MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIKATPOLICY

för Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat

OID: 1.2.246.517.1.10.202
OID: 1.2.246.517.1.10.302
OID: 1.2.246.517.1.10.352

13.1.2026

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio, Saaripuu Tuire, Taija Malinen
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
1.0	Godkänd version 1.0., dokument förenligt med eIDAS-förordningen	3.5.2018 TS
1.1	Godkänd version, Befolkningsregistercentralens namnbyte, publicering.	1.1.2020 TS
1.2	Uppdaterad version, tillgänglighetsegenskaper, namnändring av lagen 661/2009	6.5.2021
1.3	Tillagd information om loggdata	1.10.2021/VA
1.4	Uppdaterade versionen och länkarna till CPS dokument	23.9.2022/SK
1.5	Ersatt termen "PUK-kod" med termen "aktiveringskod". Tillagd information om aktiveringskod. Tillagd definitionen för ISO IEC 27001 till avsnitt 5.2. Tagit bort SSCD och lagt till QSCD i avsnitt 5.2. Korrigerat RSA-nyckelbiträkning till avsnitt 9.2.8. Uppdaterat länkar.	8.3.2023/AG
1.6	Avlägsnat ordet ”kryptering” i flera avsnitt (verifikation och kryptering -> verifikation). I avsnitt 5.1 uppdaterad information om aktiveringskod. I avsnitt 9.2.8 tillagd information ”minst 384-bitars ECC-nycklar”. I avsnitt 9.3.6 updaterad ordet ”omedelbart” -> ”utan fördröjelse (efter att begäran om spärrning har anlänt)”	15.9.2023/TM
1.7	Tillagd ”0.4.0.2042.1.7 (ETSI Organization Validated Certificate Policy)” i avsnitt 7.1, 7.2 och 7.3.1.	30.11.2023/TM
1.8	Konsoliderade dokumenten G2 och G3. Uppdaterar överensstämmelse med EU nr 910/2014 -> ändrad till eIDAS-förordningen. Uppdaterad personuppgiftslagen -> dataskyddslagen	13.9.2024/TV
1.9	Omnämnandet om att publicera certifikatet i en offentlig katalog togs bort från avsnitt 6.3.4, 8.3, 9.3.1 och 9.3.5	30.4.2025 / TV

1.10	Lade till information om tillgängligheten av certifikatens statusinformation till stycke 8.4.4. Lade till information om betroddheten av certifikat och deras statusinformation om CA:ns privata nyckel äventyrats till stycke 9.3.7.	1.9.2025 / TV
1.11	Termen aktiveringskod har ersatts med PUK-kod där det är relevant, eller lagts till där det behövs i avsnitt 5.1, 5.2, 8.4.5 och 9.3.1	4.11.2025 / TV

Innehållsförteckning

CERTIFIKATPOLICY

1 Förord

Detta dokument grundar sig på en teknisk specifikation som har upprättats av tekniska kommittén ETSI (ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), som är inriktad på elektroniska signaturer och system.

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

Denna certifikatpolicy gäller för följande certifikatutfärdare för medborgarcertifikat:

- VRK CA – G3-rotcertifikatets VRK Gov. Root CA – Utfärdat av G2
- DVV– G4R rotcertifierare DVV Gov. Root CA – Utfärdad av G3 RSA
- DVV– G4E rotcertifierare DVV Gov. Root CA – Utfärdad av G3 ECC

2 Inledning

Elektronisk kommunikation förutsätter att källan till den elektroniska informationen kan identifieras på ett sätt som kan jämföras med en signatur för hand på dokument. Detta kan i allmänhet genomföras med hjälp av elektroniska signaturer. De som tillhandahåller certifikattjänster, och allmänt benämns certifikatutfärdare, producerar certifikat som behövs för att skapa elektroniska signaturer.

De som använder elektroniska signaturer kan lita på att de är autentiska om certifikatutfärdaren tillämpar tillbörliga förfaranden och skyddsmetoder för att minimera de funktionella och ekonomiska riskerna i anslutning till systemen med öppna krypteringsnycklar.

Detta dokument grundar sig på de särskilda kraven på den tillförlitlighet hos elektroniska signaturer som definierats enligt följande förordning:

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 (eIDAS Förordningen). I dokumentet fastställs kraven på verksamheten och förvaltningspraxisen hos dem som utfärdar signeringscertifikat enligt eIDAS Förordningen.

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

Denna certifikatpolicy tillämpas på Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat som utfärdas för finska medborgare och i Finland fast bosatta utlänningar som är registrerade i befolkningsdatasystemet.

Medborgarcertifikatet består av tre olika certifikat med två olika användningsändamål: autentisering och elektroniska signaturer. Autentiseringscertifikatet är ett verktyg för

stark autentisering enligt lagen. Signeringscertifikat är verktyg för elektroniska signaturer som är förenliga med lagen om stark autentisering och betrodda elektroniska tjänster. Det ena av de två signeringscertifikaten som uppfyller samma kravnivå baserar sig på en RSA-algoritm och den andra på en EEC-algoritm. Innehavaren av certifikatet kan använda vilket som helst av dessa certifikat för elektroniska signaturer.

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

3 Tillämpning

I detta dokument fastställs kraven på förfaranden som gäller utfärdare av autentiseringscertifikat och signeringscertifikat samt Myndigheten för digitalisering och befolkningsdata i egenskap av leverantör av verktyg för stark autentisering. Kraven ställs på verksamheten och förvaltningspraxisen hos dem som utfärdar certifikat för att de som ansöker om certifikat, de undertecknare som certifikatutfärdaren har certifierat samt de förlitande parterna ska kunna lita på att elektroniska signaturer kan styrkas med certifikatet.

Myndigheten för digitalisering och befolkningsdatas identifieringsverktyg för stark autentisering tillhandahålls i samma produktionsmiljö, med likadana tekniska och funktionella lösningar och med iakttagande av samma förfaranden som vid tillhandahållandet av det av Myndigheten för digitalisering och befolkningsdata utfärdade certifikatet för elektroniska signaturer.

Kraven på förfaranden som gäller certifikatutfärdaren innehåller krav på tillhandahållandet av registreringstjänster, processen för att skapa certifikat, distributionen av certifikat, hanteringen av återkallelser, spärrstatus och vid behov tillhandahållandet av ett verktyg för signaturframställning. Övriga funktioner hos en tillhandahållare av certifikattjänster, såsom tidsstämplar, attributcertifikat och tjänster som stöder konfidentialiteten omfattas inte av tillämpningsområdet för detta dokument. I detta dokument behandlas inga krav på certifikatutfärdarens certifikat och inte heller för certifikathierarkier eller dubbel certifiering. Dessa krav på förfaranden har begränsats till certifieringen av nycklar som används i samband med elektroniska signaturer.

Dessa krav har gällt i synnerhet signeringscertifikat som utfärdas för allmänheten och som används för att stöda elektroniska signaturer och certifikatutfärdare som utfärdar signeringscertifikat i enlighet med eIDAS Förordningen. Certifikat som utfärdas i enlighet med dessa krav på förfaranden kan användas för identifiering av en person när personen agerar för egen räkning eller för en annan fysisk person, en juridisk person eller en sammanslutning som personen företräder.

Dessa krav på förfaranden gäller användningen av kryptering med öppen nyckel vid certifiering av elektroniska signaturer.

Sakkunniga oberoende organ kan använda detta dokument som grund för bedömningen av huruvida certifikatutfärdaren uppfyller kraven på utfärdandet av signeringscertifikat.

Det rekommenderas att innehavare av ett certifikat och parter som litar på ett certifikat läser mer om hur utfärdaren verkställer sin certifikatpolicy i dokumentet om certifieringspraxisen.

I detta dokument preciseras emellertid inte hur oberoende parter kan bedöma att de krav som specificerats här har uppfyllts; exempelvis fastställs inte kraven på den information som ska tillställas ett oberoende bedömningsorgan eller kraven på ett oberoende bedömningsorgan.

4 Referensförteckning

I detta dokument refereras till bestämmelser och föreskrifter i följande dokument. Bestämmelserna och föreskrifterna är bindande i anslutning till de funktioner som behandlas i detta dokument.

Referenserna till publiceringsdagen och numret på upplagan eller versionen är antingen exakta eller av allmän natur.

Vid exakta referenser tillämpas inga senare revideringar av källan.

Vid referenser av allmän natur tillämpas den senaste versionen av källan.

Material med anknytning till detta dokument finns bland annat på .http://docbox.etsi.org/Reference ETSI garanterar inte att länken fungerar på lång sikt.

Föreskrivande referenser:

[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5 CA/Browser Forum.

[4] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

Vägledande referenser:

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user regarding a particular subject area.

[i.1] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.3] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data.

