande av medborgarcertifikat

Utfärdaren beviljar medborgarcertifikatet då utfärdaren godkänner certifikatansökan.

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

5.3 Mottagning av medborgarcertifikat

Medborgarcertifikat kan avhämtas personligen vid registreringsstället.

Vid tidpunkten för överlåtelse av medborgarcertifikatet betonar man för sökanden att det inte är möjligt att skapa kopior av privata nycklar och att sådana inte heller senare kan tillverkas.

Innehavaren av medborgarcertifikatet kan ladda ner ett kortläsarprogram på Myndigheten för digitalisering och befolkningsdatas webbplats med vilket medborgarcertifikatet kan användas i elektronisk kommunikation.

5.4 Medborgarcertifikatets giltighetstid och spärrning av certifikatet

5.4.1 Förutsättningar för spärrning av medborgarcertifikatet

Medborgarcertifikatet ska införas på spärrlista när det finns anledning att misstänka missbruk av certifikatet på grund av att det har försvunnit eller stulits. Medborgarcertifikat kan spärras genom att ringa det avgiftsfria allmänna spärrtjänstnumret. Begäran om spärrning av ett certifikat ska göras omedelbart när misstanke om möjligheten till missbruk har uppstått.

Innehavaren av medborgarcertifikatet ansvarar för att förhindra att de privata nycklar som denne har och aktiveringskoderna används i strid mot användningsvillkoren genom att sörja för sitt kort och sina koder på det sätt som nämns i användningsvillkoren.

5.4.2 Person som gör begäran om spärrning

Begäran om spärrning av medborgarcertifikatet görs vanligen av innehavaren av certifikatet. Om uppringaren är någon annan som innehavaren av det certifikat som ska spärras, identifieras förutom innehavaren också uppringaren.

Begäran om spärrning kan också göras av utfärdaren, korttillverkaren eller registreraren. Den metod som använts för att identifiera den person som gjort begäran om spärrning registreras.

Grunderna och tidpunkten för spärrningen och uppgifterna om den som gjort spärrningen sparas.

5.4.3 Spärrning

Ett medborgarcertifikat kan spärras på följande sätt:

a) Genom att ringa spärrtjänsten

b) Genom att besöka registreraren

Uppgiften om införandet av medborgarcertifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärrning har konstaterats vara behörig och godkänd. Spärrlistan är giltig i åtta timmar.

5.4.4 Annullering av identitetskort

Polisen kan annullera identitetskortet alltid när kortinnehavaren begär det. Ett identitetskort som beviljats en minderårig annulleras också om vårdnadshavaren återkallar sitt samtycke. Ett identitetskort kan också annulleras om det är försvunnet, stulet, skadat eller dess markeringar har ändrats eller om kortet används olagligt av någon annan än den person för vilken identitetskortet har beviljats. Ett identitetskort kan också annulleras om uppgifter avsedda för medborgarcertifikatet har ändrats. Polisen gör en anmälan om spärrning av medborgarcertifikat på identitetskort som den har annullerat under identitetskortets giltighetstid och efter att giltighetstiden har upphört när identitetskortet är försvunnet eller stulet. Om innehavaren av identitetskortet vill göra en anmälan om spärrning av medborgarcertifikatet innan annulleringen, ska denne själv anmäla om spärrningen till spärrtjänsten.

5.4.5 Andra sätt att förhindra användningen av medborgarkortet

Kortinnehavaren ansvarar för spärrningen av medborgarcertifikatet. Ett medborgarcertifikat kan på kortinnehavarens anmälan införas på spärrlistan och då kan certifikatet som beviljats av Myndigheten för digitalisering och befolkningsdata inte längre användas. Däremot kan andra applikationer som eventuellt finns på kortets tekniska underlag användas enligt deras användningsändamål. Att förhindra användningen av medborgarcertifikat påverkar inte godtagbarheten av identitetskortet som identitetskort och hos finsk medborgare som resedokument.

Medborgarcertifikatet spärras genom ett telefonsamtal till det avgiftsfria spärrtjänstnumret. Medborgarcertifikatinnehavarens ansvar upphör, när en specificerande uppgift som möjliggör spärrningen har mottagits. Samtidigt upphör medborgarcertifikatinnehavarens ansvar för användningen av medborgarcertifikatet. Vid behov kan anmälan också göras av en annan person. Då ska anmälarens identitet och kontakt med innehavaren av det identitetskort som upphävs säkerställas.

