MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Certifikatpolicy

Finlands chipförsedda resedokument och uppehållstillståndshandlingar för Signeringscertifikat

OID: 1.2.246.517.2.10.5

CERTIFIED SFS ORGANIZATION ISO 9001

kiwa ISO/IEC 27001

Innehållsförteckning

Definitioner och förkortningar

Definitioner

Signeringscertifikat: Certifikat vars motsvarande privata nyckel används för att digitalt signera den data som ska lagras i resedokumentet och uppehållstillståndshandlingens fjärravläsbara chip.

Den som ansöker om Signeringscertifikat: En juridisk person som ansöker om Signeringscertifikat och som identifieras på ett tillförlitligt sätt i samband med ansökan. En juridisk person är finska staten, som enligt passlagen representeras av Polisstyrelsen och enligt utlänningslagen av Migrationsverket.

Innehavare av Signeringscertifikat: En juridisk person vars identifieringsuppgifter och offentliga nyckel har certifierats med Certifikatutfärdarens elektroniska signatur och som innehar den privata nyckeln i anslutning till certifikatet. En juridisk person är finska staten, som enligt passlagen representeras av Polisstyrelsen och enligt utlänningslagen av Migrationsverket.

Nyckelpar: Nycklar som används tillsammans inom ett offentligt nyckelsystem, varav den ena är offentlig och den andra privat. Nycklarnas användningsändamål har fastställts i certifikatet (se certifikatinnehavarens Signeringscertifikat).

Digital signatur: Den elektroniska signaturen säkerställer äktheten och integriteten hos de signerade uppgifterna, dvs. att säkerställa uppgifternas ursprung och att de inte har ändrats efter att resedokumentet och uppehållstillståndshandlingen utarbetades.

ECC-algoritm och ECC-nyckel: ECC-algoritm är en allmänt använd algoritm för offentliga nycklar. De privata och offentliga nycklarna till Signeringscertifikatet är ECC-nycklar.

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

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

Offentligt nyckelsystem: Dataskyddsinfrastruktur där dataskyddstjänster produceras med ett offentligt nyckelsystem.

Offentligt nyckelsystem: Dataskyddstjänst, exempelvis elektronisk identifiering av personer, som produceras genom att använda offentliga och privata nycklar, certifikat och icke-symmetrisk kryptering.

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.

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-algoritm är en allmänt använd algoritm för en offentlig nyckel. De privata och offentliga nycklarna till Signeringscertifikatet 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.

Finlands chipförsedda resedokument: Det allmänna resedokumentet som polisen beviljat, där den tekniska delen har ett Signeringscertifikat för att säkerställa äktheten och integriteten av datainnehållet som lagras på chipet.

Finlands chipförsedda uppehållstillståndshandling: Polisens eller Migrationsverkets beviljade uppehållstillståndshandling, där den tekniska delen har ett Signeringscertifikat för att säkerställa äktheten och integriteten av datainnehållet som lagras på chipet.

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 informationstekniskt system för att skapa certifikat och underteckna spärrlistor.

Certifikatbeskrivning: Ett dokument som 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. De certifikatpolicyer som Myndigheten för digitalisering och befolkningsdata publicerar är offentligt tillgängliga. Varje policy identifieras av en egen kod.

Certifikatregister: Ett register som är förenligt med lagen om stark autentisering och betrodda elektroniska tjänster som en Certifikatutfärdare som tillhandahåller allmänheten godkända certifikat är skyldig att föra. Uppgifterna ska bevaras i minst 10 år efter att certifikatets giltighetstid har gått ut.

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. Med Certifikatutfärdare avses Myndigheten för digitalisering och befolkningsdata.

Certifikatutfärdarens certifikat: Certifikat som Certifikatutfärdaren själv beviljat och som innehåller en offentlig nyckel som motsvarar utfärdarens privata nyckel och med vars hjälp äktheten hos elektroniska signaturer som utfärdats av utfärdaren kontrolleras. Certifikatutfärdarens certifikat innehåller bl.a. utfärdarens namn, placeringsland och offentliga nyckel.

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

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

Objektidentifierare (OID): Kod som identifierar bl.a. den organisation som utfärdat certifikatet och certifieringspraxisen enligt vilken certifikatet beviljats. OID-koden ingår i certifikatets datainnehåll.

Privat nyckel: Den privata delen av nyckelparet som används för icke-symmetrisk kryptering i ett offentligt nyckelsystem. Den privata signeringsnyckeln har sparats i det datasystem som certifikatinnehavaren administrerar.

Förkortningar

CA	Certification Authority, Certifikatutfärdare
CP	Certificate Policy, certifikatpolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
MDB	Myndigheten för digitalisering och befolkningsdata
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, säkerhetsmodul
HST	Elektronisk identifiering av person
HTTP	Hypertext Transfer Protocol
ICAO	Intenational Civil Aviation Organization
ICAO PKD	ICAO Public Key Directory
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
PKI	Public Key Infrastructure, system med offentlig nyckel
RSA	Rivest, Shamir, Adleman, en algoritm för offentlig nyckel, asymmetrisk algoritm

1.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 certifikatpolicy tillämpas på Signeringscertifikat för chipförsedda resedokument och uppehållstillståndshandlingar (nedan Signeringscertifikat) som beviljats av Myndigheten för digitalisering och befolkningsdata och som beviljas de myndigheter som anges i passlagen (671/2006) och utlänningslagen (301/2004).