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Termbeskrivningar:

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1], ETSI

EN 319 411-1 [2], the Regulation (EU) N° 910/2014 [i.1] and the following apply:

EU Qualified Certificate: qualified certificate as specified in Regulation (EU) No 910/2014 [i.1]

Qualified Electronic Signature/Seal Creation Device: As specified in Regulation (EU) No 910/2014 [i.1].

5 Definitioner och förkortningar

5.1 Definitioner

I detta dokument används följande begrepp och 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 (t.ex. elektronisk signatur).

Aktiveringskod: Aktiveringsuppgift, som används för att aktivera och fastställa egna, personliga PIN-koder.

Undertecknare: person som på certifikatet har antecknats som innehavare av den hemliga nyckel som har kopplats till den öppna nyckeln i certifikatet.

Signaturframställningsdata: en unik uppsättning av uppgifter, exempelvis koder eller hemliga krypteringsnycklar, som undertecknaren använder för att skapa en elektronisk signatur.

När det handlar om signeringscertifikat som grundar sig på kryptering med öppen nyckel, såsom inom tillämpningsområdet för detta dokument, ingår hemliga nycklar i de uppgifter som används för att skapa signaturen. I detta dokument används begreppet hemlig nyckel för de uppgifter som används för att skapa en signatur.

Anordning för signaturframställning: en för ändamålet konfigurerad programvara eller maskinvara som uppgifterna för skapandet av signaturer behandlas med.

Signaturverifieringsdata: en uppsättning av uppgifter, exempel koder eller öppna krypteringsnycklar som används för verifiering av elektroniska signaturer.

När det handlar om signeringscertifikat som grundar sig på kryptering med öppen nyckel, såsom inom tillämpningsområdet för detta dokument, ingår öppna nycklar i de uppgifter som används för att autentisera signaturen. I detta dokument används begreppet öppen nyckel för de uppgifter som används för att autentisera en signatur.

Signeringscertifikat: Ett certifikat vars användningsändamål är en oavvislig elektronisk signatur.

Attribut: en uppgift som anger en aktörs egenskap, såsom medlemskap eller roll i en grupp, eller någon annan uppgift om aktören.

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

ECC-algoritm och ECC-nyckel: En ECC-algoritm omfattar algoritmer i anslutning till olika krypteringsmetoder med elliptiska kurvor. Algoritmerna utgör ett krypteringssystem som bygger på en öppen nyckel. På samma sätt som RSA-nyckelparet består en ECC-nyckel av en öppen och en hemlig nyckel.

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.

Identitetskort: Ett av polisen utfärdat identitetsbevis i vars tekniska del kortinnehavarens medborgarcertifikat har lagrats.

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: Informationssäkerhetsstruktur där informationssäkerhetstjänster produceras enligt metoder 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.

Medborgarcertifikat: Medborgarcertifikatet består av ett certifikatpar med två skilda användningsändamål: autentisering och signering. Om medborgarcertifikatets datainnehåll bestäms i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

Avancerad elektronisk signatur: En elektronisk signatur som uppfyller följande krav:

a) den är entydigt knuten till undertecknaren
b) den gör det möjligt att identifiera undertecknaren
c) den är skapad med en metod som endast undertecknaren kontrollerar
d) den är knuten till andra elektroniska data på ett sådant sätt att eventuella senare förvanskningar av dessa data kan upptäckas.

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 och verifiering av elektroniska signaturer.

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

Chip: Teknisk plattform som certifikatet och de hemliga nycklarna lagras på. Ett chip kan finnas på ett 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.

PIN-kod: Aktiveringsuppgift som används för att aktivera en hemlig nyckel på ett chip. PIN 1: baskod för autentisering. PIN 2: signeringskod för elektroniska signaturer.

PUK-kod: PIN Unlock Key PUK-koden behövs för att låsa upp en spärrad 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. En del av nyckelparen i anslutning till medborgarcertifikat är RSA-nycklar.

Spärrlista: En förteckning som signeras och publiceras elektroniskt av certifikatutfärdaren över certifikat som spärrats under deras giltighetstid och tidpunkten för spärrningen. Av spärrlistan framgår publiceringstidpunkten för den liksom 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.

Elektronisk signatur: uppgift i elektroniskt format som är fogad eller logiskt knuten till andra elektroniska uppgifter och som används som metod för verifiering av de andra uppgifterna i fråga.

Elektronisk kommunikationskod: En identifikator som består av siffror och ett kontrolltecken och som kan användas för att individualisera finska medborgare och utlänningar som enligt lagen om hemkommun är fast bosatta i Finland och införda i befolkningsdatasystemet.

Elektronisk signatur: avancerad elektronisk signatur som grundar sig på ett signeringscertifikat och som har skapats med en säker anordning för signaturframställning.

Säker anordning för signatursframställning: anordning för signaturframställning som uppfyller kraven i eIDAS Förordningen.

Certifikat: Ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar undertecknarens identitet. Certifikatet innehåller en kod som individualiserar den aktuella certifieringspraxisen.

Certifikat: innehåller användarens öppna nyckel samt andra uppgifter vars förfalskning har förhindrats genom kryptering av dem med certifikatutfärdarens hemliga nyckel. Den mer exakta beskrivningen grundar sig på ITU-T:s rekommendation X.509.

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

Certifikatbeskrivning: Ett dokument som innehåller de centrala punkterna i certifikatpolicyn och certifieringspraxisen.

Tillhandahållare av certifikattjänster: sammanslutning, juridisk person eller fysisk person som utfärdar certifikat eller tillhandahåller andra tjänster i anslutning till elektroniska signaturer.

I detta dokument behandlas tillhandahållare av certifikattjänster som utfärdar signeringscertifikat (eller tillhandahåller deltjänster för utfärdande av signeringscertifikat – se punkt 4.1). Andra tjänster, såsom tidstämpling och system med reservnycklar, behandlas inte i detta dokument.

Certifikatpolicy: regelverk som visar hur ett visst certifikat lämpar sig för en viss sammanslutning och/eller tillämpningsklass som berörs av gemensamma säkerhetskrav. Den mer exakta beskrivningen grundar sig på ITU-T:s rekommendation X.509.

Certifikatregister: Ett register som är förenligt med lagen om stark autentisering och betrodda elektroniska tjänster och som den som tillhandahåller signeringscertifikat för

allmänheten är skyldig att föra. Uppgifterna ska bevaras i minst fem år efter att certifikatets giltighetstid har gått ut.

Datasystem för certifiering: Ett datatekniskt system som består av certifikatsystem, datakommunikation, certifikatregister och spärrlisttjänster, rådgivnings- och spärrtjänst samt administration av certifikat och kort.

Koden som individualiserar certifieringspraxisen är en del av certifikatets datainnehåll.

Certifieringspraxis: ett utlåtande om den praxis som certifikatutfärdaren iakttar vid utfärdandet, administrationen, återkallandet och förnyandet av certifikat samt byte av certifikatens nyckelpar. Varje certifieringspraxis har en egen individualiserande kod.

Certifikatutfärdare: En organisation som utfärdar certifikat, svarar för produktionen av certifikat och upprättar en certifikatpolicy och en certifieringspraxis som beskriver verksamheten. En eller flera aktörer litar på certifikatutfärdarens verksamhet. Certifikatutfärdaren tillhandahåller certifikattjänster. Den mer exakta beskrivningen grundar sig på ITU-T:s rekommendation X.509. Begreppet certifikatutfärdare förtydligas i punkt 4.2.

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 medborgarcertifikat 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.

Certifikatsökande/-innehavare: En fysisk person som ansöker om certifikat, som identifieras på ett personligt sätt och som vid mottagandet av certifikatet blir innehavare av det.

Certifikatinnehavarens signeringscertifikat: Med den öppna nyckeln som finns lagrad på certifikatet verifieras med hjälp av motsvarande hemliga nyckel, dvs. med signeringsnyckeln, certifikatinnehavarens elektroniska signatur. För att underteckna elektroniskt behövs en signerings-kod (PIN 2).

Certifikatinnehavarens autentiseringscertifikat: Ett certifikat som används för elektronisk identifiering av personer. och för kryptering av data Certifikatinnehavaren använder sin hemliga autentiseringsnyckel för elektronisk identifiering. För användningen av nyckeln behövs en baskod (PIN 1).

Certifikatanvändning och användningsområde: I detta dokument avses med certifikatanvändning användningen av såväl själva certifikatet som tillhörande nycklar. Till exempel avser användningen av certifikat för elektroniska signaturer användningen av dels hemliga nycklar för signaturer, dels öppna nycklar och certifikat för verifiering av signaturer.

Förlitande part: mottagare av certifikatet som litar på certifikatet i fråga och/eller på elektroniska signaturer som har autentiserats med certifikatet. Den mer exakta beskrivningen grundar sig på RFC 3647-specifikationen.

Spärrlista över certifikat: en signerad förteckning över certifikat vars utfärdare inte längre anser att certifikaten är i kraft. Den mer exakta beskrivningen grundar sig på ITU-T:s rekommendation X.509.