Spärrtjänsten informerar den som gjort begäran om spärrning av medborgarcertifikat om att begäran om spärrning har lyckats under samma samtal.

Om personen som gjort begäran om spärrning av ett medborgarcertifikat som överlåtits till medborgarcertifikatinnehavaren är annan än medborgarcertifikatinnehavaren och begäran om spärrning inte beror på medborgarcertifikatinnehavarens kontakt

med utfärdaren eller registreraren, underrättas medborgarcertifikatinnehavaren om spärrningen av medborgarcertifikatet också per brev.

Ett spärrat certifikat kan inte tas i bruk igen.

5.4.6 Att förhindra användningen av medborgarcertifikat som identitetskort och hos finsk medborgare som resedokument

Kortinnehavaren kan göra en anmälan om försvunnet eller stulet identitetskort hos polisen. Polisen gör en anteckning om anmälan i polisens identitetskortregister och då godkänns kortet inte längre som identitetskort eller resedokument. I samband med anmälan om försvunnet och stulet kort medborgarcertifikatet anmäler polisen medborgarcertifikatet som ingår i kortets tekniska del på spärrlistan. Efter att kortinnehavaren har meddelat att identitetskortet har hittats, gör polisen en anteckning om detta i identitetskortregistret. Efter detta godkänns identitetskortet igen som identitetskort eller hos finsk medborgare som resedokument.

I samband med att det nya identitetskortet överlämnas klipper polistjänstemannen bort det högra nedre hörnet vid fotografiet på identitetskortet som upphört att gälla. Innehavaren av identitetskortet kan dock använda ett kort som gjorts ogiltigt på detta sätt för hantering av krypterade dokument och filer och utnyttja de applikationer och uppgifter som denne sparat på kortet.

5.4.7 Spärrning av medborgarcertifikat på uppdrag av Myndigheten för digitalisering och befolkningsdata

Myndigheten för digitalisering och befolkningsdata spärrar medborgarcertifikatet alltid när uppgiften om medborgarcertifikatinnehavarens död har kommit till Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata gör en anmälan om detta till rättsinnehavarna till den döda innehavaren av medborgarcertifikatet. Myndigheten för digitalisering och befolkningsdata kan spärra medborgarcertifikat som undertecknats med dess privata nyckel, om det finns anledning att misstänka att Myndigheten för digitalisering och befolkningsdatas privata nycklar har röjts eller hamnat i fel händer.

Myndigheten för digitalisering och befolkningsdata spärrar de medborgarcertifikat som den beviljat om ett fel upptäcks i medborgarcertifikatens datainnehåll.

Samtliga gällande medborgarcertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade medborgarcertifikatets giltighetstid har löpt ut.

Om den privata nyckeln eller annan teknisk metod som använts vid skapandet av Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat har röjts eller på annat vis blivit oanvändbar ska Myndigheten för digitalisering och befolkningsdata meddela det inträffade till samtliga kortinnehavare och Traficom på ändamålsenligt sätt.

Myndigheten för digitalisering och befolkningsdata kan spärra ett medborgarcertifikat av ett särskilt skäl.

5.4.8 Tidpunkten för spärrning

Medborgarcertifikatet spärras omedelbart i samband med begäran om spärrning.

5.4.9 Krav på avbrott av certifikatets giltighet

Giltigheten av medborgar certifikat kan inte avbrytas tillfälligt. Ett spärrat medborgarcertifikat kan inte tas i bruk igen.

5.4.10 Person som gör begäran om avbrott

Giltigheten av medborgar certifikat kan inte avbrytas tillfälligt.

5.4.11 Begäran om avbrott

Giltigheten av medborgar certifikat kan inte avbrytas tillfälligt.

5.4.12 Begränsningar av avbrottstid

Giltigheten av medborgar certifikat kan inte avbrytas tillfälligt.

5.4.13 Publiceringsfrekvens för spärrlista

Uppgiften om införandet av medborgarcertifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärrning har konstaterats vara behörig och godkänd. Spärrlistan är giltig i åtta timmar.

Spärrlistan innehåller tidpunkten för publicering av nästa spärrlista.

Ny spärrlista publiceras senast vid tidpunkten för upphörande av den gällande spärrlistans giltighet.