1.1.Allmänt

Ett certifikat är ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar certifikatinnehavarens identitet. Ett Signeringscertifikat som är förenligt med denna certifikatpolicy grundar sig på systemet och metoderna med offentlig nyckel. Uppgifterna i Certifikatutfärdarens certifikat och Signeringscertifikat har undertecknats elektroniskt med Certifikatutfärdarens privata nyckel. I certifieringspraxisen definieras innehållet i Signeringscertifikat enligt denna certifikatpolicy. Certifieringspraxisen är hemlig, men en offentlig sammanfattning av den publiceras.

Syftet med Signeringscertifikatet för chipförsedda resedokument och uppehållstillståndshandlingar är att verifiera den digitala signaturen på resedokumentet och uppehållstillståndshandlingens chip. Den digitala signaturen säkerställer äktheten och integriteten hos de signerade uppgifterna, dvs. att säkerställa uppgifternas ursprung och att de inte har ändrats efter att resedokumentet och uppehållstillståndshandlingen utarbetades. Med Certifikatutfärdarens certifikat kontrolleras äktheten hos Signeringscertifikaten. Myndigheten för digitalisering och befolkningsdata garanterar att certifikatuppgifterna är korrekta.

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

I utfärdarens funktioner ingår produktion av certifikat-, register- och spärrtjänster samt registrering. 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.

1.2.Identifikationsuppgifter

Denna certifikatpolicy heter Certifikatpolicy för Signeringscertifikat för finska chipförsedda resedokument och uppehållstillståndshandlingar, vars OID är 1.2.246.517.2.10.5.

Certifikatpolicyn och den offentliga sammanfattningen av certifieringspraxisen finns på adressen http://www.dvv.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 innehavaren av Signeringscertifikatet enligt Certifikatut-

färdarens ansvar som beskrivs i kapitel 2.2.1. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de tekniska leverantörer som utfärdaren anlitar.

Denna certifikatpolicy har registrerats av Myndigheten för digitalisering och befolkningsdata. Det är en myndighet som upprätthåller ett personregister vars uppdrag enligt passlagen och utlänningslagen är att producera certifikattjänster för finska chipförsedda resedokument och uppehållstillståndshandlingar.

1.3.1.Certifikatutfärdare

Certifikatutfärdarens uppgifter är att

- erbjuda sådana certifikat-, katalog-, spärr- och registreringstjänster enligt certifikatpolicyn och certifieringspraxisen som avses i passlagen och utlänningslagen
- identifiera den som ansöker om Signeringscertifikat
- se till att datainnehållet i certifikaten är felfria
- sörja för spärrning av certifikat och publicering av spärrlistor
- iaktta en god dataskyddsnivå vid behandlingen av uppgifter om certifikatinnehavaren samt en god informationsbehandlingssed.

1.3.2.Registreraren

Registreringen av Signeringscertifikatet sker enligt förfarandet i kapitel 3. En närmare beskrivning av förfarandet ges i certifieringspraxisen.

- Registreraren handlar på uppdrag och ansvar av Certifikatutfärdaren.
- Registreraren följer Certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Registreraren identifierar Den som ansöker om Signeringscertifikat enligt certifieringspraxisen. Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med Certifikatutfärdaren.

1.3.3.Spärrtjänst

Spärrtjänsten för certifikat spärrar de Signeringscertifikat som Innehavaren av Signeringscertifikatet vill spärra innan deras giltighetstid går ut. Spärrade Signeringscertifikat förs in på spärrlistan.

1.3.4.Registertjänst

Registertjänsten är en offentlig Webbtjänst med ett register där alla beviljade certifikat av Utfärdaren, Signeringscertifikat och spärrlistor finns tillgängliga. Registertjänsten finns på ldap://ldap.fineid.fi. CSCA-certifikat, spärrlistor, Ds-certifikat för pass, DS-certifikat för identitetskort och DS-certifikat för uppehållstillstånd publiceras i registertjänsten.

1.3.5.ICAO PKD

ICAO:s register över offentlig nyckel (ICAO PKD) är ett centraliserat datalager som används för att dela information som behövs för att verifiera elektroniska maskinläsbara resedokument (eMRTD), såsom pass, identitetskort och signerade streckkoder (Visible Digital Seals). CSCA-certifikat, spärrlistor och dokumentcertifikat publiceras i ICAO PKD-registertjänsten.

1.3.6.Innehavare av Signeringscertifikat

Finska staten, som Polisstyrelsen och Migrationsverket företräder, beviljas Signeringscertifikat i enlighet med denna certifikatpolicy.

Innehavaren av Signeringscertifikatet 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 att granska elektroniska signaturer.

En förlitande part ska kontrollera att det certifikat som används är i kraft, att certifikatet inte finns på spärrlistan och att certifikatkedjan är enhetlig.

1.3.8.Användning av certifikat

Myndigheten för digitalisering och befolkningsdata följer denna certifikatpolicy när den utfärdar Signeringscertifikat. Innehavare av Certifikatutfärdarens certifikat och Signeringscertifikat samt förlitande parter ska handla i enlighet med denna certifikatpolicy.

Ett Signeringscertifikat enligt denna certifikatpolicy används för att kontrollera elektroniska signaturer.

Certifikatpolicyn och certifieringspraxisen innehåller krav som gäller skyldigheterna för Utfärdaren, registreraren, Innehavarens av Signeringscertifikatet 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 har registrerats av Myndigheten för digitalisering och befolkningsdata. Det är en myndighet som underhåller ett personregister, vars uppgift enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifieringstjänster (661/2009) är att, förutom sina andra uppgifter, producera certifierade tjänster för elektronisk kommunikation samt certifikat enligt passlagen och utlänningslagen för Finlands chipförsedda resedokument och uppehållstillståndshandlingar. Myndigheten för digitalisering och befolkningsdata svarar för administrationen av denna certifikatpolicy och för uppdateringar i den.

