MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIKATPOLICY FÖR TILLFÄLLIGA CERTIFIKAT

OID: 1.2.246.517.1.10.304
OID: 1.2.246.517.1.10.354

1.6.2021

CERTIFIED SFS ORGANIZATION ISO 9001

SERTIFIOITU inspecta ORGANISAATIO ISO/IEC 27001

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

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Version 1.0	1.6.2021/VA

Innehållsförteckning

CERTIFIKATPOLICY FÖR TILLFÄLLIGA CERTIFIKAT
Definitioner och förkortningar

Definitioner

Aktiveringsuppgift: Konfidentiell uppgift (PIN-kod) som behövs för att aktivera de hemliga nycklarna på ett chip och att använda dem i metoder med öppen nyckel.

Nyckelpar: Nycklar som används tillsammans inom ett system med nycklar, varav den ena är öppen och den andra hemlig. Ändamålet med nycklarna har fastställts på certifikatet (se certifikatinnehavarens autentiserings- och krypteringscertifikat).

Asymmetrisk kryptering: Vid asymmetrisk kryptering används ett nyckelpar med en öppen och en hemlig nyckel. Ett meddelande som krypterats med öppen nyckel kan endast öppnas med den hemliga nyckeln i nyckelparet i fråga.

Öppen nyckel: Den öppna delen av nyckelparet som används för asymmetrisk kryptering enligt metoden med öppen nyckel. Certifikatutfärdaren bekräftar med sin elektroniska signatur att den öppna nyckeln hör till certifikatinnehavaren. Den öppna nyckeln är en del av certifikatets datainnehåll.

System med öppen nyckel: Dataskyddsinfrastruktur där dataskyddstjänster produceras med ett system med öppen nyckel.

Metod med öppen nyckel: Informationssäkerhetstjänst, exempelvis elektronisk identifiering av personer, som produceras med hjälp av öppna och hemliga nycklar, certifikat och asymmetrisk kryptering.

Kortläsarprogram: Kortläsarprogram används på arbetsstationen som s.k. slutanvändarprogram. Med hjälp av programmet kan användaren dra fördel av sitt kort och de certifikat som finns lagrade på det i olika användarmiljöer och tillämpningar, till exempel vid elektronisk kommunikation, för säker e-post och vid inloggning på arbetsstationen.

Förlitande part: Den part som litar på uppgifterna i certifikatet och använder certifikatet för olika informationssäkerhetstjänster, såsom elektronisk identifiering av certifikatets innehavare.

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

Chip: Teknisk plattform som certifikatet och de hemliga nycklarna lagras på. Ett chip kan finnas på ett aktivkort, identitetskort, ett betalkort eller ett SIM-kort för en mobilterminal.

Mobilterminal: Mobiltelefon eller annan mobilenhet som ett chip med certifikat och hemliga nycklar kan användas med.

OCSP: Online Certificate Status Protocol, standard för verifiering av certifikatstatus i realtid över internet

Organisationscertifikat: Ett kvalificerat certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för en fysisk person. Datainnehållet i certifikatet fastställs i lagen om stark autentisering och betrodda elektroniska tjänster.

PIN-kod: Aktiveringsuppgift som används för att aktivera en hemlig nyckel på ett chip. PIN 1: baskod för autentisering och kryptering.

PUK-kod: Kod som behövs för att öppna en låst PIN-kod.

Registrerare: En registrerare ska för certifikatutfärdarens räkning och på dennes ansvar kontrollera identiteten hos den som ansöker om certifikat i enlighet med certifikatpolicyn och certifikatpraxisen.

RSA-algoritm och RSA-nyckel: RSA-algoritmen är en allmänt använd öppen nyckelalgoritm. Hemliga och öppna nycklar i anslutning till tillfälliga certifikat 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: Teknisk leverantör som för certifikatutfärdarens räkning tar emot och förmedlar begäranden om spärrning av certifikat till certifikatsystemet.

Yrkesutbildad person inom hälso- och sjukvården: En person som med stöd av lagen om yrkesutbildade personer inom hälso- och sjukvården har erhållit rätt att utöva yrke (legitimerad yrkesutbildad person) eller tillstånd att utöva yrke (yrkesutbildad person som beviljats tillstånd) eller en person som med stöd av nämnda lag har rätt att använda i förordning av statsrådet avsedd yrkesbeteckning för en yrkesutbildad person inom hälso- och sjukvården (yrkesutbildad person med skyddad yrkesbeteckning) och som registrerat sig i centralregistret över yrkesutbildade personer inom hälso- och sjukvården.

Yrkeskort för social- och hälsovården (yrkeskort) MDB: ett aktivkort som innehåller ett yrkescertifikat som utfärdats för en yrkesutbildad person inom social- och hälsovården.

Personal inom hälso- och sjukvården: personal hos tjänsteleverantörer inom social- och hälsovården såsom avses i lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994) som inte hör till kategorin yrkesutbildade personer inom hälso- och sjukvården. Till denna personalgrupp hör till exempel stöd-, kansli- och informationstjänstpersonal vid en verksamhetsenhet inom hälso- och sjukvården En person som arbetar hos en tjänsteleverantör inom hälso- och sjukvården men som inte är en yrkesutbildad person.

Personalkort för social- och hälsovården (personalkort): Ett aktivkort som innehåller ett certifikat som MDB utfärdat för en person som hör till den övriga personalen inom hälsovården (inte en yrkesutbildad person).

Studerande inom hälso- och sjukvården: På villkor som ges i statsrådets förordning kan en studerande som studerar till ett visst yrke tillfälligt vara verksam i någon legitimerad yrkesutbildad persons uppgifter under ledning och tillsyn av en sådan

legitimerad yrkesutbildad person. På studeranden tillämpas då lämpliga delar av det som föreskrivs om yrkesutbildade personer inom hälso- och sjukvården. Studerande inom medicin, odontologi och farmaci får yrkeskorten för hälso- och sjukvården. En studerande som studerar för något annat yrke inom hälso- och sjukvården och som uppfyller villkoren får ett organisationsbestämt personalkort för hälso- och sjukvården.

Aktörer inom social- och hälsovården: Person som arbetar för en tjänsteleverantör inom social- och hälsovården men som inte är en yrkesutbildad person inom social och hälsovården eller hör till den övriga personalen inom social- och hälsovården. I gruppen i fråga ingår övriga personer och specialgrupper som använder riksomfattande datasystem, såsom informationssäkerhetsansvariga samt datasystemleverantörer, konsulter osv.

Aktörskort för social- och hälsovården (aktörskort): Ett aktivkort som innehåller ett certifikat som MDB utfärdat för en annan aktör inom social- och hälsovården.

Tillfälligt certifikat: Certifikat som Myndigheten för digitalisering och befolkningsdata utfärdat för en fysisk person och som kan användas för autentisering och kryptering eller för autentisering och kryptering samt elektroniska signaturer.

Reservkort: Reservkort till en organisations aktivkort. Ett tillfälligt certifikat för kortinnehavaren har lagrats på reservkortets tekniska del (chipet). Av särskilda skäl kan ett reservkort även utfärdas för en person som inte har något aktivkort som är knutet till en organisation.

Certifikat: Ett intyg i elektronisk form som kan användas för identifiering av en person och kryptering av data, och som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar undertecknarens identitet. Certifikatet innehåller en medföljande unik kod enligt certifieringspraxis.

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

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

Certifikatpolicy: Ett dokument där man beskriver principerna för utfärdande 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 förs av en certifikatregister som tillhandahåller certifikat för allmänheten. Uppgifterna förvaras i minst fem år efter att certifikatets giltighetstid har gått ut.

Datasystem för certifiering: 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: Certifikatutfärdande organisation som svarar för produktionen av certifikat samt utarbetar certifikatpolicy och certifieringspraxis som beskriver organisationens verksamhet.

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

Certifikatutfärdarens hemliga nyckel: En hemlig nyckel som används för signering av utfärdarens certifikat och spärrlistor.

Certifikatsökande: Person som ansöker om tillfälligt certifikat och som identifieras på ett tillförlitligt sätt i samband med ansökan.

Certifikatinnehavare: En person vars identitet och öppna nyckel har bekräftats med certifikatutfärdarens elektroniska signatur och som innehar de hemliga nycklar som certifikatet hänför sig till.

Certifikatinnehavarens autentiserings- och krypteringscertifikat: Ett certifikat som används för elektronisk identifiering av personer och för kryptering av data. Certifikatinnehavaren använder sin hemliga autentiserings- och krypteringsnyckel för elektronisk identifiering och för dekryptering av krypterade data eller meddelanden. För användningen av nyckeln behövs en baskod (PIN 1).