Vid systemuppdateringar och motsvarande undantagssituationer kan MDB publicera spärrlistor med olika publiceringsfrekvenser och längre giltighetstider.

5.4.14 Krav på kontroll av spärrlista

Den förlitande partens skyldigheter har beskrivits i kapitel 2.1.4.

5.4.15 Kontroll av certifikatets status online

Utfärdaren erbjuder en onlinekontrolltjänst för certifikatets status dvs. OCSP-tjänst. Utfärdaren publicerar till och med en spärrlista över spärrade certifikat.

5.4.16 Krav på kontroll av certifikatets status online

Utfärdaren erbjuder en onlinekontrolltjänst dvs. OCSP för certifikatets status.

5.4.17 Särskilda krav gällande avslöjande av certifikatinnehavarens privata nyckel

Certifikatinnehavaren ansvarar för att skydda användningen av sina privata nycklar genom att sörja för sitt chips eller kort och sina koder på det sätt som nämns i användningsvillkoren. Certifikatinnehavaren ska omedelbart anmäla certifikaten till

spärrlistan om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

5.5 Övervakning av systemet

För övervakning av systemet sparar utfärdaren logguppgifter om händelser i certifikatproduktionen, hanteringen av användningsrättigheter för certifikatsystemet, konfigurationen, beställningsprogram och applikationer med ändringar, säkringar samt återställning av dessa. Utfärdaren övervakar också dokument som gäller verksamheten. Om upptäckta avvikelser rapporteras på överenskommet sätt.

5.6 Arkivering av uppgifter om medborgarcertifikat

5.6.1 Material som sparas

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 medborgarcertifikat tillämpas för en del dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i 10 år från tidpunkten då medborgarcertifikaten upphört att gälla. Utfärdaren arkiverar följande uppgifter:

a) Certifikatsökandens undertecknade ansökningsblankett, verifikat för mottagande av identitetskortet och de allmänna användarvillkoren för certifikatet.

b) Uppgifterna på identitetskortet som beviljats av polisen samlas in i identitetskortregistret som polisen upprätthåller och ansvarar för.

c) Beviljade medborgarcertifikat, deras datainnehåll och extra uppgifter med anknytning till hanteringen av deras livscykel från att medborgarcertifikatets giltighetstid har löpt ut eller certifikatet har spärrats.

d) Åtgärder med anknytning till skapande och förnyande av utfärdarens privata nyckel

e) Begäran om spärrning av medborgarcertifikat

f) Spärrlistor sparade i det offentliga registret och övrig information om spärrningen av medborgarcertifikat

g) Gällande certifikatpolicy och tidigare certifikatpolicyn och motsvarande certifieringspraxis

h) Åtgärder utförda av användare som registrerats som administratörer för certifikatsystemet och användare av certifikatsystemet sparas loggfiler

i) Granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet

Det arkiverade materialet förvaras enligt bestämmelserna för myndigheter som fungerar som utfärdare.

5.6.2 Skydd av arkiv

Polisen förvarar handlingar med anknytning till ansökning om identitetskort, autentisering av personer och överlåtelse av kort som arkiveras i ändamålsenliga lokaler.

Materialet som arkiveras förvaras i lokaler med hög skyddsnivå och passagekontroll.

5.6.3 Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

5.6.4 Metoder för införskaffning och tryggande av arkiverat material

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

Utfärdaren ser till att arkiven är tillgängliga och läsbara även utifall att utfärdarens verksamhet avbryts eller upphör.

Uppgifter kan överlåtas ur arkivet i den mån detta är motiverat med tanke på certifikatinnehavaren eller den förlitande parten.

5.7 Hantering av kontinuerlig verksamhet och undantagsfall

Myndigheten för digitalisering och befolkningsdata har en kontinuitets- och beredskapsplan för att verksamheten ska kunna bedrivas ostört utan avbrott.

5.7.1 Utfärdarens privata nyckel har röjts eller Utfärdarens certifikat har spärrats

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

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

a) Utfärdaren 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) Utfärdaren skapar en ny nyckel i enlighet med punkt 6.

c) Samtliga gällande medborgarcertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade medborgarcertifikatets giltighetstid har löpt ut.

d) Utfärdaren arkiverar uppgifter enligt 38 § i lagen om stark autentisering och betrodda elektroniska tjänster för den tid lagen kräver samt följer också annars bestämmelserna i arkivlagen i fråga om arkivering av uppgifter.