1.4.2.Kontaktuppgifter

Förfrågningar om certifikatpolicyn kan riktas till följande adress:

Myndigheten för digitalisering och befolkningsdata	kirjaamo@dvv.fi
PB 00531 (Fågelviksgränden 2)	Tfn +358 295 536 000
00581 Helsingfors	Fax +358 295 535 555
FO-nummer: 0245437–2	

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

2.Allmänna villkor

Denna certifikatpolicy trädde i kraft den 27 maj 2011 (version 1.0). Förfaringssättet för att göra ändringar i och publicera certifikatpolicyn beskrivs i punkt 8 i detta dokument. I punkt 8 ingår också versionshantering, av vilken framgår de ändringar som gjorts i certifikatpolicyn efter den 27 maj 2011.

2.1.Skyldigheter

2.1.1.Certifikatutfärdarens skyldigheter

- Myndigheten för digitalisering och befolkningsdata har en lagstadgad uppgift att fungera som Certifikatutfärdare.
- Utfärdaren iakttar i sin verksamhet gällande lagstiftning.
- Certifikatutfärdaren 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 ansvarar för alla delområden av certifikatverksamheten, även för tillförlitligheten och funktionaliteten hos de tekniska leverantörer eller personer som Certifikatutfärdaren anlitar, såsom de tjänster och produkter som registrerarna producerar.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy som beskriver de förfaringssätt, användarvillkor, ansvarsfördelning och andra synpunkter på hur Signeringscertifikatet används på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur Utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren iakttar certifikatpolicyn och certifieringspraxisen.
- Utfärdaren publicerar en sammanfattning av 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 obehörig användning.

2.1.2.Registrerarens skyldigheter

- Registreraren efterlever certifikatpolicyn och certifieringspraxisen i samband med registreringen.
- Registreraren identifierar företrädaren för sökanden av Signeringscertifikatet personligen och tillförlitligt på det sätt som beskrivs i certifieringspraxisen så att sökandens identifieringsuppgifter och andra uppgifter som behövs för utfärdandet av certifikatet kontrolleras noggrant.
- Registreraren ser till att registreringsuppgifterna behandlas omsorgsfullt och konfidentiellt.
- Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med Certifikatutfärdaren.

2.1.3.Skyldigheter för innehavare av Signeringscertifikat

- Användningsändamålet och villkoren för Signeringscertifikatet har fastställts i denna certifikatpolicy och certifieringspraxis. Ett Signeringscertifikat får användas endast i enlighet med dess användningsändamål och -villkor.
- Innehavaren av Signeringscertifikatet ansvarar för att de uppgifter som anmälts vid ansökan om certifikatet är korrekta.
- Innehavaren av Signeringscertifikatet ansvarar för användningen av certifikatet.
- Innehavaren av Signeringscertifikatet ansvarar för att förhindra att den privata nyckel som tillhör denne används på ett sätt som strider mot användningsändamålet genom att sörja för detta på det sätt som nämns i detta dokument och i certifieringspraxisen.
- En privat nyckel som motsvarar Signeringscertifikatet ska utan dröjsmål anmälas till Certifikatutfärdaren på det sätt som beskrivs i kapitel 4.4.

2.1.4.Den förlitande partens skyldigheter

Förlitande parter ska iaktta certifikatpolicyn och certifieringspraxisen.

Förlitande parter kan i god tro lita på certifikat när de har kontrollerat att certifikatet är i kraft, att det inte finns på spärrlistan och att certifikatkedjan är enhetlig. Förlitande parter är skyldiga att kontrollera certifikaten mot spärrlistan. För att säkerställa att certifikatet är i kraft ska den förlitande parten iaktta de kontrollåtgärder på spärrlistan som presenteras nedan.

En förlitande part som kopierar en spärrlista från registret, ska försäkra sig om spärrlistans äkthet genom att kontrollera den elektroniska signaturen för Den som har signerat spärrlistan. Dessutom ska förlitande parter kontrollera spärrlistans giltighetstid.

Om det på grund av funktionsstörningar i utrustningen eller registertjänsten inte är möjligt att få tillgång till den senaste spärrlistan från registret, bör certifikatet inte godkännas, i fall giltighetstiden för den senast erhållna spärrlistan har gått ut. Alla godkännanden av Signeringscertifikat efter att denna giltighetstid gått ut sker på den förlitande partens egen risk.

2.1.5.Skyldigheter vid publicering av Signeringscertifikat

Signeringscertifikaten publiceras i ett allmänt tillgängligt offentligt register och de spärrade Signeringscertifikaten publiceras på en spärrlista, där den förlitande parten ska kontrollera certifikatets giltighet.

2.2.Ansvar

2.2.1.Certifikatutfärdarens ansvar

Myndigheten för digitalisering och befolkningsdata ansvarar som Certifikatutfärdare för säkerheten i hela certifikatsystemet. Utfärdaren svarar för införskaffade tjänster på samma sätt som om utfärdaren själv hade producerat tjänsten. Skadeståndsansvaret för Myndigheten för digitalisering och befolkningsdata, Polisstyrelsen och Migrationsverket har avtalats genom avtal mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket.

Myndigheten för digitalisering och befolkningsdata svarar för att Signeringscertifikatet har skapats enligt de förfaranden som beskrivs i certifikatpolicyn och certifieringspraxisen och utgående från de uppgifter som den som ansöker om Signeringscertifikat lämnat. Befolkningsregistercentralen svarar för de uppgifter som den har lagrat på Signeringscertifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar för att Signeringscertifikatet, när det används på behörigt sätt, kan användas från överlåtelsetidpunkten under hela dess giltighetstid, om det inte finns upptaget på spärrlistan. Ett Signeringscertifikat har överlåtits till en person som har identifierats på det sätt som beskrivs i certifieringspraxisen.