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.

5.2 Förkortningar

ISO/IEC 27001	ISO IEC 27001, internationellInternationell standard för kontroll av informationssäkerhetin-formationssäkerhet
CA	Certification Authority, certifikatutfärdare
CSP	Certification Service Provider: tillhandahållare av certifikattjänster
CP	Certificate Policy, certifikatpolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
EEC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, säkerhetsmodul
HST	Elektronisk identifiering av person
HTTP	Hypertext Transfer Protocol
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
RSA	Rivest, Shamir, Adleman, RSA-kod, en algoritm för den öppna nyckeln, en asymetrisk algoritm
SATU	Elektronisk kommunikationskod
SIM	Subscriber Identity Module
MDB	Myndigheten för digitalisering och befolkningsdata
QSCD	Qualified Signature Creation Device: godkänt verktyg för skapande av elektronisk signatur

6 Allmänna begrepp

6.1 Certifikatutfärdare

Certifikatutfärdaren skapar och utfärdar certifikat. De som anlitar certifikattjänsterna, dvs. de som ansöker om certifikatet och de förlitande parterna litar på certifikatets

funktion. Utfärdaren bär det övergripande ansvaret för tillhandahållandet av de certifikattjänster som fastställs i punkt 6.2. Utfärdaren individualiseras på certifikatet. Signeringscertifikat signeras med utfärdarens hemliga nyckel.

Utfärdaren kan anlita övriga partner inom sina certifikattjänster för tillhandahållandet av delar av tjänsten. Utfärdaren ansvarar emellertid alltid för hela tjänsten och säkerställer att de krav på förfaranden som fastställts i detta dokument också uppfylls. Utfärdaren kan exempelvis införskaffa samtliga deltjänster av underleverantörer, även tjänster för skapande av certifikat. Nyckeln som används för att signera certifikaten innehas dock av utfärdaren och utfärdaren har helhetsansvaret för att de krav som fastställs i detta dokument uppfylls och för att certifikat som utfärdas för allmänheten är förenliga med eIDAS Förordningen.

Certifikatutfärdaren kan bevilja certifikat åt sin egen verksamhet. I så fall följer den samma förutsättningar som om certifikatet skulle beviljas åt någon annan organisation.

Certifikatutfärdaren är en tillhandahållare av certifikattjänster som avses i eIDAS Förordningen.

I detta dokument fastställs kraven på förfaranden som gäller utfärdare av signeringscertifikat samt Myndigheten för digitalisering och befolkningsdata i egenskap av leverantör av verktyg för stark autentisering. Kraven ställs på verksamheten och förvaltningspraxisen hos dem som utfärdar certifikat för att de som beställer certifikat, de undertecknare som certifikatutfärdaren har certifierat samt de förlitande parterna ska kunna lita på att elektroniska signaturer kan styrkas med certifikatet.

Myndigheten för digitalisering och befolkningsdatas identifieringsverktyg för stark autentisering tillhandahålls i samma produktionsmiljö, med likadana tekniska och funktionella lösningar och med iakttagande av samma förfaranden som vid tillhandahållandet av det av Myndigheten för digitalisering och befolkningsdata utfärdade certifikatet för elektroniska signaturer.

Myndigheten för digitalisering och befolkningsdata (MDB) hör till finansministeriets förvaltningsområde. MDB är en myndighet som upprätthåller personregister. Enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) har MDB till uppgift att producera tjänster inom certifierad elektronisk kommunikation. Sedan 1.12.2010 har Myndigheten för digitalisering och befolkningsdata varit lagstadgad certifikatutfärdare för hälso- och sjukvården (lag om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lag om elektroniska recept (61/2007). Myndigheten för digitalisering och befolkningsdatas Certifikattjänster ansvarar för ämbetsverkets certifikatverksamhet. MDB har tillhandahållit certifikatbaserade signerings- och autentiseringsverktyg sedan år 1999 och utfärdat signeringscertifikat sedan 31.3.2003.

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

tekniska leverantörer som MDB anlitar. MDB:s Certifikattjänster upprätthåller dokument över certifikatpolicyer, certifieringspraxis och certifikatbeskrivningar. Dokumenten finns på https://dvv.fi/sv/certifikatpolicydokument.

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 tillämpas på betrodda tjänster från och med 1.7.2016. Skyldigheterna enligt eIDAS Förordningen har till vissa delar satts i kraft även i och med ändringen av lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) som trädde i kraft 1.7.2016. I lagen föreskrivs om tillhandahållandet av tjänster för stark autentisering och elektroniska signaturer samt om deras rättsverkningar. Om identitetskort föreskrivs i lagen om identitetskort (663/2016) och om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

MDB producerar beträffande informationssäkerheten förstklassiga certifikat för elektroniska signaturer och elektronisk identifiering samt relaterade tjänster för den offentliga och den privata sektorn. Med hjälp av certifikatet styrks identiteten hos innehavaren av certifikatet och bekräftas riktigheten, integriteten och autenticiteten hos de uppgifter som ingår i certifikatet. En elektronisk signatur som gjorts med hjälp av ett signeringscertifikat och en identifiering av en person som gjorts med hjälp av ett verktyg för stark autentisering ger medborgarna möjlighet till trygg och flexibel elektronisk kommunikation som är oberoende av tid och rum. I Finland utövar Traficom tillsyn över dem som tillhandahåller signeringscertifikat och tjänster för stark autentisering.

Denna certifikatpolicy som beskriver utfärdandet av medborgarcertifikat har registrerats av Myndigheten för digitalisering och befolkningsdata.

Denna certifikatpolicy beskriver de detaljerade kraven på utfärdandet och produktionen av signeringscertifikat, vilka grundar sig på eIDAS Förordningen och är förenliga med lagen om stark autentisering och elektroniska betrodda tjänster, samt de detaljerade kraven på ansvarsfördelningen vid utfärdandet och produktionen. signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de krav som ställs på kvalificerade signeringscertifikat och på anordningar för skapande av kvalificerade elektroniska signaturer såsom föreskrivs i artikel 28 och 29 i eIDAS Förordningen. Graden av tillförlitlighet på autentiseringscertifikatet är "hög" enligt eIDAS Förordningen och i förordningen om tillitsnivåer som utfärdats med stöd av eIDAS Förordningen.

Detta dokument beskriver vidare olika lösningar och förfaranden i anslutning till utfärdande av autentiseringscertifikat, produktion av autentiseringscertifikat och registrering av uppgifter, med iakttagande av kraven på produktionsmiljön för signeringscertifikat, när autentiseringscertifikatet tillhandahålls som ett verktyg för stark autentisering inuti ett medborgarcertifikat och är förenligt med lagen om stark autentisering och elektroniska betrodda tjänster.

Ett medborgarcertifikat består av ett certifikatpar som har två särskilda användningsändamål. Autentiseringscertifikatet uppfyller kraven på identifieringsverktyg för stark

autentisering. signeringscertifikatet, som enbart är avsett för att genomföra signaturer, uppfyller kraven på signeringscertifikat. Myndigheten för digitalisering och befolkningsdata garanterar identiteten hos den som ansöker om ett certifikat.

6.2 Certifikattjänster

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. Datainnehållet i certifikat som är förenliga med denna certifikatpolicy fastställs i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

Ett medborgarcertifikat enligt denna certifikatpolicy kan utfärdas för en finländsk medborgare eller för en enligt lagen om hemkommun (201/1994) i Finland fast bosatt utlänning vars personuppgifter har registrerats i befolkningsdatasystemet.

Myndigheten för digitalisering och befolkningsdata, som är certifikatutfärdare, specificerar innehavaren av certifikatet med hjälp av en elektronisk kommunikationskod (SATU), som även är en del av certifikatets datainnehåll. Den elektroniska kommunikationskoden är en teknisk identifieringskod enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster, som skapats separat för elektronisk kommunikation och som inte innehåller uppgifter som identifierar personen.

Ett medborgarcertifikat kan utfärdas och lagras på olika tekniska underlag som utfärdats av en myndighet, dvs. på chip som finns på identitetskort. Denna certifikatpolicy är en gemensam beskrivning av medborgarcertifikat som kan finnas på dessa olika tekniska underlag.

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

Utfärdandet av Myndigheten för digitalisering och befolkningsdatas signeringscertifikat har i detta dokument, av skäl som hänger samman med klassificeringen av kraven, indelats i följande deltjänster:

Registreringstjänst: I registreringstjänsten verifieras undertecknarens identitet och eventuella attribut som relaterar till undertecknaren. Dessa förmedlas till tjänsten för skapande av certifikat.

Registreringstjänsten innehåller också en funktion för leverans av nycklar som skapas av kunden själv eller någon annan utfärdare. I Myndigheten för digitalisering och befolkningsdatas registreringstjänst behandlas inga andra nyckelpar än sådana som centralen själv skapat.