5.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas säkerhetspolicy beaktas åtgärder som förorsakas av problem med den externa säkerheten. Myndigheten för digitalisering och befolkningsdata har fått ISO 27001-dataskyddscertifikatet som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även utifall en eventuell katastrof. I samband med beviljande och underhåll av medborgarcertifikat följer Myndigheten för digitalisering och befolkningsdata de förfaranden som fastställts för datasäkerhet.

5.8 Då utfärdarens verksamhet upphör

Utfärdarens verksamhet anses upphöra då samtliga tjänster med anknytning till utfärdarens beviljande av certifikat upphör permanent. Utfärdarens verksamhet anses inte upphöra om certifieringstjänsten överförs från en organisation till en annan.

Utfärdaren meddelar de parter som nämns i punkt a) i punkt 4.8 om att certifikattjänsterna upphör så snart som möjligt, dock minst en månad innan tidpunkten för detta.

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

a) Samtliga gällande certifikat spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.

b) Utfärdaren upphäver samtliga avtalspartners befogenheter för att utföra åtgärder med anknytning till processen för beviljande av certifikat för utfärdarens del.

c) Utfärdaren ser till att tillgången till utfärdarens arkiv enligt kapitel 4.6 bevaras även efter att utfärdarens verksamhet har upphört.

d) Utfärdaren ansvarar för att uppgifterna enligt 38 § i lagen om stark autentisering och betrodda elektroniska tjänster arkiveras samt följer också annars bestämmelserna i arkivlagen i fråga om arkivering av uppgifter.

6 Krav på fysisk, funktionell och personalsäkerhet

Myndigheten för digitalisering och befolkningsdata har beviljats dataskyddscertifikat som säkerställer att MDB:s dataskydd uppfyller kraven i standarden ISO/IEC 27001.

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. MDB svarar i egenskap av certifikatutfärdare för säkerheten inom certifikatproduktionen och själva produktionen på ett ändamålsenligt sätt inom samtliga delområden.

Myndigheten för digitalisering och befolkningsdata följer god informationshantering. Tjänster som anknyter till tillhandahållande av certifikat har organiserats till Myndigheten för digitalisering och befolkningsdatas certifikattjänster.

6.1 Arrangemang kring fysisk säkerhet

Myndigheten för digitalisering och befolkningsdata har beviljats dataskyddscertifikat som säkerställer att MDB:s dataskydd uppfyller kraven i standarden ISO/IEC 27001. Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. MDB svarar i egenskap av certifikatutfärdare för säkerheten inom certifikatproduktionen och själva produktionen på ett ändamålsenligt sätt inom samtliga delområden.

6.1.1 Läge och lokalernas egenskaper

Utfärdarens system finns i maskinsalar med hög säkerhetsnivå och uppfyller anvisningarna och bestämmelserna för säkerheten i maskinsalar.

Säkerheten i verksamhetslokalerna är förverkligad på så vis att obehöriga inte har tillträde till lokalerna genom att låsa lokalerna tillräckligt effektivt, använda lokaler som är stadiga och tillräckligt hållbara. Onödiga fönster i maskinlokalerna har undvikits och hållbara byggmaterial har valts för konstruktionerna.

6.1.2 Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässig uppgifter inom certifikatsystemet 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.

6.1.3 Elmatning och luftkonditionering

Maskinsalarna är behörigt luftkonditionerade. I lokalerna har man berett sig på okontrollerade elavbrott med reservkraftlösningar som byggts i fastigheterna.

6.1.4 Brandsäkerhet

Maskinsalarna har nödvändiga larmmekanismer i fall av brand, nödvändig första släckningsutrustning samt automatiska släckningssystem.

6.1.5 Förvaring av uppgifterna

De uppgifter som ska arkiveras och säkerhetskopiorna förvaras i olika lokaler än utfärdarens utrustning.

Uppgifterna har skyddats mot försvinnande, ändring och olovlig användning.

6.1.6 Hantering av onödigt informationsmaterial

Säkerhetsklassificerat informationsmaterial kasseras på ett pålitligt sätt genom att förstöra.

6.1.7 Vattenskador

Maskinsalarna har behöriga detektorer för fuktighet.

6.1.8 Reservarrangemang

Utrustningslösningarna är förverkligade i enlighet med god dataadministrationssed på så vis att man vid problem med systemet kan övergå till att använda reservsystemet utan att riskera konfidentialiteten, integriteten och användbarheten hos uppgifterna i systemet.