Genom att underteckna Signeringscertifikatet med sin privata nyckel försäkrar Certifikatutfärdaren att uppgifterna i Signeringscertifikatet har kontrollerats i enlighet med certifikatpolicyn och certifieringspraxisen.

Certifikatutfärdaren ansvarar för att rätt Signeringscertifikat förs in på spärrlistan och att det dyker upp på spärrlistan inom den tidsfrist som anges i denna certifikatpolicy.

2.2.2.Registrerarens ansvar

Myndigheten för digitalisering och befolkningsdata registrerar Signeringscertifikatet. I fråga om registreringen iakttas de förfaringssätt och ansvar som beskrivs i denna certifikatpolicy och i certifieringspraxisen i anslutning till den.

2.2.3.Ansvar för innehavare av Signeringscertifikat

Innehavaren av ett Signeringscertifikat ansvarar för de ekonomiska och juridiska följderna av sitt agerande.

Ansvaret för användningen av Signeringscertifikatet upphör när innehavaren har meddelat spärrtjänsten de uppgifter som behövs för att spärra Signeringscertifikatet och efter att ha fått notifikationen om spärrningen av den som tagit emot begäran. För att ansvaret ska upphöra måste begäran om spärrning göras omedelbart när det har konstaterats att skäl för anmälan upptäckts.

2.2.4.Ansvaret för förlitande parter i Signeringscertifikat

Den förlitande parten kan inte lita på Signeringscertifikatet i god tro om giltighetstiden för Signeringscertifikatet inte har kontrollerats från spärrlistan och om certifikatkedjans integritet inte har kontrollerats. Godkännandet av Signeringscertifikatet i nämnda fall befriar Myndigheten för digitalisering och befolkningsdata och innehavaren av Signeringscertifikatet från ansvaret. Den förlitande parten ska kontrollera att det beviljade Signeringscertifikatet har använts i enlighet med dess användningsändamål.

2.2.5.Begränsning av ansvar

Skadeståndsansvaret för Myndigheten för digitalisering och befolkningsdata, Polisstyrelsen och Migrationsverket har avtalats genom avtal mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket. I övriga situationer har Myndigheten för digitalisering och befolkningsdatas, Polisstyrelsens och Migrationsverkets ansvar begränsats till påvisade direkta skador. Som direkta skador ersätts dock högst 10 000 euro för varje skadefall eller skadefall som har samband med varandra.

Myndigheten för digitalisering och befolkningsdata ansvarar inte för skador som orsakas av att den privata nyckeln till innehavaren av Signeringscertifikatet röjs, om inte avslöjandet beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdata ansvarar inte för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till innehavaren av Signeringscertifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar inte för att de allmänna dataförbindelserna eller datanäten fungerar eller för att Signeringscertifikatet inte kan användas på grund av att utrustningen eller programvaran som används av innehavaren av Signeringscertifikatet eller den förlitande parten inte fungerar eller för att Signeringscertifikatet används i strid med dess avsedda användningsändamål.

Certifikatutfärdaren har rätt att avbryta tjänsten för den tid ändringar eller underhåll av systemet utförs. Om avbrottet har betydelse för den som ansöker om Signeringscertifikat ska detta avtalas gemensamt med Polisstyrelsen och Migrationsverket. Om ändringar eller underhåll av spärrlistan meddelas på förhand.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Den förlitande parten ska därför stå för sina egna kostnader och Certifikatutfärdaren är inte skyldig att ersätta den förlitande parten för kostnaderna för utveckling av certifikattjänsten. Certifikatutfärdaren, Polisstyrelsen och Migrationsverket kommer separat överens om utvecklingsåtgärder och -kostnader.

Certifikatutfärdaren ansvarar inte för åtgärder, fel eller kostnader till följd av Signeringscertifikatet.

2.3.Ekonomiskt ansvar

2.3.1.Certifikatutfärdare

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av de certifikattjänster som beskrivs i denna certifikatpolicy bestäms enligt den överenskommelse som tillämpas vid respektive tidpunkt och i tillämpliga delar enligt bestämmelserna i skadeståndslagen (412/1974).

Skadeståndsansvaret för Myndigheten för digitalisering och befolkningsdatas, Polisstyrelsens och Migrationsverket har avtalats genom avtal mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket. I andra situationer har Myndigheten för digitalisering och befolkningsdatas, Polisstyrelsens och Migrationsverkets ansvar begränsats till påvisade direkta skador. Som direkta skador ersätts dock högst 10 000 euro för varje skadefall eller skadefall som har samband med varandra.

2.3.2.Övriga parter

Förlitande parter kan lita på Signeringscertifikat om de har kontrollerat att de inte har införts på spärrlistan och att deras giltighetstid inte har löpt ut, certifikatkedjan är sammanhängande och de inte har andra skäl att betvivla att de används korrekt.

Den förlitande parten ansvarar för utnyttjandet av Signeringscertifikatet och rättshandlingarna i anslutning till utnyttjandet av det samt för de ekonomiska och juridiska påföljderna i anslutning till dem.

2.3.3.Certifikatutfärdarens ekonomiförvaltning

De certifikattjänster som Myndigheten för digitalisering och befolkningsdata producerar omfattas av det ekonomiförvaltningssystem och den tillsyn som separat har fastställts.

2.4.Tolkning och verkställighet

2.4.1.Tillämplig lagstiftning och myndighetsrekommendationer

Ett Signeringscertifikat som utfärdats i enlighet med denna certifikatpolicy uppfyller kraven i passlagen och utlänningslagen samt följer Internationella civila luftfartsorganisationens (ICAO) rekommendationer med några undantag som beror på ärendets natur. Undantagen beskrivs i detalj i sammanfattningen av Certifieringspraxisen.