Certifikatanvändning och användningsområde: I detta dokument avses med användning av certifikat såväl användning av själva certifikatet som användning av medföljande nycklar.

Hemlig nyckel: Den hemliga delen av nyckelparet som används för asymmetrisk kryptering i metoden med öppen nyckel. Certifikatinnehavarens hemliga nycklar har lagrats på ett chip där de skyddas mot obehörig användning.

Förkortningar

CA	Certification Authority, certifikatutfärdare
CP	Certificate Policy, certifikatpolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, säkerhetsmodul
HST	Elektronisk identifiering av person

HTTP	Hypertext Transfer Protocol
ISO 27001	ISO IEC 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, standard för verifiering av certifikatstatus i realtid över internet
OID	Object Identifier, objektidentifierare
PDS	PKI Disclosure Statement, certifikatbeskrivning
PIN	Personal Identification Number, PIN-kod
PKI	Public Key Infrastructure, system med öppen nyckel
PUK	PIN Unblocking Key, PUK-kod
RSA	Rivest, Shamir, Adleman, en algoritm för öppen nyckel, asymmetrisk algoritm
MDB	Myndigheten för digitalisering och befolkningsdata

1 Inledning

En certifikatpolicy är en beskrivning av förfaranden och verksamhetsprinciper som ska iakttas när certifikat utfärdas. Certifieringspraxis är en mer detaljerad beskrivning av utfärdarens verksamhet.

Denna certifikatpolicy tillämpas på Myndigheten för digitalisering och befolkningsdatas tillfälliga certifikat. Certifikatuppgifterna förmedlas till den förlitande parten via ett offentligt register med certifikatsökandens samtycke eller på annat sätt enligt avtal med kundorganisationen.

Ett tillfälligt certifikat stöder användningen av Myndigheten för digitalisering och befolkningsdatas organisationscertifikat, OID: 1.2.246.517.1.10.303 och 1.2.246.517.1.10.353

1.1 Allmänt

Ett certifikat är ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar certifikatinnehavarens identitet. Certifikatets uppgifter har signeras digitalt med certifikatutfärdarens hemliga nyckel. Ett certifikat som är förenligt med denna certifikatpolicy grundar sig på systemet och metoderna med öppen nyckel. Om datainnehållet i ett certifikat som är förenligt med denna certifikatpolicy föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster.

Ett tillfälligt certifikat är ett autentiserings- och krypteringscertifikat eller ett autentiserings- och krypteringscertifikat och ett signeringscertifikat. Myndigheten för digitalisering och befolkningsdata garanterar identitetens riktighet.

Ett tillfälligt certifikat som är förenligt med denna policy kan utfärdas för organisationskunder. Om en organisationskund registrerar tillfälliga certifikat för personalen inom social- och hälsovården eller för aktörer inom social- och hälsovården ska alla parter som avses i denna certifikatpolicy förutom certifikatpolicyn även iaktta kraven i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna.

Myndigheten för digitalisering och befolkningsdata, som är certifikatutfärdare, specificerar innehavaren av certifikatet med hjälp av en elektronisk kommunikationskod, som även är en del av certifikatets datainnehåll. Koden är en teknisk identifieringskod som inte innehåller identifierande uppgifter om personen. Ett tillfälligt certifikat kan lagras på olika aktivkort.

Myndigheten för digitalisering och befolkningsdatas certifikatpolicy och certifieringspraxis har bägge en egen objektidentifierare (OID).

I egenskap av certifikatutfärdare har MDB till uppgift att producera certifikat-, register- och spärrtjänster, sköta registrering samt tillverka och individualisera aktivkort som innehåller certifikat. Dessa funktioner beskrivs närmare i kapitel 1.3.

Myndigheten för digitalisering och befolkningsdata utarbetar en separat certifikatpolicy för varje certifikattyp som utfärdas liksom en certifieringspraxis för varje tekniskt underlag. Certifikatpolicyn beskriver separat för varje certifikattyp vilka förfaranden

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

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen) tillämpas på signeringscertifikat inom betrodda tjänster från och med 1.7.2016. I detta dokument fastställs kraven på verksamheten och förvaltningspraxisen hos dem som utfärdar autentiserings- och signeringscertifikat enligt Förordningen. I kraven på förfaringssätt i detta dokument beskrivs användningen av anordningar för signaturframställning.

Certifikatutfärdaren är en tillhandahållare av certifikattjänster som avses i Förordningen.

Enligt lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) är Myndigheten för digitalisering och befolkningsdata leverantör av identifieringsverktyg vidtillhandahållandet av certifikatbaserade identifieringsverktyg för allmänheten. I Finland utövar Traficom tillsyn över tillhandahållarna av identifieringstjänster.

Sedan 1.12.2010 har Myndigheten för digitalisering och befolkningsdata varit lagstadgad certifikatutfärdare för hälso- och sjukvården och sedan 1.4.2015 för socialvården till följd av de ändringar som gjordes i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) samt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019)) Myndigheten för digitalisering och befolkningsdatas enhet Certifikattjänster ansvarar för ämbetsverkets certifikatverksamhet.

1.2 Identifikationsuppgifter

Denna certifikatpolicy heter Certifikatpolicy för Myndigheten för digitalisering och befolkningsdatas tillfälliga certifikat, OID 1.2.246.517.1.10.304 och 1.2.246.517.1.10.354.

Certifikatpolicyn hänvisar till rotcertifikatutfärdarens certifikatpolicy, OID 1.2.246.517.1.10.301 och 1.2.246.517.1.10.351.

När det gäller signeringscertifikat som tillhandahålls allmänheten iakttar Myndigheten för digitalisering och befolkningsdata en certifikatpolicy förenlig med betrodda tjänster i Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], punkten QSCD; OID: 0.4.0.194112.1.2. Signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar kvalificerade certifikat och anordningar för framställning av elektroniska signaturer som beskrivits i artikel 28 och 29 i Förordningen.

Graden av tillförlitlighet på autentiseringscertifikatet är "hög" enligt Förordningen och i förordningen om tillitsnivåer som utfärdats med stöd av Förordningen.

Såväl certifikatpolicyn som certifieringspraxisen finns på www.fineid.fi.

1.3 Certifikatutfärdaren och tillämpningsområden för certifikat

Certifikatutfärdaren tillhandahåller certifikattjänster på villkor som föreskrivs i denna policy och ansvarar för att de fungerar för certifikatinnehavarna enligt certifikatutfärdarens ansvar som beskrivs i kapitel 2.2.1. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifikatpolicy har registrerats av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister; enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019), lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) har Myndigheten för digitalisering och befolkningsdata bland annat till uppgift att tillhandahålla tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdatas certifikattjänst indelas i följande funktioner.

1.3.1 Certifikatutfärdare

Certifikatutfärdarens uppgifter är att

- tillhandahålla certifikat- och registertjänster och spärrtjänster i enlighet med certifikatpolicyn och certifieringspraxisen
- identifiera certifikatsökande personligen
- se till att datainnehållet i certifikaten är felfria
- sörja för spärrning av certifikat och publicering av spärrlistor
- iaktta en god dataskyddsnivå vid behandlingen av personuppgifter om certifikatinnehavarna samt en god informationsbehandlingssed
- skapa en kommunikationskod för individualisering av personer
- tillhandahålla ett system för kortbeställning och -administration som behövs för registrering och spärrning av kort.

1.3.2 Registrerare

Registreringen av ett tillfälligt certifikat görs med beaktande av lagen om stark autentisering och betrodda elektroniska tjänster och det förfaringssätt som beskrivs i dokumentet om certifieringspraxisen. Tillfälliga certifikat på en organisations reservkort registreras av en samarbetspartner som ingått registreringsavtal med Myndigheten för digitalisering och befolkningsdata. En närmare beskrivning av förfaringssättet ges i certifieringspraxisen för det aktuella tekniska underlaget.

- Registreraren agerar på uppdrag av certifikatutfärdaren och på dennes ansvar.
- Registreraren iakttar certifikatpolicyn och certifieringspraxisen.

- Registreraren identifierar certifikatsökanden på det sätt som beskrivs i certifieringspraxisen.
- Registreringsstället skickar in uppgifterna om identifieringen av certifikatsökanden och ansökan, och utifrån dessa uppgifter skapas certifikatet.
- Registreraren iakttar principerna om god behandling av personuppgifter.
- Myndigheten för digitalisering och befolkningsdata övervakar att kundorganisationen iakttar avtalsvillkoren om registreringen och bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster.
- Registreraren använder certifikatutfärdarens beställnings- och administrationssystem för registrering, beställning av reservkort och spärrning av tillfälliga certifikat.