Registreringen av medborgarcertifikatet iakttar det förfaringssätt som beskrivs i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster. En närmare beskrivning av förfaringssättet ges i certifieringspraxisen för det aktuella tekniska underlaget.

Tjänst för skapande av certifikat: I tjänsten skapas och undertecknas certifikat som grundar sig på identiteten och de övriga attributen som verifierats i registreringstjänsten.

Distributionstjänst: Via distributionstjänsten distribueras certifikaten till undertecknarna och ställs certifikaten till förfogande för de förlitande parterna, om undertecknaren ger tillstånd till det. Vidare får beställare och förlitande parter tillgång till certifikatutfärdarens användningsvillkor samt all publicerad information om certifikatpolicyn och certifieringspraxisen via distributionstjänsten. Myndigheten för digitalisering och befolkningsdata skickar uppgifterna till ett offentligt register. Registertjänsten är en offentlig webbtjänst som innehåller samtliga medborgarcertifikat som utfärdats av certifikatutfärdaren samt certifikatutfärdarens certifikat och spärrlista. Registertjänsten finns på ldap://ldap.fineid.fi.

Tjänst för hantering av återkallanden: Tjänsten för hantering av återkallanden spärrar ett certifikat som en certifikatinnehavare önskar spärra innan certifikatets giltighetstid löper ut.

I tjänsten handläggs begäranden och anmälningar om återkallande och fastställs behövliga åtgärder utifrån handläggningen. Tjänstens resultat distribueras med hjälp av spärrlistan.

Tjänst för information om spärrstatus:

Via tjänsten för information om spärrstatus distribueras information om spärrade certifikat till de förlitande parterna. I tjänsten kan man använda spärrlistor eller förmedla statusinformation om enskilda certifikat i realtid. Myndigheten för digitalisering och befolkningsdata förmedlar uppgifterna till spärrtjänsten så att de blir tillgängliga för de förlitande parterna. Statusinformationen uppdateras regelbundet. Detta beskrivs i detalj i handboken om certifieringspraxisen.

Tillhandahållande av en anordning för signaturframställning för undertecknare:

Anordningen för signaturframställning tillverkas och levereras till undertecknaren. Vad gäller certifikatet, de till certifikatet kopplade nyckelparen och aktiveringsuppgifterna agerar den som tillverkar och individualiserar ett aktivkort eller ett chip på certifikatutfärdarens uppdrag och ansvar och i enlighet med ett samarbetsavtal. Aktivkort och chip individualiseras enligt de uppgifter som registreraren lämnat.

Det enda syftet med den tillämpade tjänsteindelningen är att klarlägga kraven på förfaranden. Indelningen av hur certifikatutfärdaren genomför sina tjänster begränsas inte i denna beskrivning.

6.2.1 Förlitande part

En förlitande part är en person eller en organisation som litar på innehållet i certifikatet och som använder certifikatet för att autentisering och elektroniska signaturer. En förlitande part ska kontrollera att det certifikat som används är i kraft.

6.3 Certifikatpolicy och certifieringspraxis

I denna punkt beskrivs förhållandet mellan certifikatpolicy och certifieringspraxis. Certifikatpolicyns form eller begränsningar som gäller certifieringspraxisens specifikationer tillämpas inte i detta kapitel.

6.3.1 Syfte

Den certifikatpolicy vars kod framgår av certifikatet anger huvudprinciperna för certifieringsverksamheten på ett allmänt plan. I certifieringspraxisen redogörs i detalj för förfaringssätten och metoderna i anslutning till certifikatverksamheten, särskilt till skapande och upprätthållande av certifikat, med hänsyn till uppfyllandet av kraven i certifikatpolicyn.

I detta dokument fastställs den certifikatpolicy som ska tillämpas för att uppfylla de krav på signeringscertifikat som föreskrivits i eIDAS Förordningen. I dokumentet beskrivs vidare hur den som utfärdar identifieringsverktyg för stark autentisering ska förfara när identifieringsverktyg för stark autentisering sätts i omlopp. I egenskap av certifikatutfärdare specificerar Myndigheten för digitalisering och befolkningsdata i sin certifieringspraxis hur dessa krav uppfylls.

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

Medborgarcertifikat som är förenliga med denna certifikatpolicy kan användas för stark autentisering av en person och för elektroniska signaturer. Medborgarcertifikat kan användas i enlighet med användningssyftet utan begränsningar i tillämpningar och tjänster som tillhandahålls av förvaltningen eller av privata organisationer.

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.

I egenskap av certifikatutfärdare ändrar Myndigheten för digitalisering och befolkningsdata objektidentifieraren för certifikatpolicyn, ifall ändringar görs i certifikatpolicyns tillämpningsområde.

6.3.2 Detaljer

Certifikatpolicyn beskriver de allmänna kraven på certifikatutfärdarens verksamhet. I certifieringspraxisen beskrivs mer detaljerat än i certifikatpolicyn åtgärder som utfärdaren vidtar vid utfärdandet av certifikat och inom den övriga förvaltningen. I certifieringspraxisen fastställs hur en utfärdare uppfyller de tekniska kraven i certifikatpolicyn samt kraven på organisationen och förfaringssätten.

I egenskap av certifikatutfärdare har Myndigheten för digitalisering och befolkningsdata sammanställt dokument för styrningen av sina interna funktioner och de funktioner som läggs ut på entreprenad. Dessa dokument är inte offentliga.

Denna certifikatpolicy är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som

åtnjuter allmänt förtroende. Myndigheten för digitalisering och befolkningsdata för ett rikstäckande personregister. Enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) har Myndigheten för digitalisering och befolkningsdata till uppgift att producera tjänster inom certifierad elektronisk kommunikation.

6.3.3 Approach

Dokumenten om certifikatpolicy respektive certifieringspraxis har upprättats för olika användningsändamål. Certifikatpolicyn är en allmän beskrivning av certifikatutfärdarens verksamhet. Certifieringspraxisen ger en detaljerad beskrivning av certifikatutfärdarens verksamhet enligt organisationsstruktur, verksamhetssätt, verksamhetslokaler och informationstekniska miljö.

6.3.4 Andra dokument som publiceras av utfärdaren

Utöver certifikatpolicyn och certifieringspraxisen kan utfärdaren även publicera andra dokument som styr certifikatverksamheten. Sådana dokument är bland annat bruksanvisningar och allmänna presentationer av certifikatverksamheten som riktar sig till konsumenter, kundorganisationer och tjänstebyggare.

Vilka rättigheter och skyldigheter en innehavare av ett medborgarcertifikat har nämns i ansökningshandlingen och i den allmänna bruksanvisningen som ges innan ansökan om medborgarcertifikat undertecknas. Ansökan och bruksanvisningen utgör avtalet med den som ansöker om medborgarcertifikat. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter. Den som ansöker om ett medborgarcertifikat godkänner de allmänna bruksvillkoren i samband med ansökan.

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

Certifikatbeskrivningen är den del av utfärdarens användarvillkor som gäller verksamheten i ett system med öppen nyckel. I egenskap av certifikatutfärdare publicerar Myndigheten för digitalisering och befolkningsdata certifikatbeskrivningen så att den är tillgänglig både för den som söker om certifikatet och för de förlitande parterna.

6.4 Certifikatsökande

En certifikatsökande kan ansöka om ett certifikat för användning i eget namn eller också för signaturer på dokument som sökanden gör i en sammanslutnings namn. Denna skillnad har beskrivits i detta dokument varje gång det är nödvändigt att göra skillnad på användning i eget namn respektive en sammanslutnings namn. När ett certifikat ansöks identifieras privatpersonen alltid på ett personligt sätt.

Den som ansöker om medborgarcertifikat är alltid en privatperson som identifierats på ett personligt sätt.

7 Inledning till certifikatpolicyer

7.1 Allmänt

Med en certifikatpolicy avses principer som visar hur ett visst certifikat lämpar sig för en viss målgrupp. I certifikatpolicyn beskrivs även gemensamt tillämpliga säkerhetskrav.

I detta dokument fastställs kraven på förfarande enligt certifikatpolicyerna. Dessa certifikatpolicyer gäller signeringscertifikat såsom definieras i eIDAS Förordningen.

Certifikat som utfärdats i enlighet med detta dokument innehåller en objektidentifierare (OID), med hjälp av vilken de förlitande parterna kan fastslå att certifikatet är gångbart och pålitligt för ett visst användningsändamål. I detta dokument specificeras certifikatpolicyn för signeringscertifikat som utfärdas för allmänheten och för vilka det förutsätts användning av säkra anordningar för signaturframställning.

I detta dokument bestäms tolkningen av begreppet allmänhet enligt den nationella lagstiftning som tillämpas på den aktuella situationen. Certifikat kan betraktas som certifikat som utfärdas för allmänheten om användningen av de aktuella certifikaten inte har begränsats till frivilliga privaträttsliga avtal mellan parter.