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av de certifikattjänster som beskrivs i denna certifikatpolicy bestäms enligt den överenskommelse som tillämpas vid respektive tidpunkt och i tillämpliga delar enligt bestämmelserna i skadeståndslagen.

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

Myndigheten för digitalisering och befolkningsdata svarar för att Signeringscertifikatet har skapats enligt de förfaranden som beskrivs i certifikatpolicyn och certifieringspraxisen och utgående från de uppgifter som den som ansöker om Signeringscertifikat lämnat.

2.4.2.Avgörande av meningsskiljaktigheter

Myndigheten för digitalisering och befolkningsdata ansvarar vid utfärdandet av certifikat för att Signeringscertifikatet uppfyller kraven i denna certifikatpolicy. Eventuella meningsskiljaktigheter löses enligt rättssystemet i Finland.

2.5.Avgifter

I detta avsnitt definieras betalningar i anslutning till Signeringscertifikat.

2.5.1.Utfärdande och förnyande av Signeringscertifikat

Ansökan om Signeringscertifikat görs enligt beskrivningen i certifieringspraxisen.

Signeringscertifikaten har prissatts enligt överenskommelserna mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket.

2.5.2.Avgifter i anslutning till användning av Signeringscertifikat

Certifikatutfärdaren debiterar innehavaren av ett Signeringscertifikat för användningen av Signeringscertifikatet, spärrtjänsten eller det offentliga registret i enlighet med överenskommelserna mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket.

2.5.3.Avgifter i anslutning till anteckning om spärrlista för Signeringscertifikat

För anmälan av ett Signeringscertifikat till spärrlistan, hämtning av spärrlistor från registret samt kontroll av ett Signeringscertifikats giltighet från spärrlistan debiteras av Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt av Myndigheten för digitalisering och befolkningsdata och Migrationsverket i enlighet med överenskommelserna mellan dem.

2.6.Publicering av och tillgång till Certifikatutfärdarens uppgifter

2.6.1.Publicering av Certifikatutfärdarens uppgifter

Certifikatutfärdaren publicerar alla för offentliggörande avsedda certifikat, Signeringscertifikat och spärrlistor i en allmänt tillgänglig offentligt register. Certifikatutfärdaren publicerar en sammanfattning av certifikatpolicyn och certifieringspraxisen.

2.6.2.Publikationsfrekvens

Ett Signeringscertifikat publiceras i det offentliga registret genast efter att det har skapats och det finns i registret under hela dess giltighetstid. Certifikatutfärdaren publicerar en spärrlista som är i kraft i 40 dygn efter publiceringen. Denna spärrlista uppdateras med 30 dygns mellanrum med en ny spärrlista.

2.6.3.Tillgång till information

Uppgifterna om registret och spärrlistan är allmänt tillgängliga på adressen ldap://ldap.fineid.fi. En närmare beskrivning av registertjänsten finns i sammanfattningen av certifieringspraxisen. Spärrlistan finns också tillgänglig på den e-postadress som anges i Signeringscertifikatet. En sammanfattningen av certifikatpolicyerna och certifieringspraxisen finns också på Certifikatutfärdarens webbplats.

2.6.4.Datalager

De konfidentiella uppgifterna i certifikatsystemet är sparade i Certifikatutfärdarens egna, konfidentiella datalager. Certifikatutfärdarens uppgifter arkiveras i enlighet med gällande arkivbestämmelser.

2.7.Dataskyddsgranskning

Polisstyrelsen, inrikesministeriets polisavdelning och Migrationsverket kan granska Certifikatutfärdarens verksamhet i enlighet med avtalen mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket.

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

2.7.1.Granskningsfrekvens

Myndigheten för digitalisering och befolkningsdata granskar årligen sina tekniska leverantörers verksamhet eller vid behov.

2.7.2.Inspektör

Datasäkerhetschefen hos Myndigheten för digitalisering och befolkningsdata eller en utomstående inspektör som är specialiserad på auditering av tekniska leverantörer i anslutning till certifikattjänster utför dataskyddsgranskningen.

2.7.3.Föremål för granskningen och granskningens omfattning

Föremålen för granskningen bestäms enligt datasäkerhetsstandarden ISO/IEC 27001, Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy eller enligt tekniska leveransavtal.

Egenskaper som granskas är konfidentialitet, integritet och tillgänglighet.

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.

2.7.4.Åtgärder vid avvikelser

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

2.7.5.Information om resultatet av granskningen

Information om resultatet av granskningen ges ut i enlighet med lagen, i datasäkerhetsstandarden ISO/IEC 27001, Myndigheten för digitalisering och befolkningsdatas datasäkerhetspolicy och enligt gällande leveransavtal. Det detaljerade och standardiserade granskningsresultatet avsett för intern användning är konfidentiellt och offentliggörs inte. Rapporter med på förhand bestämd utformning utarbetas separat för användning utanför organisationen.

Myndigheten för digitalisering och befolkningsdata informerar Polisstyrelsen, inrikesministeriet och Migrationsverket om resultaten av inspektionen.

2.8.Uppgifternas offentlighet

2.8.1.Uppgifter som publiceras av Certifikatutfärdaren

Uppgifterna i certifikatsystemet är konfidentiella om de inte grundar sig på bestämmelserna om utlämnande av uppgifter i dataskyddslagen (1050/2018), lagen om offentlighet i myndigheternas verksamhet (621/1999) eller på de ändamål som fastställts i certifikatpolicyn eller certifieringspraxisen.

2.8.2.Offentlig information

Uppgifterna i det offentliga registret och spärrlistan är offentliga, likaså sammanfattningen av certifieringspraxisen och de uppgifter som fastställts i certifikatpolicyn.