1.3.3 Tillverkning och individualisering av reservkort eller chip

- De som tillverkar och individualiserar reservkort eller chip, relaterade nyckelpar och aktiveringsuppgifter agerar på certifikatutfärdarens uppdrag och ansvar och i enlighet med ett samarbetsavtal.
- De som tillverkar och individualiserar reservkort eller chip iakttar certifikatpolicyn och certifieringspraxisen.
- Reservkort och chip individualiseras enligt de uppgifter som registreraren lämnat.

1.3.4 Spärrtjänst

När det gäller reservkort används ingen likadan spärrtjänst för certifikat som för andra kort, utan registreraren i certifikatinnehavarens organisation spärrar ett reservkort i systemet för beställning och administration av kort. Certifikat som en certifikatinnehavare önskar spärra innan certifikatets giltighetstid löper ut spärras i detta system. Spärrade certifikat förs in på spärrlistan.

1.3.5 Publicering av uppgifter om tillfälliga certifikat

Registertjänsten är en offentlig webbtjänst som innehåller certifikatutfärdarens certifikat och spärrlista. Skapade tillfälliga certifikat publiceras inte i något register. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

1.3.6 Certifikatinnehavare

Tillfälliga certifikat i enlighet med denna certifikatpolicy kan utfärdas för personer som identifierats i enlighet med lagen om stark autentisering och betrodda elektroniska tjänster eller – när det handlar om tillfälliga certifikat personalen inom social- och hälsovården eller aktörer inom social- och hälsovården – kan certifikat dessutom överlåtas med beaktande av de krav som ställs i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna. Endast anställda och aktörer inom social- och

hälsovården kan vara innehavare av tillfälliga certifikat för personalen eller aktörerna inom social- och hälsovården.

Certifikatinnehavaren bör iaktta certifikatutfärdarens certifikatpolicy och certifieringspraxis.

1.3.7 Förlitande part

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

1.3.8 Användning av certifikat

Myndigheten för digitalisering och befolkningsdata iakttar denna certifikatpolicy vid utfärdandet av tillfälliga certifikat. Certifikatinnehavare och förlitande parter bör handla i enlighet med denna certifikatpolicy.

Tillfälliga certifikat som är förenliga med denna certifikatpolicy kan användas för stark autentisering av en person, kryptering av information eller för elektroniska signaturer. Certifikatet kan användas i enlighet med användningssyftet utan begränsningar inom förvaltningen 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.

1.4 Kontaktuppgifter

1.4.1 Organisation som förvaltar certifikatpolicyn

Denna certifikatpolicy är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister: Enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019) har Myndigheten för digitalisering och befolkningsdata bland annat till uppgift att tillhandahålla tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdata svarar för administrationen av denna certifikatpolicy och för uppdateringar i den.

Upphovsrätterna i enlighet med denna certifikatpolicy hör till Myndigheten för digitalisering och befolkningsdata.

1.4.2 Kontaktperson

Förfrågningar om certifikatpolicyn kan riktas 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

Frågor om certifikatpolicyn besvaras av enheten Certifikattjänster vid Myndigheten för digitalisering och befolkningsdata.

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.fineid.fi

2 Allmänna villkor

Certifikatpolicyn träder i kraft 1.6.2021. Förfaringssättet för att göra ändringar i och publicera certifikatpolicyn beskrivs i punkt 8 i detta dokument.

2.1 Skyldigheter

2.1.1 Certifikatutfärdarens skyldigheter

- Myndigheten för digitalisering och befolkningsdata har ett lagstadgat uppdrag att agera som certifikatutfärdare.
- Kundorganisationen ansvarar för sin del för spärrningen av certifikaten i enlighet med avtalet mellan MDB och kundorganisationen.
- Kundorganisationen ska kontrollera att uppgifterna om slutanvändarna är korrekta på det sätt som MDB och kundorganisationen har avtalat om.
- Utfärdaren iakttar gällande lagstiftning i sin verksamhet.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser samt möjlighet att täcka eventuella krav på skadestånd.
- Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer eller personer, såsom registrerare, och korttillverkare.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning vid utfärdandet av tillfälliga certifikat liksom andra aspekter på användningen av tillfälliga certifikat på ett allmänt plan.

- Utfärdaren utarbetar och upprätthåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren iakttar certifikatpolicyn och certifieringspraxisen.
- Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen och gör dem allmänt tillgängliga.
- Utfärdaren anställer tillräckligt med personal med sådan expertis, erfarenhet och kompetens som krävs för produktionen av certifikattjänster.
- Utfärdaren använder pålitliga system och produkter som är skyddade från obehörig användning.
- Utfärdaren tillhandahåller offentligt information om certifikat och certifikatverksamheten, utgående från vilken utfärdarens verksamhet och pålitlighet kan bedömas.
- Certifikatutfärdaren kan bevilja certifikat åt sin egen verksamhet. I så fall följer den samma förutsättningar som om certifikatet skulle beviljas åt någon annan organisation.

2.1.2 Registrerarens skyldigheter

- Registreraren iakttar certifikatpolicyn och certifieringspraxisen i samband med registreringen.
- Registreraren identifierar den som ansöker om certifikatet personligen och tillförlitligt på det sätt som beskrivs i certifieringspraxisen så att sökandens identitet och de övriga för utfärdandet behövliga uppgifterna kontrolleras omsorgsfullt.
- Registreraren ser till att personuppgifterna hanteras omsorgsfullt och konfidentiellt.
- Registreraren ger sökanden information om villkoren för användningen av certifikatet.
- Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med utfärdaren.

2.1.3 Certifikatinnehavarens skyldigheter

- Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen för varje enskild typ av certifikat samt i användaranvisningarna för certifikatinnehavaren. Ett certifikat får bara användas för sitt ändamål för autentisering, kryptering av information eller elektroniska signaturer.
- Innehavaren av ett tillfälligt certifikat ansvarar för att de uppgifter som lämnades vid ansökan är korrekta.

- Innehavaren av ett tillfälligt certifikat ansvarar för användningen av det, för de rättshandlingar som innehavaren gör med det och för de ekonomiska följderna av rättshandlingarna.

- Innehavaren av tillfälligt certifikat förvarar de hemliga nycklarna på chipet och de koder som behövs för användningen av chipet skilt från varandra och strävar efter att förhindra att de hemliga nycklarna försvinner, råkar i händerna på utomstående, skadas eller används av obehöriga. Om en certifikatinnehavare överlåter chipet eller röjer PIN-koden för en annan person, t.ex. genom att låna ut dem, befrias certifikatutfärdaren och den förlitande parten från de ansvar som eventuellt uppkommer vid användningen av chipet.

- Ett tillfälligt certifikat ska behandlas och skyddas lika omsorgsfullt som andra liknande chip, kort eller dokument, såsom kreditkort, körkort och pass. Personliga PIN-koder ska förvaras fysiskt på en annan plats än det tillfälliga certifikatet och det chip som innehåller hemliga nycklar.

- Om mikrochipet eller kortet har försvunnet eller om det finns risk för att de missbrukas ska en anmälan göras omedelbart till registreraren i certifikatinnehavarens organisation, som spärrar certifikatet i systemet för beställning och administration av kort.

2.1.4 Den förlitande partens skyldigheter

Den förlitande parten är skyldig att säkerställa att certifikatet används i enlighet med användningsändamålet. För ett autentiserings- och krypteringscertifikat är användningsändamålet återigen att identifiera personer och kryptera information. Ett signeringscertifikat kan bara användas för elektroniska signaturer.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan i god tro lita på det tillfälliga certifikatet efter att ha kontrollerat att certifikatkedjan är intakt, att det tillfälliga certifikatet är i kraft och att certifikatet inte finns på spärrlistan. En part som förlitar sig på ett tillfälligt certifikat är skyldig att kontrollera att certifikatet inte har tagits upp på spärrlistan. För att säkerställa tillförlitligheten hos ett tillfälligt certifikat ska den förlitande parten iaktta följande åtgärder för kontroll av spärrlistan eller ta fram statusuppgiften via OCSP-tjänsten.

En förlitande som kopierar spärrlistan från registret ska säkerställa spärrlistans autenticitet genom att kontrollera utfärdarens elektroniska signatur. Dessutom ska den förlitande parten kontrollera spärrlistans giltighetstid.