Tillgången till reservdelar och service för viktig utrustning är säkrad.

6.2 Funktionella krav

6.2.1 Ansvarsfördelning

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för registrering och datatekniska uppdrag inom produktionen av certifikat. Myndigheten för digitalisering och befolkningsdata fungerar som certifikatutfärdare och svarar för certifikatverksamheten.

Utfärdarens uppgifter delas in i följande ansvarsområden:

Datasäkerhetsansvarig

Registreringsansvarig

Administratör för systemet

Användare av systemet

Övervakare av systemet

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

6.2.2 Antal personer som behövs för uppgifterna

Skapande, aktivering, säkerhetskopiering och returnering av ufärdarens privata nyckel är åtgärder som utförs med två personer som fungerar som administratörer för systemet närvarande. Likaså är annullering av utfärdarens privata nyckel endast möjligt med två berättiga personer närvarande. Vid formateringen av den kryptografiska modulen för utfärdarens privata nyckel närvarar minst två personer som fungerar som administratörer för systemet.

Användning av systemet fordrar närvaron av en person som innehar rättigheterna för uppgiften.

Registrering och autentisering av medborgarcertifikat på identitetskort fordrar närvaron av en person. Uppdraget utförs av polisen.

6.2.3 Uppgiftsspecifik autentisering

För Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat på identitetskort

Registreraren är polisen enligt det s.k. samserviceavtalet.

Administratör av certifikatsystemet

Autentiseras med ett personligt kontrollkort för administration av systemet. Administratörer för systemet är certifikatsystemleverantörens systemexperter samt personer som befullmäktigats för uppdraget av Myndigheten för digitalisering och befolkningsdata.

Användare av certifikatsystemet

Autentiseras med ett personligt identitetskort för användning av systemet. Användare av certifikatsystemet är maskinsalsverksamheten, initiativtagare till tekniska certifikatbegäranden och spärrtjänsten.

6.3 Personlig säkerhet

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

Av personalen vid Myndigheten för digitalisering och befolkningsdatas certifikattjänst förutsätts en utbildningsnivå som motsvarar arbetsuppgifterna samt kännedom om certifikatverksamheten. Experter följer kontinuerligt utvecklingen av branschen i Finland och Europa och arbetar med expertuppgifter inom branschen.

I samband med konkurrensutsättningen har utfärdaren bedömt kompetensen hos de tekniska leverantörernas nyckelexperter och anställda gällande genomförandet av certifikattjänsten. De datatekniska leverantörerna upprätthåller kompetensen hos personalen inom serviceproduktion i fråga om utrustning, program, metoder och datasäkerhet. Dessutom ansvarar de tekniska leverantörerna för att personalen känner till datahanteringsuppgifterna vid certifikattjänsten på det sätt som tjänsten förutsätter.

6.3.1 Utförande av bakgrundskontroll av personalen

Myndigheten för digitalisering och befolkningsdata utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar i de tekniska leverantörernas certifikatmiljö. Säkerhetskontrollen utförs av skyddspolisen. Myndigheten för digitalisering och befolkningsdata förbehåller sig rätten att inte godkänna en anställd hos en teknisk leverantör för en uppgift där man arbetar med certifikatsystemet.

6.3.2 Förfarande vid utförande av bakgrundskontroll

Personalens arbetserfarenhet kartläggs vid rekryteringen och personen fyller i en blankett som lämnas in till skyddspolisen. Blanketten används för att utföra en mindre säkerhetsutredning för personen.

Samtliga personer som arbetar med centrala uppgifter hos utfärdaren, producenterna av certifikattjänster, registertjänster och spärrlistan samt korttillverkarna ska:

- fylla i en blankett som lämnas in till skyddspolisen, som används för att utföra en mindre säkerhetsutredning 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.

6.3.3 Krav på utbildning

Personalen på Myndigheten för digitalisering och befolkningsdata 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.

6.3.4 Underhåll av expertis och kompetens

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

6.3.5 Krav på uppgiftsrotation

Då utfärdaren planerar arbetsrotation inom sin verksamhet ska uppgifterna organiseras på så vis att den anställda kan utföra sina nya uppgifter på bästa möjliga sätt. Vid planeringen av personalrotationen beaktas bland annat de krav som datasäkerheten ställer, säkerställandet av konfidentialiteten och principerna för god hantering av personuppgifter, som har beskrivits i Myndigheten för digitalisering och befolkningsdatas uppförandekoder för hantering av personuppgifter.