2.8.3.Information om upphörande eller spärrning av Signeringscertifikat

Giltighetstiden för Signeringscertifikatet har antecknats på Signeringscertifikatet. Signeringscertifikat som spärrats under giltighetstiden publiceras på en allmänt tillgänglig spärrlista.

2.8.4.Information som lämnas ut till myndigheter

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

2.8.5.Övriga uppgifter

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

2.8.6.Utlämnande av uppgifter på begäran av innehavaren av Signeringscertifikatet

Innehavaren av Signeringscertifikatet har rätt att få uppgifter om sig själv i enlighet med gällande lagstiftning och överenskommelser mellan Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen samt mellan Myndigheten för digitalisering och befolkningsdata och Migrationsverket.

Övriga principer för utlämnande av uppgifter

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 följer av myndigheternas rätt att få uppgifter ur certifikatsystemet.

Myndigheten för digitalisering och befolkningsdata följer dataskyddslagen och speciallagstiftningen vid behandlingen av personuppgifter. 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 uppgifterna om Signeringscertifikat och dokumentation i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata har full ägande- och användarrätt till denna certifikatpolicy.

3.Identifiering av den som ansöker om Signeringscertifikat

3.1.Registrering

I kapitlen 4.1–4.3 presenteras den praxis och de verksamhetsprocesser som iakttas vid identifiering och verifiering av dem som ansöker om Signeringscertifikat.

Rättigheterna och skyldigheterna för den som ansöker om Signeringscertifikat nämns i ansökningshandlingen, som utgör uppdraget för sökanden att ansöka om certifikat.

3.1.1.Benämningspraxis

Certifikatutfärdaren av Signeringscertifikat för chipförsedda resedokument är:

CN (Common name) = CSCA Finland

OU (Organizational unit) = VRK

O (Organization) = Finland

C (Country) = FI

I certifieringspraxisen beskrivs benämningspraxisen i detalj för innehavaren av Signeringscertifikatet. Uppgifterna på Signeringscertifikatet fastställer entydigt innehavaren av certifikatet.

3.2.Förnyelse av nyckelpar

Den offentliga nyckeln till Signeringscertifikatet kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt Signeringscertifikat.

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

3.3.Förnyelse av nyckelpar efter att ett Signeringscertifikatet införts på spärrlistan

Den offentliga nyckeln till Signeringscertifikatet och motsvarande privata nyckel kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt Signeringscertifikat.

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

4.Funktionella krav

4.1.Ansökan om Signeringscertifikat

Rättigheterna och skyldigheterna för den som ansöker om Signeringscertifikat nämns i ansökningshandlingen, som utgör kontraktet för den som ansöker om Signeringscertifikat. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter. I ansökningshandlingen nämns tydligt att den som ansöker om Signeringscertifikat med sin underskrift bekräftar att uppgifterna är riktiga samt godkänner att stämpelcertifikatet skapas och publiceras i det offentliga registret.

Den som ansöker om Signeringscertifikat ansvarar för att alla uppgifter som är väsentliga för Signeringscertifikatet och som sökanden har lämnat till Certifikatutfärdaren är riktiga. Innehavaren av Signeringscertifikatet ska använda Signeringscertifikatet endast i enlighet med dess användningsändamål.

4.2.Utfärdande av Signeringscertifikat

Certifikatutfärdaren utfärdar Signeringscertifikatet i och med godkännandet av certifikatansökan.

Utfärdaren ansvarar vid utfärdandet av Signeringscertifikatet för att dess innehåll överensstämmer med den godkända ansökan.

4.3.Leverans av Signeringscertifikat till den som ansöker om Signeringscertifikat

Ett Signeringscertifikat hämtas personligen från registreringsstället eller skickas elektroniskt undertecknat per e-post till den som ansöker om Signeringscertifikat.

4.4.Spärrning av Signeringscertifikat

4.4.1.Förutsättningar för spärrning av Signeringscertifikat

Ett Signeringscertifikat ska sättas upp på spärrlistan när det finns skäl att misstänka missbruk till exempel på grund av att den privata nyckeln har röjts. Begäran om spärrning ska göras medelbart om man misstänker att det blivit möjligt att missbruka kortet.

4.4.2.Den som begär spärrning och identifiering

Begäran om spärrning av Signeringscertifikat görs av utsedda företrädare för en organisation som innehar Signeringscertifikatet.

Grunderna för spärrningen av Signeringscertifikatet, tidpunkten och uppgifterna om utföraren registreras.

Innehavaren av Signeringscertifikatet kan om denne så önskar få Signeringscertifikatet spärrat innan dess giltighetstid går ut.

Alla begäranden om spärrning, grunderna för spärrningen, sättet att identifiera den som gjorde begäran om spärrning och Certifikatutfärdarens åtgärder med anledning av begäran arkiveras.

Spärrningen av Signeringscertifikatet beskrivs i detalj i certifieringspraxisen.

4.4.3.Spärrhändelse

Ett Signeringscertifikat spärras inom tre vardagsdygn efter att begäran om spärrning mottagits.

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

Spärrtjänsten meddelar den som begärt spärrning av ett Signeringscertifikat om spärrning av Signeringscertifikatet.

Spärrning av Signeringscertifikat på begäran av Myndigheten för digitalisering och befolkningsdata

Myndigheten för digitalisering och befolkningsdata spärrar de Signeringscertifikat som den beviljat om ett fel upptäcks i deras datainnehåll och innehavaren av Signeringscertifikatet godkänner spärrningen.