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.

Denna certifikatpolicy heter Certifikatpolicy för Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat, OID 1.2.246.517.1.10.202, 1.2.246.517.1.10.302 och 1.2.246.517.1.10.352.

Certifikatpolicyn hänvisar till certifikatutfärdarens certifikatpolicy, OID 1.2.246.517.1.10.201, 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 eIDAS Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], punkten QCP-n-QSCD; OID: 0.4.0.194112.1.2 och 0.4.0.2042.1.7 (ETSI Organization Validated Certificate Policy). Signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana kvalificerade elektroniska signaturer som motsvarar kvalificerade certifikat och anordningar för framställning av elektroniska signaturer som beskrivits i artikel 28 och 29 i eIDAS Förordningen.

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

Denna certifikatpolicy är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata svarar för administrationen av denna certifikatpolicy och för uppdateringar i den.

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

Ansvarsområdet Förvaltning vid Myndigheten för digitalisering och befolkningsdatas Certifikattjänster besvarar frågor som gäller certifikatpolicyn och ansvarar för kommunikationen kring dessa dokument.

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

Myndigheten för digitalisering och befolkningsdata äger samtliga uppgifter som anknyter till medborgarcertifikaten och dokumentationen i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata äger samtliga ägande- och användarrättigheter till denna certifikatpolicy.

7.2 Identifieringskoder

När det gäller signeringscertifikat som tillhandahålls allmänheten iakttar Myndigheten för digitalisering och befolkningsdata en certifikatpolicy förenlig med betrodda tjänster i eIDAS Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], punkten QSCD; OID: 0.4.0.194112.1.2 och 0.4.0.2042.1.7 (ETSI Organization Validated Certificate Policy). 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 eIDAS Förordningen.

Ett signeringscertifikat som utfärdats i enlighet med denna certifikatpolicy uppfyller kraven i eIDAS Förordningen.

Certifikatpolicyn träder i kraft vid datumet som nämns på pärmsidan..

Certifikatutfärdaren inkluderar certifikatpolicyernas OID-koder även i de bruksvillkor som görs tillgängliga för dem som ansöker om certifikat och de förlitande parterna och uttrycker på det sättet vilka certifikatpolicyer som iakttas.

7.3 Användarkrets och tillämpbarhet

7.3.1 QCP-n-QSCD-certifikatpolicy

När det gäller signeringscertifikat som tillhandahålls allmänheten iakttar Myndigheten för digitalisering och befolkningsdata en certifikatpolicy förenlig med betrodda tjänster i eIDAS Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], punkten QSCD; OID: 0.4.0.194112.1.2 och 0.4.0.2042.1.7 (ETSI Organization Validated Certificate Policy). 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 eIDAS Förordningen.

Signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de krav som ställs på kvalificerade signeringscertifikat och på anordningar för skapande av kvalificerade elektroniska signaturer såsom föreskrivs i artikel 28 och 29 i förordningen.

7.4 Överensstämmelse med krav

7.4.1 Allmänt

Certifikatutfärdaren har rätt att använda nämnda objektidentifierare bara när certifikatutfärdaren uttrycker att den aktuella signeringscertifikatpolicyn följs och på beställarens eller de förlitande parternas begäran kan intyga överensstämmelsen med kraven.

De metoder som krävs för att intyga överensstämmelsen med kraven kan variera efter lagstiftningen i certifikatutfärdarens hemviststat. Att certifikatutfärdaren stämmer överens med kraven kontrolleras regelbundet samt alltid när det görs betydande ändringar i certifikatutfärdarens verksamhet.

7.4.2 Certifikatpolicyn för QCP-n-QSCD

En certifikatutfärdare som är förenlig med kraven ska påvisa att

a) de krav som ställts på certifikatutfärdare har uppfyllts

b) Certifikatutfärdaren har tagit i bruk de administrativa åtgärder som uppfyller samtliga krav.

8 Skyldigheter och ansvar samt begränsningar av ansvaret

Kraven i denna punkt tillämpas på **QCP-n-QSCD**–certifikatpolicyn, om inte annat anges.

8.1 Certifikatutfärdarens skyldigheter

Certifikatutfärdaren säkerställer att alla krav som gäller den för certifikatutfärdaren valda certifikatpolicyn uppfylls.

Certifikatutfärdaren ansvarar för att de i certifikatpolicyn fastställda förfarandena iakttas även om certifikatutfärdarens verksamhet genomförs enligt uppdragsavtal.

Certifikatutfärdaren tillhandahåller alla delområden av certifikattjänsten i enlighet med certifieringspraxisen.

8.1.1 Certifikatutfärdarens skyldigheter

Myndigheten för digitalisering och befolkningsdata har en lagstadgad uppgift att driva verksamhet som certifikatutfärdare.

Utfärdaren iakttar gällande lagstiftning i sin verksamhet.

Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.

Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt hantera eventuella krav på skadeersättning.

Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer eller personer, såsom registrerare, och korttillverkare.

Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning vid utfärdandet av medborgarcertifikat liksom andra aspekter på användningen av medborgarcertifikat 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 medborgarcertifikat och certifikatverksamheten, utifrån vilka utfärdarens verksamhet och pålitlighet kan bedömas.

Certifikatutfärdaren säkerställer att signaturframställningsdata är konfidentiell.

Certifikatutfärdaren varken lagrar eller kopierar de framställningsdata som överlåtits till en undertecknare.

8.1.2 Registrerarens skyldigheter

Registreraren agerar på certifikatutfärdarens ansvar och för certifikatutfärdarens räkning, och iakttar de förfaringssätt som överenskommits med certifikatutfärdaren.

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.

8.2 Skyldigheter för den som ansöker om certifikat

Certifikatutfärdaren ålägger genom avtal sökanden att iaktta alla nedan nämnda skyldigheter. Om undertecknaren och sökanden är olika aktörer ska sökanden informera undertecknaren om alla skyldigheter som gäller denne.

Användningsändamålet för ett av Myndigheten för digitalisering och befolkningsdata utfärdat medborgarcertifikat har för respektive certifikattyp fastställts i certifieringspolicyn, certifieringspraxisen och bruksanvisningen till innehavaren. Certifikatet får bara användas för elektroniska signaturer och autentisering.

Innehavaren av medborgarcertifikatet ansvarar för att de uppgifter som lämnats vid ansökan om medborgarcertifikatet är riktiga.

Innehavaren av medborgarcertifikatet ansvarar för användningen av det, för de rättshandlingar som innehavaren gör med medborgarcertifikatet och för de ekonomiska följderna av rättshandlingarna. När det gäller certifikatet för elektroniska signaturer gäller bestämmelserna i eIDAS Förordningen och i lagen om stark autentisering och betrodda elektroniska tjänster.

Innehavaren av medborgarcertifikatet förvarar de hemliga nycklarna på chipet och de koder som behövs för användningen av nycklarna 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 medborgarcertifikatet.

Medborgarcertifikatet ska behandlas och skyddas med samma omsorg som när det gäller andra chip, kort eller dokument, såsom kreditkort, körkort och pass. Personliga PIN-koder ska förvaras fysiskt på en annan plats än medborgarcertifikatet och det chip som innehåller hemliga nycklar.

Om ett chip eller ett kort försvinner eller det finns risk för missbruk ska detta anmälas utan dröjsmål till certifikatutfärdarens avgiftsfria spärrtjänst +358 800 162 622.

8.3 Information till de förlitande parterna

Ansvaret hos en utfärdare av signeringscertifikat som utfärdas för allmänheten omfattar de parter som har grundad anledning att förlita sig på certifikatet.

Spärrade medborgarcertifikat publiceras på en spärrlista. De förlitande parterna ska kontrollera mot spärrlistan att ett medborgarcertifikat är giltigt. Uppgiften om ett certifikats status kan också kontrolleras i OCSP-tjänsten.

Den förlitande parten är skyldig att säkerställa att certifikatet används i enlighet med användningsändamålet. Ett signeringscertifikat kan bara användas för detta ändamål. För ett autentiseringscertifikat är användningsändamålet återigen att identifiera personer och kryptera information.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan i god tro lita på medborgarcertifikatet efter att parten kontrollerat att **medborgarcertifikatet är i kraft.** Den förlitande parten är skyldig att kontrollera uppgiften om certifikatets status. För att säkerställa att det går att lita på medborgarcertifikatets giltighet ska den förlitande parten vidta följande åtgärder för granskning av spärrlistan, ifall spärrlistan används för att kontrollera statusuppgiften.

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 medborgarcertifikat inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Om en förlitande part ändå godkänner ett medborgarcertifikat efter att spärrlistans giltighetstid gått ut, sker det på den förlitande partens eget ansvar.