Även inom arbetsrotationen efterlevs Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och dataskyddsplan samt Myndigheten för digitalisering och befolkningsdatas övriga allmänna anvisningar.

6.3.6 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).

6.3.7 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 certifikattjänster.

6.3.8 Handlingar som tillhandahålls personalen

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

7 Tekniska säkerhetsarrangemang

7.1 Skapande och sparande av nyckelpar

7.1.1 Skapande av nyckelpar

Skapandet av nyckeln grundar sig på inmatat slumptal som är tillräckligt långt och som har skapats så att det är omöjligt att kalkylmässigt spåra det, även om man skulle veta när och med hurdan utrustning det har skapats. Den algoritm som används för att generera slumptalet och genereringsmetoden uppfyller kvalitetskraven som är bl.a. algoritmens tillförlitlighet, genereringsmetodens icke-upprepbarhet och slumptalets äkta slumpmässighet. Utfärdaren publicerar inte den noggrannhet och metod som används för sannolikhet.

Certifikatutfärdare:

Utfärdaren skapar privata nycklar för signering och publika nycklar som motsvarar de privata nycklarna för signering. Nycklarna förvaras i kryptografiska moduler som administreras av utfärdaren. De överensstämmer till sin säkerhetsnivå med nivå 3 i FIPS 140-1.

Innehavare av certifikat:

Nycklarna kan skapas som satsvis körning före certifieringen eller direkt i samband med certifieringen. I båda fall sparas den privata nyckeln på identitetskortet som läs- och skrivskyddad.

Utfärdaren skapar certifikatinnehavarens nycklar med chipset på identitetskortet. Av privata nycklar skapas inga kopior.

7.1.2 Överlåtelse av en privat nyckel till certifikatsökanden

Ett identitetskort som innehåller medborgarcertifikatinnehavarens privata nycklar och för vilken ursprungliga aktiveringskoder krävs som aktiveringsuppgift, levereras till kunden så att det inte är i samma ställe med identitetskortet förrän de överlåts till sökanden. Detta genomförs med hjälp av olika överföringsrutter och genom att överlåta kortet och koderna vid olika tidpunkter.

Identitetskortet som innehåller medborgarcertifikatet överlåts till certifikatsökanden i enlighet med det förfarande som överenskommits med registreraren som representerar utfärdaren.

7.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren

De publika nycklarnas integritet skyddas ända fram till certifieringen. Efter att nycklarna har skapats gör korttillverkaren certifikatbegäran till certifikatsystemet.

Certifikatbegäran innehåller uppgifterna om den publika nyckeln och andra uppgifter om certifikatet. Teleförbindelsen mellan systemet för certifikatbegäran och systemet för skapande av begäran krypteras och de personer som startar systemet för certifikatbegäran identifieras med administrationskort som beviljats av utfärdaren.

7.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren

Utfärdarens publika nyckel är en del av utfärdarens certifikat som placeras på identitetskortet. Utfärdarens certifikat får fritt spridas och är tillgängligt också i det offentliga registret och utfärdarens www-tjänst.

7.1.5 Nycklarnas längder

Utfärdarens privata nyckel som används för att signera medborgarcertifikatet samt den motsvarande publika nyckeln är RSA-nycklar med storleken 4096 bitar och 384 bitar ECC-nycklar.

Certifikatinnehavarens privata och publika nycklar är RSA-nycklar med minst 2048 bitar och 384 bitar ECC-nycklar.

7.1.6 Nycklarnas användningsändamål:

Fältet som fastställer användningssyftet i certifikatets datainnehåll anger användningssyftet för nyckeln kopplad till certifikaten (till exempel verifikation och kryptering av information eller elektronisk signatur). Användningen av nyckeln begränsas endast till sitt användningsändamål. En nyckel som avsetts för elektronisk signatur ska alltså endast användas för detta ändamål och inte till exempel för verifikation och kryptering av information.

Certifikatutfärdarens certifikat:

Ändamål: Underskrift av certifikat och spärrlistor. Den tekniska beskrivningen finns i FINEID S2-bestämmelserna.