I enlighet med det ovan nämnda kan Myndigheten för digitalisering och befolkningsdata spärra certifikat som undertecknats med den privata nyckel som myndigheten använder, om det finns skäl att misstänka att Myndigheten för digitalisering och befolkningsdatas privata nyckel har röjts eller hamnat i fel händer.

Samtliga giltiga Signeringscertifikat som utfärdats med den röjda nyckeln ska spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.

Om den privata nyckel eller annan teknisk metod som Myndigheten för digitalisering och befolkningsdata använder vid skapandet av certifikat har röjts eller på annat sätt blivit oanvändbar, ska Myndigheten för digitalisering och befolkningsdata underrätta innehavaren av Signeringscertifikatet om händelsen på behörigt sätt.

4.4.4.Publiceringsfrekvens för spärrlista

Information om att certifikatet har förts in på spärrlistan är offentligt tillgänglig senast tre vardagsdygn efter att begäran om spärrning har konstaterats vara giltig och godkänd. Spärrlistan gäller i 40 dygn efter publiceringen. Denna spärrlista uppdateras med 30 dygns mellanrum med en ny spärrlista. Den nya spärrlistan publiceras senast när den gällande spärrlistan upphör att gälla.

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

4.4.5.Krav i anslutning till kontroll av spärrlistor

Den förlitande partens skyldigheter beskrivs i avsnitt 2.1.4

4.4.6.Kontroll av ett certifikats status i realtid

Certifikatutfärdaren tillhandahåller tillsvidare ingen tjänst för kontroll av certifikatens status i realtid, dvs. en OCSP-tjänst.

4.4.7.Krav i anslutning till kontroll av ett certifikats status i realtid

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

4.5.Övervakningen av systemet

Övervakningen av systemet beskrivs i certifieringspraxisen.

4.6.Arkivering av uppgifter i anslutning till Signeringscertifikat

4.6.1.Material som arkiveras

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten att få uppgifter bestäms enligt lagen om offentlighet i myndigheternas verksamhet. Uppgifterna i certifikatregistret ska förvaras i 10 år från tidpunkten då certifikaten upphört att gälla.

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

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

4.6.2.Skydd av arkiv

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

4.6.3.Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

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.Hantering av verksamhetens kontinuitet och behandling av undantagsfall

Myndigheten för digitalisering och befolkningsdata har en kontinuitets- och beredskapsplan som möjliggör kontinuiteten i Myndigheten för digitalisering och befolkningsdatas verksamhet.

Beredskap för undantagssituationer är beskriven i certifieringspraxisen.

4.7.1. Certifikatutfärdarens privata nyckel har röjts eller Certifikatutfärdarens certifikat har spärrats

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

4.7.2. 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 informationssäkerhetscertifikatet ISO 27001, som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även vid en eventuell katastrof.

4.8. Avslutande 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 certifieringspraxisen så snart som möjligt, dock minst en månad före tidpunkten för nedläggningen.

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

a) 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.

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

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

d) Utfärdaren sörjer för arkiveringen av uppgifterna samt följer även i övrigt arkivlagens bestämmelser om arkivering av uppgifter.

5. Fysiska krav, funktionella krav och krav på personalens säkerhet

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

5.1. Arrangemang i anslutning till den fysiska säkerheten

Myndigheten för digitalisering och befolkningsdata har beviljats ett datasäkerhetscertifikat som garanterar att informationssäkerheten vid Myndigheten för digitalisering och befolkningsdata uppfyller kraven i standarden ISO/IEC 27001. Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. Myndigheten för digitalisering och befolkningsdata 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 lokalernas egenskaper

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

Säkerheten i lokalerna garanteras i och med att obehöriga inte har tillträde till dem.

5.1.2.Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässiga 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.

5.1.3 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.

5.2.Funktionella krav

5.2.1.Ansvarsfördelning

Myndigheten för digitalisering och befolkningsdata använder tekniska leverantörer för datatekniska uppgifter inom certifikatproduktionen. Myndigheten för digitalisering och befolkningsdata fungerar som Certifikatutfärdare och svarar för certifikatverksamheten.

5.2.2.Antal personer som krävs för olika uppgifter

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

Det är möjligt att återkalla Certifikatutfärdarens privata nyckel bara om två behöriga personer övervakar åtgärden.

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 av Signeringscertifikat och identifiering av sökande kräver att en person är närvarande.

5.2.3.Uppgiftsspecifik identifiering

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

5.3.Personsäkerhet

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

Myndigheten för digitalisering och befolkningsdatas 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 befolkningsdatas utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar i de tekniska leverantörernas certifikatmiljö.

5.3.2.Förfarande vid utförande av bakgrundskontroll

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

Förfarandet för säkerhetsutredningen beskrivs detaljerat i certifieringspraxisen.

5.3.3.Krav på utbildning

Personalen hos 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 som genomförs av myndighetens förvaltningsenhet.

5.3.4.Underhåll av expertis och kompetens

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

5.3.5.Krav på uppgiftsrotation

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

Även inom arbetsrotationen efterlevs Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och dataskyddsplan samt 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 myndighetens interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

5.3.7.Personal som representerar organisationen

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

5.3.8.Handlingar som tillhandahålls personalen

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

6.Tekniska säkerhetsarrangemang

De tekniska säkerhetsarrangemangen beskrivs i detalj i certifieringspraxisen.

6.1.Skapa och lagra nyckelpar

6.1.1.Skapa nyckelpar

Certifikatutfärdaren skapar sin privata signeringsnyckel och en offentlig nyckel som motsvarar den privata signeringsnyckeln. Utfärdarens privata nycklar förvaras i kryptografiska moduler.