Om det på grund av störningar i systemet eller tjänsten inte går att få tillgång till den nyaste spärrlistan, får ett tillfälligt certifikat inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Om en förlitande part ändå godkänner ett tillfälligt certifikat efter att spärrlistans giltighetstid gått ut, sker det på den förlitande partens eget ansvar.

2.1.5 Skyldigheter vid publicering av tillfälliga certifikat

Spärrade tillfälliga certifikat publiceras på en spärrlista som den förlitande parten kan använda för att kontrollera att certifikatet är giltigt. Skapade tillfälliga certifikat publiceras inte i något register.

2.2 Ansvar

2.2.1 Certifikatutfärdarens ansvar

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

Myndigheten för digitalisering och befolkningsdata ansvarar för att tillfälliga certifikat skapas i enlighet med den förfaranden som lagts fram i lagen om stark autentisering och betrodda elektroniska tjänster, certifikatpolicyn och certifieringspraxisen samt att de uppfyller de i lagstiftningen fastställda skadeståndsansvaren för certifikatutfärdaren eller, om det handlar om tillfälliga certifikat som skapas för personalen eller för aktörer inom social- och hälsovårdsbranschen, utöver de ovan nämnda även är förenliga bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna. Myndigheten för digitalisering och befolkningsdata ansvarar endast för de uppgifter som Myndigheten för digitalisering och befolkningsdata har lagrat på certifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar för att det tillfälliga certifikatet kan användas från tidpunkten från överlåtelsen till giltighetstidens utgång – förutsatt att det används på tillbörligt sätt. Ett tillfälligt certifikat överlåts till en person som identifierats på det sätt som förutsätts vid tillfälliga certifikat. Före undertecknandet av avtalet har certifikatinnehavaren fått bruksanvisningar för det tillfälliga certifikatet.

Genom att underteckna det tillfälliga certifikatet med sin hemliga nyckel intygar certifikatutfärdaren att personuppgifterna på certifikatet har kontrollerats på det sätt som beskrivs i certifikatpolicyn och certifieringspraxisen.

Certifikatutfärdaren ansvarar för att certifikat som spärrats av registreraren i certifikatinnehavarens organisation tas upp på spärrlistan inom den tid som föreskrivs i denna certifikatpolicy.

2.2.2 Registrerarens ansvar

Ett tillfälligt certifikat registreras av ett registreringsställe som registrerar certifikatsökanden för certifikatutfärdarens, dvs. Myndigheten för digitalisering och befolkningsdatas räkning utifrån ett avtal som ingåtts separat för denna verksamhet. Registreraren ansvarar för sin registreringsverksamhet och för spärrning av certifikat. Vid registreringen iakttas kraven i lagen om elektronisk autentisering och betrodda elektroniska tjänster och i certifieringspraxisen eller, om det handlar om tillfälliga certifikat som utfärdas för personalen eller för aktörer inom social- och hälsovården, utöver de ovan nämnda även bestämmelserna i lagen om elektronisk behandling av

klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna.

2.2.3 Certifikatinnehavarens ansvar

Innehavaren av ett tillfälligt certifikat ansvarar för användningen av det, för de rättshandlingar som innehavaren gör med det och för de ekonomiska följderna av rättshandlingarna.

Om ett kort som innehåller ett chip blir kvar i en kortläsare finns det risk för missbruk av det tillfälliga certifikatet. En certifikatinnehavare som avslutar en terminalsession ska avlägsna chipet med det tillfälliga certifikatet från avläsaren och på föreskrivet sätt stänga de program som har använts eller annars avbryta den tekniska förbindelse som behövs för användningen av certifikatet.

Certifikatinnehavarens ansvar för användningen av certifikatet upphör när han eller hen har meddelat registreraren i certifikatinnehavarens organisation om behovet av att spärra certifikatet och fått bekräftelse på att begäran om spärrning har emottagits. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

2.2.4 Den förlitande partens ansvar

En part som förlitar sig på ett tillfälligt certifikat kan inte i god tro lita på certifikatet ifall parten inte har kontrollerat att organisationscertifikatet är i kraft med hjälp av OCSP-tjänsten eller spärrlistan. Om det tillfälliga certifikatet godkänns i en sådan situation frias Myndigheten för digitalisering och befolkningsdata från ansvar. Den förlitande parten ska kontrollera att det utfärdade certifikatet motsvarar användningsändamålet i den rättshandling där det används.

2.2.5 Begränsning av ansvar

Myndigheten för digitalisering och befolkningsdata omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna i skadeståndslagen (412/1974).

Myndigheten för digitalisering och befolkningsdata ansvarar inte för eventuella skador som orsakas av att PIN-koden eller certifikatinnehavarens hemliga nycklar röjs, om inte avslöjandet direkt har orsakats av Myndigheten för digitalisering och befolkningsdatas 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, dock högst 15 procent av den aktuella kundorganisationens certifikatfakturering under de föregående 3 månaderna (MDB:s andel).

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 certifikatinnehavaren.

Myndigheten för digitalisering och befolkningsdata ansvarar inte för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel internet, eller för att en rättshandling inte kan utföras på grund av att certifikatinnehavarens utrustning eller kortläsarprogram inte fungerar eller för att certifikatet används i strid med sitt syfte.

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

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

Certifikatutfärdaren ansvarar inte för ett fel i en nättjänst eller en tillämpning avsedd för slutanvändare som använder certifikatet eller för kostnaderna för detta fel.

2.3 Ekonomiskt ansvar

2.3.1 Certifikatutfärdare

Myndigheten för digitalisering och befolkningsdata omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna i skadeståndslagen (412/1974).

Myndigheten för digitalisering och befolkningsdata ansvarar gentemot en förlitande part högst till beloppet av de omedelbara skadorna, såsom beskrivits i ovan i avsnittet om begränsningar av ansvaret.

2.3.2 Övriga parter

Förlitande parter kan lita på att tillfälliga certifikat eller elektroniska signaturer är korrekta efter att ha kontrollerat att certifikatkedjan är intakt, att certifikatet inte har upptagits på någon spärrlista och att certifikatets giltighetstid inte har gått ut, när det inte föreligger andra skäl att misstänka att certifikatet inte används korrekt. Uppgiften om ett certifikats status kan också kontrolleras i en OCSP-tjänst.

Utfärdaren svarar för ett tillfälligt certifikat enligt åtagandena i denna certifikatpolicy och i den certifieringspraxis som gäller tillfälliga certifikat.

2.3.3 Certifikatutfärdarens ekonomiförvaltning

Myndigheten för digitalisering och befolkningsdatas certifikattjänster omfattas av ett system för ekonomisk förvaltning och tillsyn som föreskrivits om separat.

Certifikatutfärdarens ekonomiförvaltning beskrivs mer ingående i certifieringspraxisen.

2.4 Tolkning och verkställighet

2.4.1 Lagstiftning som tillämpas

Myndigheten för digitalisering och befolkningsdata omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna i skadeståndslagen (412/1974). Om det tillfälliga certifikatet har skapats för en medlem av personalen inom social- och hälsovården eller aktörer inom social- och hälsovården, iakttas dessutom bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de bestämmelser och villkor som meddelats med stöd av dem.

Myndigheten för digitalisering och befolkningsdata iakttar god behandling av personuppgifter enligt personuppgiftslagen (523/1999) och god informationshantering enligt lagen om offentlighet i myndigheternas verksamhet (621/1999). Informationssäkerheten på Myndigheten för digitalisering och befolkningsdata tryggas bl.a. genom kontinuerlig utbildning. Myndigheten för digitalisering och befolkningsdata har också berett uppförandekoder både för informationstjänsterna och för certifikattjänsterna.

Myndigheten för digitalisering och befolkningsdata skaffar tjänster i anslutning till registrering och identifiering av personer med stöd av ett separat, privaträttsligt avtal om registreringsåtgärderna. Myndigheten för digitalisering och befolkningsdata kan skaffa dessa tjänster till exempel genom att iaktta bestämmelserna i lagen om samservice inom den offentliga förvaltningen (223/2007).

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

Myndigheten för digitalisering och befolkningsdata ansvarar för att tillfälliga certifikat skapas i enlighet med den förfaranden som lagts fram i lagen om stark autentisering och betrodda elektroniska tjänster, certifikatpolicyn och certifieringspraxisen samt att de uppfyller de i lagstiftningen fastställda skadeståndsansvaren för certifikatutfärdaren eller, om det handlar om tillfälliga certifikat som skapas för personalen eller för aktörer inom social- och hälsovårdsbranschen, utöver de ovan nämnda även är förenliga bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna.