8.4 Ansvar

Det ansvar som fastställs i eIDAS Förordningen och i lagen om stark autentisering och betrodda elektroniska tjänster gäller certifikatutfärdare som utfärdar signeringscertifikat för allmänheten. Det ansvar som fastställts i lagen om stark autentisering och betrodda elektroniska tjänster gäller tjänsteleverantörer som tillhandahåller identifieringsverktyg eller -tjänster för stark autentisering.

8.4.1 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 medborgarcertifikatet har skapats med iakttagande av de förfaringssätt som lagts fram i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster, lagen om stark autentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet, certifikatpolicyn och certifieringspraxisen samt i enlighet med de uppgifter som sökanden av certifikatet har

uppgivit. Myndigheten för digitalisering och befolkningsdata ansvarar endast för de uppgifter som Myndigheten för digitalisering och befolkningsdata har lagrat på medborgarcertifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar för att medborgarcertifikatet kan användas från tidpunkten från överlåtelsen till giltighetstidens utgång – förutsatt att det används på tillbörligt sätt. Medborgarcertifikatet överlåts till en person som identifierats på det sätt som medborgarcertifikatet förutsätter. Före undertecknandet av avtalet har certifikatinnehavaren fått bruksanvisningar för medborgarcertifikatet.

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

Utfärdaren ansvarar för at rätt persons medborgarcertifikat införs på spärrlistan och att de tas upp på spärrlistan inom den tid som anges i denna certifieringspolicy.

8.4.2 Registrerarens ansvar

Registreraren av medborgarcertifikat är ett registreringsställe som registrerar som registrerar certifikatsökande för utfärdarens, dvs. Myndigheten för digitalisering och befolkningsdatas räkning och på dennes ansvar. Vid registreringarna iakttas kraven i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster och i lagen om stark autentisering och betrodda elektroniska tjänster samt – om medborgarcertifikatet placeras på ett identitetskort – lagen om identitetskort.

8.4.3 Certifikatinnehavarens ansvar

Medborgarcertifikatet är innehavarens elektroniska identitet och får därför inte överlåtas att användas av någon annan.

Innehavaren av medborgarcertifikatet 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 medborgarcertifikatet. När en terminalsession avslutas eller terminalen lämnas utan tillsyn ska certifikatinnehavaren avlägsna chipet med 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 medborgarcertifikatet upphör när han eller hon anmält behövliga uppgifter till spärrtjänsten för spärrningen av certifikatet och fått ett meddelande av den tjänsteman som tog emot samtalet att spärrningen har gjorts. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

8.4.4 Den förlitande partens ansvar

En part som förlitar sig på ett medborgarcertifikat kan inte i god tro lita på certifikatet och på att en elektronisk signatur är riktig ifall parten inte har kontrollerat att medborgarcertifikatet är i kraft via OCSP-tjänsten eller med hjälp av spärrlistan. Om statusuppgiften om ett certifikat inte har kontrollerats men parten trots detta godkänner det, befrias Myndigheten för digitalisering och befolkningsdata från ansvaret. Den förlitande parten ska kontrollera att det utfärdade certifikatet motsvarar användningsändamålet i den rättshandling där det används.

Certifikaten och deras statusinformation kan vara ogiltiga ifall CA:ns privata nyckel har äventyrats.

8.4.5 Begränsning av ansvar

Myndigheten för digitalisering och befolkningsdata ansvarar inte för eventuella skador som orsakas av att PIN-koden, aktiveringskoden, PUK-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 åsamkats dem, om skadan beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdata svarar inte för indirekta skador eller följdskador som medborgarcertifikatet har orsakats certifikatinnehavaren. Myndigheten för digitalisering och befolkningsdata svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till 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 programvara 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 kostnaderna 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 medborgare och organisationer som använder medborgarcertifikatet eller för kostnaderna för detta fel.

Certifikatutfärdaren svarar inte för skador som orsakas av force majeure, till exempel: strejk, eldsvåda, krig, uppror, konfiskering, valutarestriktioner, myndighetsåtgärder,

lagstiftning och myndighetsbestämmelser, störningar i telekommunikation, eller dylika signifikanta och ovanliga orsaker oberoende av certifikatutfärdaren.

8.4.6 Övriga parter

Förlitande parter kan lita på att medborgarcertifikat eller elektroniska signaturer är korrekta efter att ha kontrollerat 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.

Utfärdaren svarar för medborgarcertifikat enligt åtagandena i denna certifikatpolicy och i den certifieringspraxis som gäller medborgarcertifikat.

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. Bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster gäller Myndigheten för digitalisering och befolkningsdata. På verksamheten tillämpas även vissa bestämmelser i skadeståndslagen (412/1974).

Om elektroniska identitetskort föreskrivs i lagen om identitetskort och om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009). Om förvaltningsmässiga frågor bestäms också i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

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

9 Krav på certifikatutfärdarens verksamhet

Denna punkt tillämpas på en specifik signeringscertifikatpolicy, QCP-n-QSCD, om inte annat anges.

Certifikatutfärdaren vidtar följande administrativa åtgärder som uppfyller kraven.

Detta dokument gäller Myndigheten för digitalisering och befolkningsdata i egenskap av utfärdare av signeringscertifikat. Genomförandet av den tjänst som beskrivs i dokumentet omfattar tillhandahållande av registreringstjänster, skapande av certifikat, distribution av certifikat, processen för återkallande av certifikat och information om spärrstatus. Om ett krav knyter an till ett visst tjänsteområde, beskrivs det under respektive underrubrik. Om inget tjänsteområde specificeras eller om det sägs "certifikatutfärdaren i allmänhet", gäller kravet utfärdarens allmänna verksamhet.

Syftet med dessa krav på förfaranden är inte att begränsa certifikatutfärdarens möjligheter att debitera för sina tjänster.

Kraven som presenteras gäller säkerhetsmål och administrativa åtgärder som vidtas för att uppnå dessa och som specifika krav ställs på, om det anses vara nödvändigt för att uppnå målen.

9.1 Certifieringspraxis

Certifikatutfärdaren intygar att tillhandahållandet av certifikattjänsterna uppfyller de krav på pålitlighet som beskrivs i eIDAS Förordningen.

Det detaljerade förfaringssättet för de åtgärder som ingår i detta dokument beskrivs separat i certifieringspraxisen för respektive certifikattyp och lagringsunderlag.

9.2 Hantering av livscykeln för nycklar inom ett system med öppen nyckel

9.2.1 Skapande av certifikatutfärdarens nyckel

Certifikatutfärdaren säkerställer att dess nycklar skapas i en säker miljö, såsom beskrivs i eIDAS Förordningen.

Inom en ändamålsenlig tid innan certifikatutfärdarens signeringsnyckel upphör att gälla (till exempel vid den tidpunkt angivits på certifikatet) skapar utfärdaren ett nytt nyckelpar för signering av certifikat och utför alla nödvändiga åtgärder för att inga störningar ska uppkomma för de parter som litar på utfärdarens nyckel. En ny nyckel skapas för certifikatutfärdaren och distribueras enligt dessa förfaringssätt.

Åtgärderna ska vidtas i tillräckligt god tid för att alla parter som står i någon relation till certifikatutfärdaren (undertecknare, certifikatsökande, förlitande parter, certifikatutfärdare på högre nivå) ska få information om att certifikatutfärdarens nyckelpar kommer att bytas och kan vidta åtgärder som behövs för en störningsfri kontinuitet i verksamheten. Detta berör inte utfärdare som upphör med sin verksamhet för den sista giltighetsdagen för det egna utfärdarcertifikatet.

9.2.2 Lagring, säkerhetskopiering och återställande av certifikatutfärdarens nyckel

Certifikatutfärdaren säkerställer att certifikatutfärdarens hemliga nycklar är fortsatt konfidentiella och intakta i enlighet med eIDAS Förordningen.

Myndigheten för digitalisering och befolkningsdata skapar sina hemliga signeringsnycklar och de öppna nycklar som motsvarar de hemliga signeringsnycklarna.

Utfärdarens hemliga nycklar förvaras i kryptografiska moduler som administreras av utfärdaren och som överensstämmer med kraven i säkerhetsstandarden.

Utfärdaren svarar för att de hemliga nycklarna är skyddade mot exponering och obehörig användning. För att tillgodose kraven på säkring av kritisk information tas en säkerhetskopia av utfärdarens hemliga nycklar.

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

Av de hemliga nycklarna på Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat tas inga kopior.

9.2.3 Distribution av certifikatutfärdarens öppna nyckel

När ett medborgarcertifikat ska skapas med öppna nycklar på ett chip görs en begäran om skapande av certifikat. I begäran kopplas certifikatsökandens registreringsuppgifter till den öppna nyckeln i fråga.

Den öppna nyckeln på ett medborgarcertifikat är en del av utfärdarcertifikatet. Medborgarcertifikatet innehåller certifikatinnehavarens öppna nyckel.

Utfärdarcertifikatet fås från det offentliga registret. Om medborgarcertifikatet finns lagrat på ett aktivkort kommer även utfärdarcertifikatet att lagras på aktivkortets chip.