Certifikatinnehavarens verifikations- och krypteringscertifikat:

Ändamål: Verifikation av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signaturcertifikat:

Ändamål: Elektronisk signatur

7.2 Skydd av privat nyckel

7.2.1 Standarder som gäller den kryptografiska modulen

Certifikatutfärdarens privata nycklar förvaras i kryptografiska moduler som administreras av utfärdaren, som överensstämmer med nödvändiga säkerhetsstandarder

Utfärdaren ser till att utfärdarens privata nycklar inte kan röjas eller missbrukas. Säkerhetskopior tas på certifikatutfärdarens privata nycklar på det sätt som fordras för den kritiska datasäkerheten.

7.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel

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

7.2.3 Överlåtelse av en privat nyckel till förlitande part

Utfärdarens privata nycklar kan inte överföras eller kopieras.

7.2.4 Säkerhetskopia av en privat nyckel

Utfärdarens privata nycklar och deras säkerhetskopior förvaras med stark kryptering i utrustning som uppfyller kraven på kritisk datasäkerhet.

7.2.5 Arkivering av en privat nyckel

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

7.2.6 Administration av en privat nyckel i kryptografiska moduler

Utfärdarens privata signaturnycklar skyddas med fysiska och logiska säkerhetsåtgärder med hög tillförlitlighet. Dessa används endast i ett system som placerats i en säker miljö. Användningen av nycklar övervakas med hjälp av särskilda administrationskort som skyddats mot osaklig användning.

Personer som utför utfärdarens betrodda arbetsuppgifter har ett administrationskort som är skyddat med aktiveringskod. Personens rätt att använda certifikatsystemet eller andra system som anknyter till certifiering verifieras med hjälp av dessa administrationskort.

När användningen av utfärdarens nyckel avslutas, kasseras nyckeln så att den inte längre kan användas eller skapas på nytt. Samtidigt kasseras nyckelns säkerhetskopior. Förfaranden för kassering av trasiga anordningar har ordnats så att privata nycklar som sparats både enhets- och programbaserat kan förstöras på ett pålitligt sätt (med tillräckligt många överskrivningar).

7.3 Andra faktorer som anknyter till nyckeladministration

7.3.1 Arkivering av en publik nyckel

Utfärdaren arkiverar alla publika nycklar som den certifierat.

7.3.2 Användningstid för publika och privata nycklar

Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat är giltigt i fem år. Certifikatet kan spärras under dess giltighetstid. Signaturcertifikatet kan användas för att verifiera riktigheten av signaturen efter att certifikatet föråldrats eller spärrats,

om den certifierade signaturen har skapats innan certifikatet spärrades eller föråldrades.

7.4 Aktiveringsuppgift

7.4.1 Skapande och ibruktagande av aktiveringsuppgift

Korttillverkaren skapar aktiveringsuppgifterna som möjliggör användningen av nycklarna. De individuella aktiveringskoderna beräknas och överförs till kortet och som krypterad till responsfilen för överföring till korttillverkarens produktionssystem. Efter leverans av korten överförs de krypterade aktiveringskoderna från korttillverkning till en separat avdelning där aktiveringskoderna skrivs ut. Efter överenskommen tid levereras de till den utdelningsadress som sökanden har angett i sin kortansökan.

7.4.2 Skydd av aktiveringsuppgift

Aktiveringskoderna har skyddats så att de inte kan läsas eller kopieras från kortet. Certifikatinnehavaren ansvarar för att skydda användningen av sina nycklar på identitetskortet genom att sörja för sitt kort och sina koder på det sätt som nämns i användningsvillkoren.

7.4.3 Andra faktorer som anknyter till aktiveringsuppgiften

För innehavaren av medborgarcertifikatet klargörs att denne har möjlighet att byta de ursprungliga PIN-koderna till nya koder. Utbytesprogrammet för aktiveringskoderna kan avgiftsfritt användas av kortinnehavaren på adressen https://dvv.fi/sv/.

PIN-koden låser sig och användningen av certifikat på identitetskortet förhindras om fel kod ges fem gånger i rad. Den låsta aktiveringskoden låses upp i samband med personligt besök vid polisstationens serviceställe för tillstånd. I detta samband kontrolleras sökandens identitet.

Aktiveringskoden levereras till den adress sökanden har uppgett inom en vecka från beställningen. Certifikatinnehavaren öppnar det låsta kortet själv med hjälp av kortläsarprogrammet. Programmet med tilläggsuppgifter finns tillgängligt på adressen https://dvv.fi/sv/.