I enlighet med lagen om stark autentisering och betrodda elektroniska tjänster utövas tillsynen över Myndigheten för digitalisering och befolkningsdatas verksamhet av Traficom, som utfärdar behövliga föreskrifter och rekommendationer för verksamheten.

Beträffande behandlingen av personuppgifter iakttar Myndigheten för digitalisering och befolkningsdata personuppgiftslagen. Myndigheten för digitalisering och befolkningsdata samarbetar kontinuerligt med dataskyddsombudsmannen i frågor som gäller behandling av personuppgifter.

Vid avgörandet av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning.

2.4.2 Avgörande av tvister

Vid utfärdandet av certifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att det tillfälliga certifikatet uppfyller de krav som ställs på det i certifikatpolicyn.

Vid avgörandet av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning. När tillfälliga certifikat sätts i omlopp, iakttas särskilt lagen om stark autentisering och betrodda elektroniska tjänster samt det förfarande för övervakning och ändringar av certifikaten som beskrivs i lagen.

Vid utfärdandet av certifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att det tillfälliga certifikatet uppfyller de krav som ställs på det i certifikatpolicyn. Eventuella tvister avgörs enligt rättssystemet i Finland av Helsingfors tingsrätt.

2.5 Avgifter

I detta avsnitt behandlas avgifterna i anslutning till användningen av tillfälliga certifikat.

2.5.1 Utfärdande och förnyelse av tillfälliga certifikat

Ansökan om ett tillfälligt certifikat görs enligt beskrivningen i certifieringspraxisen.

Anskaffningspriset för ett reservkort bestäms enligt vid var tid gällande förordning om avgifterna för Myndigheten för digitalisering och befolkningsdatas prestationer.

Tillfälliga certifikat prissätts enligt gällande prislista för Myndigheten för digitalisering och befolkningsdatas affärsekonomiska prestationer.

2.5.2 Avgifter i anslutning till användning av tillfälliga certifikat

Certifikatutfärdaren kan inte debitera certifikatinnehavare separat för användningen av certifikaten, spärrlistan eller det offentliga registret. Enskilda tillhandahållare av e-tjänster kan debitera för användningen av sin egen tjänst. Användningen av ett certifikat förutsätter ingen särskild anmälan eller särskilt tillstånd av utfärdaren.

2.5.3 Avgifter i anslutning till spärrning av tillfälliga certifikat

Det kostar ingenting att anmäla ett tillfälligt certifikat till spärrlistan. Att hämta spärrlistor från registret och kontrollera att ett tillfälligt certifikat är i kraft är också gratis.

2.5.4 Övriga avgifter

För rådgivningstjänsten debiteras en särskild avgift enligt gällande prislista.

Om en tjänsteleverantör vill tillhandahålla en informationsförsörjningstjänst mellan de tillfälliga certifikatens identifieringskoder och identifieringsuppgifterna i sitt eget bakgrundssystem eller andra uppdateringsuppgifter, kan tjänsteleverantören ansöka om tillstånd hos Myndigheten för digitalisering och befolkningsdata för utlämning av uppgifter till informationsförsörjningstjänsten. Denna tjänst prissätts enligt gällande lag om grunderna för avgifter till staten och finansministeriets förordning om Myndigheten för digitalisering och befolkningsdatas prestationer.

Bruksvillkoren för ett tillfälligt certifikat överlåts till certifikatinnehavaren vid mottagandet av certifikatet.

2.6 Publikation av och tillgång till information

Publicering av information från certifikatutfärdaren

Certifikatutfärdaren publicerar certifikatutfärdarens certifikat och spärrlistor i ett avgiftsfritt och allmänt tillgängligt offentligt register. Skapade tillfälliga certifikat publiceras inte. Certifikatutfärdaren publicerar certifikatpolicyn, dokument över olika certifieringspraxis, certifikatbeskrivningen (PDS) samt övriga offentliga dokument med anknytning till produktionen av certifikattjänster på sin webbplats.

2.6.1 Publikationsfrekvens

Certifikatutfärdaren publicerar en spärrlista som är i kraft i åtta timmar efter publiceringen. Spärrlistan uppdateras med en ny spärrlista en gång i timmen.

2.6.2 Tillgång till information

Uppgifterna i registret och spärrlistan är offentligt tillgängliga. De offentliga FINEID-specifikationerna som certifikatutfärdaren publiceras finns på certifikatutfärdarens webbplats. Certifikatpolicyerna och certifieringspraxisen finns också på certifikatutfärdarens webbplats.

2.6.3 Datalager

Information som publiceras av certifikatutfärdaren finns på certifikatutfärdarens webbplats och i ett offentligt register som är förenligt med denna certifikatpolicy. Konfidentiella data i certifikatsystemet har sparats i certifikatutfärdarens egna, konfidentiella datalager. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Personuppgifter behandlas särskilt omsorgsfullt. Myndigheten för digitalisering och befolkningsdata har publicerat särskilda uppförandekoder enligt personuppgiftslagen som gäller produktionen av certifikattjänster. Utfärdaren har även berett en registerbeskrivning i enlighet med personuppgiftslagen angående hanteringen av personuppgifter i certifikatsystemet.

2.7 Granskning av informationssäkerheten

Traficom, som utövar tillsyn över dem som tillhandahåller identifieringstjänster, har rätt att granska utfärdarens verksamhet på villkor som bestämts i lagen om stark autentisering och betrodda elektroniska tjänster.

2.7.1 Granskningsfrekvens

Myndigheten för digitalisering och befolkningsdata granskar de tekniska leverantörernas lokaler, utrustning och verksamhet på ett ändamålsenligt sätt.

Granskningsförfarandet beskrivs i detalj i certifieringspraxisen.

2.7.2 Granskare

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

2.7.3 Föremål för granskningen och granskningens omfattning

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

Granskningen utförs med beaktande av genomförandet av åtta delområden inom informationssäkerhet. Egenskaper som kontrolleras är bl.a. konfidentialitet, integritet och användbarhet.

Vid granskningen jämförs policyn, certifieringspraxisen och tillämpningsanvisningarna med verksamheten med hänsyn till hela certifikatorganisationen och -systemet. Myndigheten för digitalisering och befolkningsdata övervakar att tillämpningsanvisningarna stämmer överens med certifikatpolicyn.

Vid granskningar beaktas utöver den administrativa informationssäkerheten även tjänsteleverantörerna.

Åtgärder vid avvikelser

Upptäckta avvikelser antecknas i granskningsrapporten och åtgärder vidtas enligt lagen, informationssäkerhetsstandarden ISO 27001 och gällande leveransavtal.

2.7.4 Information om resultatet av granskningen

Information om resultatet av granskningen ges ut i enlighet med lagen, informationssäkerhetsstandarden ISO 27001, Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy och gällande leveransavtal. Det detaljerade och formbundna granskningsresultatet avsett för internt bruk är konfidentiellt och offentliggörs inte. Formbundna rapporter utarbetas separat för bruk utanför organisationen.

Myndigheten för digitalisering och befolkningsdata rapporterar om granskningsresultaten bland annat till Traficom.

2.8 Publicering av information

2.8.1 Information som publiceras av certifikatutfärdaren

Uppgifterna i certifikatsystemet är konfidentiella, såvida de inte grundar sig på bestämmelserna om utlämnande av uppgifter i personuppgiftslagen, lagen om offentlighet i myndigheternas verksamhet, lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster eller lagen om stark autentisering och betrodda elektroniska tjänster eller på ändamål som fastställts i certifikatpolicyn eller certifieringspraxisen.

2.8.2 Offentlig information

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

Information om att ett tillfälligt certifikats giltighetstid har gått ut eller avbrutits

När ett tillfälligt certifikats giltighetstid börjar och upphör finns angivet på certifikatet. Certifikat som spärrats under giltighetstiden publiceras på en allmänt tillgänglig spärrlista.

2.8.3 Information som lämnas ut till myndigheter

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

2.8.4 Övrig information

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

2.8.5 Utlämnande av information på certifikatinnehavarens begäran

Certifikatinnehavaren har rätt att få uppgifter som rör honom eller henne själv, t.ex. personuppgifter, i enlighet med gällande lagstiftning.

2.8.6 Övriga principer gällande utlämnande av information

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

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

2.9 Immateriella rättigheter

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 certifikatpolicy.

3 Identifiering av certifikatsökanden

3.1 Registrering

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

I ansökningshandlingen nämns tydligt att den som ansöker om ett tillfälligt certifikat intygar riktigheten hos uppgifterna med sin underskrift samt godkänner att certifikatet skapas och publiceras enligt avtalet. På samma gång godkänner sökanden reglerna och villkoren i anslutning till användningen av tillfälliga certifikat och förbinder sig att förvara certifikaten och PIN-koderna omsorgsfullt samt att anmäla eventuellt missbruk eller försvunnet kort.