Utfärdarcertifikatet innehåller utfärdarens öppna nyckel. Utfärdarcertifikatet registreras i det offentliga registret. Innehavarcertifikatet lagras likaså i det offentliga registret. Utfärdarcertifikatet fås från utfärdarens offentliga register och på utfärdarens webbplats.

Utfärdaren arkiverar alla certifierade öppna nycklar.

9.2.4 System med reservnyckel

Av de hemliga nycklarna på Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat tas inga kopior.

9.2.5 Användning av certifikatutfärdarens nyckel

Certifikatutfärdaren ansvarar för att de hemliga signeringsnycklarna bara används för användningsändamålet.

Certifikatutfärdarens certifikat (utfärdarcertifikatet):

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

9.2.6 När certifikatutfärdarens nyckel går ut

Certifikatutfärdaren säkerställer i enlighet med eIDAS Förordningen att de hemliga signeringsnycklarna inte används efter att deras livscykel är till ända.

9.2.7 Hantering av livscykeln för krypteringsutrustning som används för signering av certifikat

Certifikatutfärdaren säkerställer att krypteringsutrustningen är säker under och efter hela dess livscykel i enlighet med eIDAS Förordningen.

9.2.8 Certifikatutfärdarens tjänster för hantering av signeringsnycklar

Certifikatutfärdaren säkerställer att alla signeringsnycklar skapas i en säker miljö och att konfidentialiteten hos undertecknarens hemliga nyckel har säkerställts i enlighet med eIDAS Förordningen.

Skapande av certifikat

Certifikatutfärdarens hemliga nyckel som används för att signera medborgarcertifikat samt den motsvarande öppna nyckeln är minst 4096-bitars RSA-nycklar och minst 384-bitars ECC-nycklar.

Certifikatinnehavarens hemliga och öppna nycklar är minst 3072-bitars RSA-nycklar och minst 384-bitars ECC-nycklar.

.

Fältet som fastställer användningssyftet i certifikatets datainnehåll anger användningssyftet för den nyckel som kopplats certifikaten. Användningen av en nyckel begränsas till det angivna användningsändamålet.

Certifikatutfärdarens certifikat (utfärdarcertifikatet):

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

Certifikatinnehavarens autentiseringscertifikat:

Ändamål: Autentisering av elektronisk identitet.Certifikatinnehavarens signeringscertifikat:

Ändamål: Elektroniska signaturer

9.2.9 Säker anordning för signaturframställning

Om utfärdaren utfärdar säkra anordningar för signaturframställning (QSCD), ska utfärdaren säkerställa att processen är förenlig med eIDAS Förordningen.

Att aktiveringsuppgifterna distribueras och anordningen för signaturframställningen vid olika tidpunkter eller längs olika kanaler är ett sätt att säkerställa att de hålls separata.

De ovan nämnda kraven på utfärdande av säkra anordningar för signaturframställning kan uppfyllas till exempel med stöd av en skyddsprofil som specificerats enligt standarden ISO/IEC 15408 eller på motsvarande sätt.

9.3 Hantering av livscykeln för certifikat inom ett system med öppen nyckel

9.3.1 Registrering av undertecknare

Certifikatutfärdaren säkerställer att undertecknarna identifieras och verifieras på tillbörligt sätt och att undertecknarens certifikatbegäranden är felfria, att uppgifterna i dem stämmer och att de grundar sig på en fullmakt i enlighet med eIDAS Förordningen.

Rättigheterna och skyldigheterna för den som ansöker om ett medborgarcertifikat ingår i ansökningsdokumentet och i de allmänna bruksvillkoren, som utgör avtalet som ingås med sökanden. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter.

I ansökningshandlingen och i bruksvillkoren nämns tydligt att den som ansöker om medborgarcertifikat intygar riktigheten hos uppgifterna med sin underskrift samt godkänner att certifikatet framställs. På samma gång godkänner sökanden reglerna och villkoren i anslutning till användningen av medborgarcertifikatet och förbinder sig att förvara medborgarcertifikatet och PIN-koderna omsorgsfullt samt att anmäla ett försvunnet kort.

Sökanden av ett medborgarcertifikat ansvarar för att samtliga uppgifter som är väsentliga för certifikatet och som sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren av ett medborgarcertifikat får bara använda det för de fastställda ändamålen.

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

Utfärdaren ansvarar vid utfärdandet av certifikatet för att datainnehållet i certifikatet är riktigt vid tidpunkten för överlåtelsen av certifikatet.

Uppgifterna på medborgarcertifikatet fastställer entydigt innehavaren av certifikatet. Utfärdaren utreder vid behov certifikatsökandens officiella identitet.

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

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

Medborgarcertifikatet kan hämtas personligen från registreringsstället.

Innehavaren av medborgarcertifikatet ansvarar för att förhindra att de privata nycklar som tillhör denne samt tillhörande aktiveringskoder eller PUK-kod används i strid med användarvillkoren. Detta ska ske genom att hantera dem på det sätt som anges i användarvillkoren.

Nyckelparet för innehavaren av Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat skapas i säkra utrymmen. Den öppna nyckeln används för att skapa certifikatet och den hemliga nyckeln förvaras på ett läs- och skrivskyddat chip.

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

Det finns två aktiverade koder: en baskod med vilken användaren kontrollerar identitetskortets underhåll och elektronisk identifiering, en signaturkod med vilken användaren kan göra en elektronisk signatur. Om användaren anger fel kod fem gånger, låses kortet och funktionen som skyddats med koden kan inte längre användas. Låsning av baskoden förhindrar användningen av samtliga tillämpningar som skyddas

med den. Låsning av signaturkoden förhindrar användningen av elektroniska signaturer. Låsta koder låses upp med PUK-koden.

Korttillverkaren skapar aktiveringsuppgifterna som gör det möjligt att använda nycklarna.

Aktiveringskoderna har skyddats så att de 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.

De aktiveringskoder som behövs för att man ska kunna använda medborgarcertifikatet behandlas i säkerhetssyfte så att de inte är samtidigt på samma plats före och under leveransen till certifikatsökanden.

Certifikatinnehavaren kan ladda ned ett kortläsarprogram från Myndigheten för digitalisering och befolkningsdatas webbplats. Med detta program kan medborgarcertifikatet användas för e-tjänster.

Den som ansöker om ett medborgarcertifikat kan registrera sin e-postadress både på medborgarcertifikatet och i befolkningsdatasystemet. E-postadressen antecknas i den form sökanden anger både på medborgarcertifikatet och i befolkningsdatasystemet. Den e-postadress som antecknats på medborgarcertifikatet införs i det offentliga registret på samma sätt som det övriga datainnehållet i medborgarcertifikatet. E-postadressen kan inte ändras så länge medborgarcertifikatet är i kraft.

9.3.2 Förnyande av certifikat, byte av nyckelpar och uppdatering av certifikat

De öppna nycklarna på medborgarcertifikatet och de hemliga nycklarna på chipet kan inte förnyas. För att ett nytt nyckelpar ska kunna bildas måste innehavaren ansöka om ett nytt medborgarcertifikat. Då iakttas samma förfaranden som vid den första certifikatansökan. Förfarandena beskrivs i detalj i dokumentet om certifieringspraxis.

9.3.3 Skapande av certifikat

Certifikatutfärdaren säkerställer att certifikaten utfärdas säkert så att deras autenticitet bevaras i enlighet med eIDAS Förordningen.

Certifikatinnehavarnas hemliga nycklar skapas säkert på ett sätt som uppfyller kraven på signeringscertifikat. Nyckelpar som en certifikatinnehavare skapar själv godkänns inte. I det skede när hemliga nycklar skapas görs inga kopior, och de kan inte heller överföras eller kopieras från ett chip. Certifikatutfärdaren och korttillverkaren har ingen åtkomst till certifikatinnehavarnas hemliga nycklar.

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

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

Av certifikatutfärdarens hemliga nycklar tas inga kopior.

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

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

9.3.4 Distribution av bruksvillkor

Utfärdaren säkerställer att bruksvillkoren och -anvisningarna ställs till förfogande för beställarna och de förlitande parterna i enlighet med eIDAS Förordningen.

Ett signeringscertifikat som utfärdats i enlighet med denna certifikatpolicy uppfyller kraven i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS Förordningen).

Informationen kan ges som en del av avtalet med beställaren eller den förlitande parten. Bruksvillkoren kan inkluderas i certifieringspraxisen så att det är lätt för läsaren att upptäcka och känna igen dem.

När det gäller avtalsvillkor för certifikat som utfärdas för allmänheten beaktas även kraven i konsumentlagstiftningen, även direktiv 93/13/EEG om oskäliga villkor i konsumentavtal.

Certifikatinnehavaren kan ladda ned ett kortläsarprogram från Myndigheten för digitalisering och befolkningsdatas webbplats. Med detta program kan medborgarcertifikatet användas för e-tjänster.