Certifikatinnehavarens nyckelpar skapas i lokaler som Polisstyrelsen och Migrationsverket gemensamt administrerar. Nyckelparet förvaras i en kryptografisk modul enligt FIPS 140-2 klass 3. Den privata nyckeln har inställts i ett läge med läs- och skrivskydd.

6.1.2.Överlåtelse av privat nyckel till den som ansöker om Signeringscertifikat

Innehavaren av Signeringscertifikatet skapar och förvarar sin privata nyckel i en kryptografisk modul.

6.1.3.Leverans av den offentliga nyckeln av innehavaren av Signeringscertifikatet till Certifikatutfärdaren

Den som ansöker om Signeringscertifikat skickar till registreraren en certifikatbegäran där uppgifterna om den som ansöker om Signeringscertifikat kopplas till den offentliga nyckeln i fråga. Signeringscertifikatet skapas utifrån en certifikatbegäran.

Signeringscertifikatet innehåller innehavarens offentliga nyckel för Signeringscertifikatet.

6.1.4.Distribution av Certifikatutfärdarens offentliga nyckel till innehavaren av Signeringscertifikatet

Certifikatutfärdarens certifikat innehåller utfärdarens offentliga nyckel. Certifikatutfärdarens certifikat registreras i det offentliga registret.

6.1.5.Längden på nycklar

Certifikatutfärdarens privata nyckel som används för att signera Signeringscertifikat samt den motsvarande offentliga nyckeln är minst 512-bitars ECC-nycklar.

Certifikatinnehavarens privata och offentliga nycklar är 512-bitars ECC-nycklar.

6.1.6.Nycklarnas användningsändamål

Fältet som fastställer användningsändamålet i certifikatets datainnehåll anger användningsändamålet för den nyckel som är kopplad till certifikatet (till exempel digital signatur). Användningen av nyckeln begränsas bara till användningsändamålet: en nyckel som är avsedd för digital signering ska således bara användas för detta ändamål.

Certifikatutfärdarens certifikat:

Ändamål: Signering av certifikat och spärrlistor.

Certifikatinnehavarens Signeringscertifikat:

Ändamål: Digital signatur

Både Certifikatutfärdarens certifikat och Signeringscertifikatet avviker till vissa delar från ICAO:s rekommendationer. Undantagen beskrivs närmare i Certifieringspraxisen.

6.2.Skydd av Certifikatutfärdarens privata nyckel

6.2.1.Standarder som gäller säkerhetsmodulen

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.

6.2.2.Personal som medverkar i behandlingen av Certifikatutfärdarens privata nyckel

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

6.2.3.Registrering av Certifikatutfärdarens privata nyckel

Certifikatutfärdaren ska förvara sin privata nyckel i en kryptografisk modul och sträva efter att förhindra att den att den försvinner, råkar i händerna på utomstående, ändras eller används av obehöriga.

6.2.4.Säkerhetskopia av privat nyckel

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

6.2.5.Arkivering av privat nyckel

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

6.2.6.Administrering av privat nyckel i kryptografiska moduler

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

Administrationen av den privata nyckeln beskrivs i detalj i certifieringspraxisen.

6.3.Övriga omständigheter i anslutning till nyckeladministration

Arkivering av offentlig nyckel

Utfärdaren arkiverar alla certifierade offentliga nycklar.

6.3.1.Giltighetstiden för offentliga och privata nycklar

Ett Signeringscertifikats giltighetstid är fem år och tre månader. Ett Signeringscertifikat kan spärras under dess giltighetstid. Ett Signeringscertifikat kan användas för att verifiera en elektronisk signatur efter att certifikatet har gått ut eller spärrats, ifall den certifierade signaturen skapades innan certifikatet spärrades eller gick ut.

6.4.Säkerhetskrav i anslutning till användningen av och åtkomsten till datorer

6.4.1.Utrustningens säkerhet

För certifikatsystemet används bara ändamålsenlig utrustning.

Förfarandet beskrivs i detalj i certifieringspraxisen.

6.5.Hantering av certifikatsystemets livscykel

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

6.5.1.Övervakning av systemutvecklingen

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

6.5.2.Hantering av säkerhet

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

6.6.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.

6.7.Övervakningen av användningen av kryptografiska moduler

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

Förfarandet beskrivs i detalj i certifieringspraxisen.

7.Certifikat- och spärrlistprofiler

7.1.Tekniska uppgifter om certifikat

I sammanfattningen av certifieringspraxisen beskrivs innehållet i Certifikatutfärdarens certifikat och certifikatinnehavarens Signeringscertifikat.

7.2.Spärrlistprofil

I sammanfattningen av certifieringspraxisen beskrivs innehållet i spärrlistan som Certifikatutfärdaren publicerat.

8.Hantering av dokument innehållande bestämmelser

8.1.Ändring av bestämmelser

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

8.2.Förfarande för ändring och godkännande av certifikatpolicyn

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för Signeringscertifikatet. Myndigheten för digitalisering och befolkningsdata, Polisstyrelsen, Migrationsverket och utrikesministeriet kan gemensamt besluta att ändra handlingarna.

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 innehavaren av Signeringscertifikatet och förlitande parter kan ändras så att ändringarna meddelas 14 dagar innan de träder i kraft.

8.3.Hantering av versioner

Certifikatpolicy för Signeringscertifikat för Finlands chipförsedda resedokument och uppehållstillståndshandlingar, v 1.2.

Version	**Datum**	**Beskrivning / ändringar**
v 1.0	27.05.2011	Godkänd version 1.0.
v 1.1	02.11.2023	Myndighetens namnändringar har lagts till. De tekniska uppgifterna har uppdaterats, bl.a. 512-bit ECC-nyckel. Föråldrade lagparagrafer har uppdaterats.
v 1.2	01.02.2024	Polisstyrelsens kommentarer har beaktats.