Utfärdaren, registreraren, korttillverkaren samt leverantörer av övriga delområden av certifikattjänsterna har ingått avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheter för samtliga parter. Sökanden av ett tillfälligt certifikat ansvarar för att samtliga uppgifter som är väsentliga för certifikatet och som sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren av ett tillfälligt certifikat får bara använda det för de fastställda ändamålen.

När en certifikatutfärdare utfärdar ett tillfälligt certifikat är det samtidigt ett godkännande av certifikatansökan.

Innehavaren av tillfälliga certifikat ansvarar för att de hemliga nycklarna och de relaterade aktiveringskoderna förvaras på det sätt som beskrivs i bruksvillkoren så att de inte används i strid med villkoren.

En certifikatinnehavare som misstänker att det blivit möjligt att använda det tillfälliga certifikatet i strid med avtalsvillkoren ska genast anmäla detta till registreraren i certifikatinnehavarens organisation, som spärrar certifikatet.

3.1.1 Benämningspraxis

Benämningspraxisen beskrivs detaljerat i certifieringspraxisen.

Certifikatutfärdarens öppna nyckel är en del av certifikatutfärdarens certifikat (utfärdarcertifikatet). Utfärdarcertifikatet fås från det offentliga registret. Om ett tillfälligt certifikat finns lagrat på ett aktivkort kommer även utfärdarcertifikatet att placeras på aktivkortets chip.

Uppgifterna om certifikatinnehavaren fastställer entydigt innehavaren. Utfärdaren utreder vid behov innehavarens officiella identitet.

3.1.2 Leverans av hemliga nycklar till certifikatinnehavaren

De hemliga nycklarna i anslutning till tillfälliga certifikat som skapats på ett chip eller i en annan säker miljö levereras till innehavaren i samband med överlåtelsen.

Leveransen av hemliga nycklar beskrivs i detalj i certifieringspraxisen.

3.2 Förnyelse av nyckelpar

De öppna nycklarna på tillfälliga certifikatet och de hemliga nycklarna på chip kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt tillfälligt certifikat.

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

3.3 Förnyelse av nyckelpar efter att ett certifikat införts på spärrlistan

De öppna nycklarna på tillfälliga certifikatet och de hemliga nycklarna på chip kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt tillfälligt certifikat.

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

3.4 Identifiering av den som begär spärrning

Certifikatinnehavaren kan begära att ett tillfälligt certifikat spärras innan dess giltighetstid löpt ut.

Begäran om spärrning ska i första hand göras av registreraren i certifikatinnehavarens organisation, om han eller hon märker att ett certifikat har försvunnit eller om det blivit möjligt att missbruka certifikatet.

Spärrningen ska göras omedelbart när det finns anledning att misstänka missbruk av ett certifikat som kommit bort eller stulits.

Alla elektroniska åtgärder i anslutning till spärrningen arkiveras.

Spärrning av certifikat beskrivs i detalj i certifieringspraxisen.

4 Funktionella krav

4.1 Ansökan om certifikat

Rättigheterna och skyldigheterna för den som ansöker om ett certifikat ingår i ansökningshandlingen och i de allmänna bruksvillkoren, som utgör avtalet som ingås med sökanden. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter. Den som ansöker om ett tillfälligt certifikat godkänner de allmänna bruksvillkoren i samband med ansökan.

I ansökningshandlingen och i bruksanvisningen nämns tydligt att den som ansöker om ett tillfälligt certifikat intygar riktigheten hos uppgifterna med sin underskrift samt godkänner att certifikatet skapas. På samma gång godkänner sökanden reglerna och villkoren i anslutning till användningen av det tillfälliga certifikatet och förbinder sig att förvara certifikatet och PIN-koderna omsorgsfullt samt att anmäla eventuellt missbruk eller försvunnet certifikat/chip.

4.2 Utfärdande av certifikat

Utfärdaren utfärdar det tillfälliga certifikatet i och med godkännandet av certifikatansökan. Utfärdaren ansvarar vid utfärdandet av det tillfälliga certifikatet för att datainnehållet i certifikatet är riktigt vid tidpunkten för överlåtelsen av certifikatet.

4.3 Mottagande av certifikat

Tillfälliga certifikat ska avhämtas personligen på registreringsstället.

Vid överlåtelsen framhävs det för certifikatsökanden att det inte finns några kopior av de hemliga nycklarna och att sådana inte heller kan göras i ett senare skede.

4.4 När ett certifikats giltighet går ut eller avbryts

4.4.1 Förutsättningar för spärrning av certifikat

Om det finns anledning att misstänka missbruk, till exempel om ett kort har kommit bort eller stulits, ska det tillfälliga certifikatet införas på spärrlistan.

4.4.2 Genomförandet av spärrningen

Registreraren i certifikatinnehavarens organisation spärrar certifikatet.

4.4.3 Spärrhändelsen

Ett certifikat kan spärras via systemet för beställning och administration av kort, vilket tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

En uppgift om att certifikatet har införts på spärrlistan och finns offentligt tillhanda senast när det gått en timme från att begäran om spärrning konstaterades behörig och godkändes. En spärrlista är i kraft i åtta timmar.

Spärrning av certifikat och konsekvenserna av spärrning beskrivs i detalj i certifieringspraxisen.

Spärrning av certifikat på Myndigheten för digitalisering och befolkningsdatas begäran

Myndigheten för digitalisering och befolkningsdata spärrar certifikat endast i följande situationer:

- Myndigheten för digitalisering och befolkningsdata kan spärra certifikat som signerats med Myndigheten för digitalisering och befolkningsdatas hemliga nyckel om det finns anledning att misstänka att Myndigheten för digitalisering och befolkningsdatas hemliga nycklar har röjts eller råkat i fel händer.
- Samtliga giltiga certifikat som utfärdats med den röjda nyckeln ska spärras på en eller flera spärrlistor vilkas giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.
- Om den hemliga nyckeln eller annan teknisk metod som använts vid skapandet av Myndigheten för digitalisering och befolkningsdatas certifikat har röjts eller på annat vis blivit oanvändbar ska Myndigheten för digitalisering och befolkningsdata meddela det inträffade till samtliga kortinnehavare.
- Myndigheten för digitalisering och befolkningsdata kan spärra ett certifikat också av annan särskild anledning.

4.4.4 Tidpunkten för en spärrhändelse

Spärrningen genomförs omedelbart i samband med begäran om spärrning. Spärrade tillfälliga certifikat kan inte återställas.

4.4.5 Krav i anslutning till avbrott i certifikatets giltighetstid

Giltighetstiden för ett tillfälligt certifikat kan inte avbrytas tillfälligt.

4.4.6 Vem kan göra begäran om avbrott?

Giltighetstiden för ett tillfälligt certifikat kan inte avbrytas tillfälligt.

4.4.7 Hur görs begäran om avbrott?

Giltighetstiden för ett tillfälligt certifikat kan inte avbrytas tillfälligt.

4.4.8 Begränsningar i avbrottstiden

Giltighetstiden för ett tillfälligt certifikat kan inte avbrytas tillfälligt.

4.4.9 Publiceringsfrekvens för spärrlista

En uppgift om att certifikatet har införts på spärrlistan och finns offentligt tillhanda senast när det gått en timme från att begäran om spärrning konstaterades behörig och godkändes. En spärrlista är i kraft i åtta timmar.

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

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

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

4.4.10 Krav i anslutning till kontroll av spärrlistor

Den förlitande partens skyldigheter beskrivs i avsnitt 2.1.4

4.4.11 Kontroll av ett certifikats status i realtid

Certifikatutfärdaren tillhandahåller en tjänst för kontroll av certifikatens status i realtid, en OCSP-tjänst. Certifikatutfärdaren publicerar en spärrlista över spärrade certifikat.

4.4.12 Krav i anslutning till kontroll av ett certifikats status i realtid

Certifikatutfärdaren tillhandahåller en tjänst för kontroll av certifikatens status i realtid.

4.4.13 Särskilda krav i en situation där certifikatinnehavarens hemliga nyckel har röjts

Certifikatinnehavaren ansvarar för en skyddad användning av de hemliga nycklarna och ska ta hand om chipet eller kortet och koderna på det sätt som beskrivs i bruksvillkoren. En certifikatinnehavare som misstänker att det blivit möjligt att använda det tillfälliga certifikatet i strid med avtalsvillkoren ska genast anmäla detta till registreraren i certifikatinnehavarens organisation, som spärrar certifikatet.