7.5 Säkerhetskrav som gäller användning av datorer och tillgång till dessa

7.5.1 Utrustningssäkerhet

Som utrustning för säkerhetssystemet används endast utrustning som lämpar sig för detta ändamål.

Utrustningssäkerheten är förverkligad i enlighet med god dataadministrationssed på så vis att man vid problem med systemet kan övergå till att använda reservsystemet utan att riskera konfidentialiteten av systemet. Tillgången till reservdelar till utrustning som är viktig för verksamhetens kontinuitet är säkrad.

Vid serviceförfarande är utomstående personals tillgång till system och lokaler som serviceproduktionen ansvarar för förhindrad. Servicebesök är endast möjligt för en

teknisk leverantör som ingått ett tekniskt leveransavtal och sekretessavtal. Lista över godkända tekniska leverantörer upprätthålls.

Servicebesök är endast möjliga under övervakning av systemets administratör eller en person som denne befullmäktigat.

Certifikatsystemets utrustning övervakas dygnet runt.

7.6 Livscykeladministration av certifikatsystemet

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

7.6.1 Övervakning som gäller systemutvecklingen

Utvecklingen och testningen av systemet sker i en separat testmiljö. Endast testade, fungerade och godkända lösningar överförs till produktionssystemet.

7.6.2 Hantering av säkerhet

Myndigheten för digitalisering och befolkningsdatas datasäkerhet admiistreras i enlighet med Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och standarden ISO 27001.

7.7 Datanätets säkerhet

Datakommunikationssäkerheten har förverkligats så att certifikatsystemets datanät är en enhetlig helhet som separerats från andra datanät på ett behörigt sätt och vars kritiska delar har fördubblats. Meddelanden som förmedlas i nätet och dess avsändare eller mottagare avslöjas inte för obehöriga parter utan särskilda åtgärder. Nätet används endast i uppgifter som anknyter till certifikatsystemet. Onödiga nättjänster har inaktiverats. Nätet har delats i logiska delar och förbindelserna mellan dessa är begränsade. Tillräckliga verifikations-, tillgångskontroll- och oavvislighetsförfaranden används.

7.8 Övervakning av användning av kryptografisk modul

Utfärdaren ser till att utfärdarens privata nycklar inte kan röjas eller missbrukas. Säkerhetskopior tas på certifikatutfärdarens privata nycklar på det sätt som fordras för den kritiska datasäkerheten.

För användning av en kryptografisk modul krävs alltid ett aktivkort för identifiering av personen och verifikation av användningsrättigheterna. Modulen kan endast aktiveras med systemanvändarens personliga administrationskod.

För att skapa en ny användningsrättighet på användarnivå krävs närvaro av två personer med administratörsstatus och motsvarande personliga administrationskort. Modulen samlar in logguppgifter om händelser.

8 Profiler för certifikat och spärrlistor

8.1 Tekniska uppgifter om certifikat

Datainnehållen i rotcertifikatet, utfärdarens certifikat och certifikatinnehavarens certifikat har beskrivits i dokument FINEID S2. Dokumentet finns tillgängligt på utfärdarens webbplats https://dvv.fi/sv/.

8.2 Profil för spärrlistor

Datainnehållen i spärrlistor som utfärdaren publicerats har beskrivits i dokument FINEID S2. Dokumentet finns tillgängligt på utfärdarens webbplats https://dvv.fi/sv/.

9 Hantering av dokument innehållande bestämmelser

9.1 Ändring av bestämmelser

Utfärdaren kan ändra bestämmelserna utgående från juridiska eller verksamhetsmässiga krav. Ändringar i bestämmelserna ska föras in i certifikatpolicy- och certifieringspraxishandlingarna på det sätt som beskrivs här näst.

9.2 Publicering och information

Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen, som är tillgängliga på adressen https://dvv.fi/sv/certifikatpolicydokument.

Offentliga bestämmelser relaterade till utfärdarens produktion av certifikat är tillgängliga på samma webbplatser.

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

9.3 Förfarande för ändring och godkännande av certifieringspraxis

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för medborgarcertifikatet. Handlingarna kan ändras med Myndigheten för digitalisering och befolkningsdatas interna ändringsförfarande.

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

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.

[Tarkenne] [Numero]
[Liite]

[Yksikkö] / Aarnio Ville 6.5.2021