4.5 Övervakningen av systemet

Övervakningen av systemet beskrivs i certifieringspraxisen.

4.6 Arkivering av data i anslutning till certifikat

4.6.1 Material som arkiveras

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas för dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i minst 5 år från tidpunkten då certifikaten upphört att gälla. Om det tillfälliga certifikatet har skapats för en medlem av personalen inom social- och hälsovården eller aktörer inom social- och hälsovården, iakttas dessutom bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de bestämmelser och villkor som meddelats med stöd av dem.

Vilka uppgifter som arkiveras av certifikatutfärdaren beskrivs i detalj i certifieringspraxisen.

Arkivuppgifterna förvaras enligt bestämmelserna för myndigheten.

4.6.2 Skydd av arkiv

Uppgifterna förvaras i lokaler med hög säkerhetsnivå och passagekontroll.

4.6.3 Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

4.6.4 Metoder för införskaffning och tryggande av arkiverat material

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

4.7 Kontinuiteten i verksamheten och hantering av exceptionella situationer

Myndigheten för digitalisering och befolkningsdata har en kontinuitets- och beredskapsplan som gör att Myndigheten för digitalisering och befolkningsdatas verksamhet kan fortsätta i exceptionella situationer.

Beredskapen för exceptionella situationer beskrivs i certifieringspraxisen.

4.7.1 Utfärdarens hemliga nyckel har röjts eller certifikatutfärdarens certifikatet har spärrats

Utfärdaren uppger i varje certifieringspraxis de åtgärder som certifikatinnehavarna, de förlitande parterna och registrerarna och certifikatutfärdarens anställda ska vidta ifall certifikatutfärdarens hemliga nyckel har röjts eller på annat sätt blivit oanvändbar.

4.7.2 Äventyrande av säkerheten till följd av en naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas säkerhetspolicy beaktas åtgärder som förorsakas om den externa säkerheten äventyras. Myndigheten för digitalisering och befolkningsdata har fått informationssäkerhetscertifikatet ISO 27001, som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även vid en eventuell katastrof.

4.8 Nedläggning av certifikatutfärdarens verksamhet

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

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

Före nedläggningen ska åtminstone följande åtgärder vidtas:

- Samtliga utfärdade och giltiga certifikat spärras på en eller flera spärrlistor, vilkas giltighetstid inte upphör förrän giltighetstiden för de sista spärrade certifikatet har löpt ut.
- Utfärdaren upphäver samtliga avtalspartners befogenheter att för utfärdarens räkning utföra uppgifter med anknytning till processen för utfärdande av certifikat.

- Utfärdaren säkerställer att tillgången till utfärdarens arkiv som nämns i punkt 4.6 bevaras även efter att utfärdarens verksamhet upphört.

- Certifikatutfärdaren iakttar bestämmelserna om arkivering i lagen om elektronisk autentisering och betrodda elektroniska tjänster och även för övrigt bestämmelserna i arkivlagen eller, om det handlar om tillfälliga certifikat som utfärdas för personalen eller för aktörer inom social- och hälsovården, utöver de ovan nämnda även bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007), kraven i bestämmelser som utfärdats med stöd av dessa lagar eller krav som fastställts utifrån bestämmelserna.

5 Fysiska krav, funktionella krav och krav på personalens säkerhet

Myndigheten för digitalisering och befolkningsdata har beviljats ett certifikat som intygar att informationssäkerheten vid MDB uppfyller kraven i standarden ISO/IEC 27001.

5.1 Arrangemang i anslutning till den fysiska säkerheten

Myndigheten för digitalisering och befolkningsdata har beviljats ett certifikat som intygar att informationssäkerheten vid MDB uppfyller kraven i standarden ISO/IEC 27001:1999. Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. MDB ansvarar i egenskap av certifikatutfärdare för säkerheten och funktionerna inom samtliga delområden av certifikatproduktionen.

Säkerhetsarrangemangen beskrivs i detalj i certifieringspraxisen.

5.1.1 Läge och byggnadernas egenskaper

Utfärdarens system finns i maskinsalar med hög nivå av säkerhet och uppfyller anvisningarna och bestämmelserna om säkerhet i datorcentraler.

Säkerheten i verksamhetslokalerna bygger på att obehöriga inte har tillträde till lokalerna.

5.1.2 Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässig uppgifter inom certifikatsystemet utförs är försedda med passerkontroll. Passerkontrollsystemet upptäcker både tillåtet och otillåtet tillträde. Tillträde till maskinsalar förutsätter autentisering, varvid personen identifieras och hans eller hennes rättigheter kontrolleras och händelsen registreras. Maskinsalarna övervakas dygnet runt.

5.1.3 Reservarrangemang

Hårdvarulösningarna har förverkligats i enlighet med god informationsförvaltningssed så 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 för och servicen på viktig utrustning har säkerställts.

5.2 Funktionella krav

5.2.1 Ansvarsfördelning

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

Certifikatutfärdarens uppgifter är indelade i uppgiftsspecifika ansvarsområden. Dessa beskrivs detaljerat i certifieringspraxisen.

5.2.2 Antalet personer som krävs för olika uppgifter

Skapande, aktivering, säkerhetskopiering och återställande av utfärdarens hemliga nycklar är åtgärder som utförs under kontrollerade former där två personer med administrationsbehörighet är närvarande.

Det är möjligt att återkalla certifikatutfärdarens hemliga nyckel bara om två behöriga personer övervakar åtgärden.

Vid formateringen av den kryptografiska modulen för utfärdarens hemliga nyckel närvarar minst två personer med administrationsbehörighet.

För användningen av systemet krävs närvaro av en för uppgiften behörig person.

Registrering av tillfälliga certifikat och identifiering av sökande kräver att en person är närvarande.

5.2.3 Uppgiftsspecifik identifiering

Identifieringen av och befattningsbeskrivningen för den som registrerar ett tillfälligt certifikat, administratören av certifikatsystemet och den som använder certifikatsystemet har beskrivits i detalj i certifieringspraxisen.

5.3 Personsäkerhet

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

Myndigheten för digitalisering och befolkningsdata fäster särskild uppmärksamhet vid såväl den egna personalens som leverantörernas och registrerarnas pålitlighet och kompetens för att utföra uppgifterna.

5.3.1 Utredning av personalens bakgrund

Myndigheten för digitalisering och befolkningsdata utför en grundläggande säkerhetsutredning av den egna personalen och av de personer som arbetar med certifikatsystemet hos de tekniska leverantörerna.

5.3.2 Förfarande vid utförande av bakgrundsutredning

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

Förfarandet för säkerhetsutredningen beskrivs detaljerat i certifieringspraxisen.

5.3.3 Krav på utbildning

Personalen på Myndigheten för digitalisering och befolkningsdata ska ha sådan utbildning att de kan utföra sina uppgifter på bästa möjliga sätt. Myndigheten för digitalisering och befolkningsdata har en utbildningsplan. Myndigheten för digitalisering och befolkningsdatas förvaltningsenhet ansvarar för genomförandet av planen.

5.3.4 Upprätthållande av sakkunskap och kompetens

Personalutbildningen planeras och ses över för att de anställda ständigt ska ha den sakkunskap som behövs för utförandet av uppgifterna på bästa möjliga sätt.

5.3.5 Krav på uppgiftsrotation

Då utfärdaren planerar arbetsrotation inom sin verksamhet ska uppgifterna organiseras så att den anställda kan utföra sina nya uppgifter på bästa möjliga sätt. I planeringen av arbetsrotationen beaktas god informationsförvaltningssed och bevarandet av en tillräcklig kompetensnivå för respektive uppgift.

Även inom arbetsrotationen iakttas Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy och informationssäkerhetsplan liksom Myndigheten för digitalisering och befolkningsdatas övriga allmänna anvisningar.

5.3.6 Åtgärder vid avvikelser

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

5.3.7 Personal som företräder 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.

5.3.8 Dokument som tillhandahålls personalen

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

6 Tekniska säkerhetsarrangemang

6.1 Skapa och lagra nyckelpar

6.1.1 Skapa nyckelpar

Certifikatutfärdare:

Certifikatutfärdaren skapar sina hemliga signeringsnycklar och de öppna nycklar som motsvarar de hemliga signeringsnycklarna. Utfärdarens hemliga nycklar förvaras i kryptografiska moduler.

Certifikatinnehavare:

Certifikatinnehavarens nyckelpar skapas under säkra förhållanden. Den öppna nyckeln används för att skapa certifikat och den hemliga nyckeln förvaras på ett läs- och skrivskyddat chip.

6.1.2 Överlåtelse av certifikatinnehavarens hemliga nyckel

Den PIN-kod som behövs för användningen av certifikatet ges till certifikatinnehavaren i samband med registreringen.

När ett reservkort överlåts får certifikatsökanden sin hemliga nyckel registrerad på chipet.

6.1.3 Leverans av certifikatinnehavarens öppna nyckel

Med hjälp av de öppna nycklarna på chipet görs en begäran om skapande av certifikat. I begäran kopplas certifikatsökandens registreringsuppgifter till den öppna nyckeln i fråga. På det här sättet uppkommer ett tillfälligt certifikat för certifikatinnehavaren.

Det tillfälliga certifikatet innehåller certifikatinnehavarens öppna nyckel.

6.1.4 Distribution av certifikatutfärdarens öppna nyckel till certifikatinnehavaren

Utfärdarcertifikatet innehåller utfärdarens öppna nyckel. Utfärdarcertifikatet lagras i ett offentligt register. Utfärdarcertifikatet fås även från utfärdarens offentliga register och på utfärdarens webbplats.

6.1.5 Längden på nycklar

Utfärdarens hemliga nyckel som använts för signering av ett tillfälligt certifikat och den motsvarande öppna nyckeln är 4096 bitars RSA-nycklar och 384 bitars ECC-nycklar.

Certifikatinnehavarens hemliga och öppna nycklar är 2048-bitars RSA-nycklar och 384 bitars ECC-nycklar.

6.1.6 Nycklarnas användningsändamål

Datainnehållet i ett certifikat har ett fält som fastställer användningsändamålet för nyckeln i anslutning till certifikatet (till exempel autentisering och kryptering av information). Användningen av nyckeln begränsas bara till användningsändamålet: en nyckel som är avsedd för autentisering och kryptering ska således bara användas för detta ändamål, och en nyckel som är avsedd för signering ska bara användas för elektroniska signaturer.

Certifikatutfärdarens certifikat:

Ändamål: Signering av certifikat och spärrlistor. Den tekniska beskrivningen finns i FINEID S2-specifikationerna.

Certifikatinnehavarens autentiserings- och krypteringscertifikat:

Ändamål: Verifiering av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signeringscertifikat

Ändamål: Elektroniska signaturer.

6.2 Skydd av hemlig nyckel

6.2.1 Standarder som gäller säkerhetsmodulen

Certifikatutfärdarens hemliga nycklar förvaras i kryptografiska moduler som administreras av utfärdaren och som är förenliga med kraven i tillämpliga säkerhetsstandarder.

Utfärdaren ser till att utfärdarens hemliga nycklar inte kan röjas eller missbrukas. För att tillgodose kraven på säkring av kritisk information tas en säkerhetskopia av utfärdarens hemliga nycklar.

6.2.2 Personal som medverkar i behandlingen av certifikatutfärdarens hemliga nyckel

För att hemliga nycklar ska kunna skapas och användas krävs att minst två personer är närvarande samtidigt eller aktiverar åtgärden.

6.2.3 Överlåtelse av hemlig nyckel till betrodd part

Certifikatinnehavarnas hemliga nycklar skapas under säkra former på det sätt som certifikatet förutsätter. Nyckelpar som en certifikatinnehavare skapar själv godkänns inte. En hemlig nyckel kan inte överföras eller kopieras från reservkortet. Certifikatutfärdaren och korttillverkaren har ingen åtkomst till certifikatinnehavarnas hemliga nycklar.

I det skede när nycklarna skapas har de ännu inte inpassats på någon person.

6.2.4 Säkerhetskopia av hemlig nyckel

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

6.2.5 Arkivering av hemlig nyckel

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

6.2.6 Administrering av hemlig nyckel i kryptografiska moduler

Certifikatutfärdarens hemliga signeringsnycklar skyddas med fysiska och logiska säkerhetsåtgärder av hög tillitsnivå. De används bara i system som förlagts till en säker miljö.

Administrationen av den hemliga nyckeln beskrivs i detalj i certifieringspraxisen.

6.3 Övriga omständigheter i anslutning till nyckeladministration

6.3.1 Arkivering av öppen nyckel

Utfärdaren arkiverar alla certifierade öppna nycklar.

6.3.2 Användningstiden för öppna och hemliga nycklar

Användningstiden är förenlig med avtalet, högst tre (3) månader. Ett certifikat kan spärras under dess giltighetstid.

6.4 Aktiveringsuppgift

6.4.1 Skapa och ta i bruk aktiveringsuppgiften

Korttillverkaren skapar aktiveringsuppgifterna som behövs för användningen av nycklarna, dvs. PIN-koden.

Förfarandet beskrivs i detalj i certifieringspraxisen.

6.4.2 Skydd av aktiveringsuppgifter

PIN-koden har skyddats så att den inte kan läsas eller kopieras från kortet. Certifikatinnehavaren ansvarar för en skyddad nyckelanvändning och ska ta hand om chipet eller kortet och koderna på det sätt som beskrivs i bruksvillkoren.

6.4.3 Övriga omständigheter i anslutning till aktiveringsuppgiften

Innehavaren av ett tillfälligt certifikat informeras om möjligheten att byta den ursprungliga PIN-koden till en ny kod. Ett gratisprogram för byte av PIN-kod finns på www.fineid.fi.

Förfarandet beskrivs i detalj i certifieringspraxisen.

6.5 Säkerhetskrav i anslutning till användningen av och åtkomsten till datorer

6.5.1 Utrustningens säkerhet

För certifikatsystemet används bara ändamålsenlig utrustning.

Förfarandet beskrivs i detalj i certifieringspraxisen.

6.6 Hantering av certifikatsystemets livscykel

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

6.6.1 Övervakning av systemutvecklingen

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

6.6.2 Hantering av säkerheten

Myndigheten för digitalisering och befolkningsdatas informationssäkerhet hanteras i enlighet med Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy och standarden ISO/IEC 27001

6.7 Säkerheten i datanätet

Informationssäkerheten har garanterats så att datanätet för certifikatsystemet utgör en helhet som separerats från andra datanät och vars kritiska delar finns i dubbla uppsättning.

En närmare beskrivning av säkerheten i datanätet ingår i certifieringspraxisen.

6.8 Övervakningen av användningen av kryptiska moduler

Utfärdaren ser till att utfärdarens hemliga nycklar är skyddade så att de inte kan röjas eller missbrukas. För att tillgodose kraven på säkring av kritisk information tas en säkerhetskopia av utfärdarens hemliga nycklar.

Förfarandet beskrivs i detalj i certifieringspraxisen.

7 Certifikat- och spärrlistprofiler

7.1 Tekniska uppgifter på certifikat

Datainnehållet i rotcertifikatet, certifikatutfärdarens certifikat och certifikatinnehavarens certifikat beskrivs i dokumentet FINEID S2. Dokumentet finns på certifikatutfärdarens webbplats, www.fineid.fi.

7.2 Spärrlistprofil

Datainnehållet i de spärrlistor som utfärdaren publicerar beskrivs i dokumentet FIN-EID S2. Dokumentet finns på certifikatutfärdarens webbplats, www.fineid.fi.

8 Hantering av specifikationsdokument

8.1 Ändring av specifikationer

Certifikatutfärdaren kan ändra specifikationerna med anledning av kraven i lagstiftningen eller funktionella krav. Ändringar i specifikationerna ska föras in i certifikatpolicy- och certifieringspraxisdokumenten på det sätt som beskrivs i det följande.

8.2 Publicering och information

Certifikatutfärdaren publicerar en certifikatpolicy och en certifieringspraxis. Dessa fås på Myndigheten för digitalisering och befolkningsdatas webbplats och på www.fineid.fi.

Certifikatutfärdarens offentliga specifikationer för certifikatproduktionen finns också på nämnda webbplatser.

Avtal om certifikatleveranser som ingåtts med de informationstekniska leverantörerna liksom beskrivningar av produktionssystemen och specifikationer av produkterna är konfidentiella.

8.3 Förfarande för ändring och godkännande av certifikatpolicyn

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för tillfälliga certifikat. Dokumenten kan ändras genom Myndigheten för digitalisering och befolkningsdatas interna ändringsförfarande.

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

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

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

2. Sådana punkter som enligt Myndigheten för digitalisering och befolkningsdata inte har någon väsentlig betydelse för certifikatinnehavare och förlitande parter kan ändras så att ändringarna meddelas 14 dagar innan de träder i kraft.