Ansökan om ett medborgarcertifikat görs enligt beskrivningen i certifieringspraxisen.

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

Medborgarcertifikat som lagrats på andra chip prissätts enligt gällande prislista för Myndigheten för digitalisering och befolkningsdatas affärsekonomiska prestationer.

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

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

För rådgivningstjänsten debiteras en särskild avgift enligt gällande prislista.

Om en tjänsteleverantör vill tillhandahålla en informationsförsörjningstjänst mellan medborgarcertifikatens 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.

Certifikatsökande får ta del av anvisningarna och bruksvillkoren i anslutning till användningen av medborgarcertifikatet innan avtalet om certifikatet ingås och beslut om utfärdande träffas, både på registreringsstället och på Myndigheten för digitalisering och befolkningsdatas webbplats.

9.3.5 Distribution av certifikat

Certifikatutfärdaren säkerställer att certifikaten ställs till förfogande för beställarna, undertecknarna och de förlitande parterna i enlighet med eIDAS Förordningen.

Datainnehållet i rotcertifikatet, certifikatutfärdarens certifikat och certifikatinnehavarens certifikat beskrivs i dokumentet FINEID S2. Dokumentet finns på utfärdarens webbplats https://dvv.fi/sv/fineid-specifikationer.

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

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

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

9.3.6 Återkallande av certifikat och avbrott i giltigheten

Certifikatutfärdaren säkerställer att certifikaten återkallas i rätt tid utifrån behöriga och bekräftade begäranden om återkallande i enlighet med eIDAS Förordningen.

Ett medborgarcertifikat kan vara i kraft i högst fem år. Certifikatet kan spärras under giltighetstiden. 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.

Certifikatinnehavaren ska omedelbart anmäla sitt medborgarcertifikat till spärrlistan om innehavaren misstänker att det uppkommit risk för att certifikatet används i strid med avtalsvillkoren eller missbrukas på annat sätt.

Certifikatinnehavaren kan begära att certifikatet spärras innan dess giltighetstid löpt ut.

Giltighetstiden för ett medborgarcertifikat kan inte avbrytas tillfälligt. Ett spärrat medborgarcertifikat kan inte tas i bruk på nytt.

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 certifikaten i strid med avtalsvillkoren ska genast anmäla certifikaten för spärrning.

Begäran om spärrning ska i första hand göras av certifikatinnehavaren, om han eller hon märker att ett certifikat har försvunnit eller om det blivit möjligt att missbruka certifikaten. Begäran om spärrning kan emellertid också göras till exempel av korttillverkaren eller registreraren.

Begäran om spärrning ska göras omedelbart när det finns anledning att misstänka missbruk av ett medborgarcertifikat som kommit bort eller stulits. Ett medborgarcertifikat kan spärras genom att man ringer det avgiftsfria numret till spärrtjänsten +358 800 162 622. Begäran om spärrning ska göras medelbart om man misstänker att det blivit möjligt att missbruka kortet.

Alla begäranden om spärrning, grunderna för spärrningen, sättet att identifiera den som gjorde begäran om spärrning och certifikatutfärdarens åtgärder med anledning av begäran arkiveras. Telefonsamtal som gäller begäranden om spärrning spelas in.

Det är i första hand certifikatinnehavaren som ska begära spärrning av ett medborgarcertifikat. Om den som ringer spärrtjänsten är en annan person än certifikatinnehavaren, ska även denne identifieras utöver certifikatinnehavaren.

En begäran om spärrning kan också göras av certifikatutfärdaren, korttillverkaren eller registreraren. Vilken metod som använts för verifieringen av den som begärde spärrning antecknas.

Grunderna och tidpunkten för spärrningen och uppgifterna om den som utförde spärrningen registreras.

En begäran om spärrning av ett medborgarcertifikat kan göras genom att man

a) ringer spärrtjänsten eller

b) besöker registreraren.

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

Om Myndigheten för digitalisering och befolkningsdata får uppgift om att en certifikatinnehavare har avlidit spärrar Myndigheten för digitalisering och befolkningsdata dennes certifikat. Myndigheten för digitalisering och befolkningsdata skickar ett meddelande om spärrningen till den avlidnes rättsinnehavare.

Myndigheten för digitalisering och befolkningsdata spärrar också certifikat ifall fel upptäcks i datainnehållet.

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 och Traficom på ändamålsenligt sätt.

Myndigheten för digitalisering och befolkningsdata kan spärra ett certifikat av särskild anledning.

Spärrningen genomförs utan fördröjelsefördjöjelse efter att begäran om spärrning har anlänt.

9.3.7 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 MDB publicera spärrlistor enligt andra intervaller och med förlängd giltighetstid.

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

Certifikatens statustjänster (OCSP och CRL) finns tillgängliga 24/7 och följer Certifikattjänsternas 99,95% SLA-krav.

9.4 Förnyelse av nyckelpar efter att ett certifikat införts på spärrlistan

De öppna nycklarna på medborgarcertifikatet och de hemliga nycklarna på chipet kan inte förnyas. För att nya nyckelpar ska kunna bildas måste en ny ansökan om medborgarcertifikat göras.

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

Datainnehållet i de spärrlistor som utfärdaren publicerar beskrivs i dokumentet FI-NEID S2. Dokumentet finns på utfärdarens webbplats https://dvv.fi/sv/.

9.5 Utfärdarens lednings- och verksamhetspraxis

9.5.1 Hantering av säkerhet

Certifikatutfärdaren säkerställer att de administrativa och affärsmässiga förfaringssätten i verksamheten är förenliga med tillbörliga och erkända standarder såsom avses i eIDAS Förordningen.

Utfärdaren sörjer för informationssäkerheten även när det gäller tjänster som köps av andra organisationer och sammanslutningar.

9.5.2 Klassificering och hantering av reserver

Certifikatutfärdaren säkerställer att nivån på skyddet av datalagren och informationen är ändamålsenlig i enlighet med eIDAS Förordningen.

Offentlig information som publiceras av Myndigheten för digitalisering och befolkningsdata i egenskap av utfärdare finns på utfärdarens webbplats. De hemliga uppgifterna i certifikatsystemet är sparade i utfärdarens eget, konfidentiella datalager. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Särskild uppmärksamhet fästs vid hanteringen av personuppgifter och Myndigheten för digitalisering och befolkningsdata har publicerat särskilda uppförandekoder för produktionen av certifikattjänster i enlighet med dataskyddslagen (1050/2018) samt i EU:s dataskyddsförordning (679/2016). Utfärdaren har även berett en dataskyddsbeskrivning i enlighet med dataskyddslagenangående hanteringen av personuppgifter i certifikatsystemet.

Uppgifterna i certifikatsystemet är hemliga, såvida de inte grundar sig på bestämmelserna om utlämnande av uppgifter i dataskyddslagen, lagen om offentlighet i myndigheternas verksamhet, lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) eller lagen om stark autentisering och betrodda elektroniska tjänster eller på ändamål som fastställts i certifikatpolicyn eller certifieringspraxisen.

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

Ett medborgarcertifikats giltighetstid har antecknats på medborgarcertifikatet. Medborgarcertifikat som spärrats under giltighetstiden publiceras på en allmänt tillgänglig spärrlista.

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

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

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

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 dataskyddslagenoch 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.

Myndigheten för digitalisering och befolkningsdatas certifikattjänster omfattas av ett system för ekonomisk förvaltning och tillsyn som föreskrivits om separat. Certifikatutfärdarens ekonomiförvaltning beskrivs detaljerat i certifieringspraxisen.

Detaljerade krav ges i standarden ISO/IEC 17799.

9.5.3 Personal och informationssäkerhet

Certifikatutfärdaren säkerställer att personalen och rekryteringspraxisen främjar och stöder en tillförlitlig verksamhet i enlighet med eIDAS Förordningen.

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare och svarar för certifikatverksamheten. Valet av leverantörer av tekniska tjänster grundar sig på ett konkurrensförfarande i anslutning till offentlig upphandling. Leverantörerna tillhandahåller tjänsterna på Myndigheten för digitalisering och befolkningsdatas ansvar och för Myndigheten för digitalisering och befolkningsdatas räkning.

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

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.

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.

Utbildningen för personalen vid Myndigheten för digitalisering och befolkningsdata planeras och genomförs så att uppgifterna kan utföras på bästa möjliga sätt. Myndigheten för digitalisering och befolkningsdata har en utbildningsplan. Myndigheten för digitalisering och befolkningsdata ansvarar för genomförandet av planen.

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.

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).

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.

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

9.5.4 Fysisk säkerhet och säkerheten i omgivningen

Certifikatutfärdaren ska säkerställa att den fysiska åtkomsten till kritiska tjänster övervakas och att de fysiska riskerna i anslutning till lagren minimeras i enlighet med eIDAS Förordningen.

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

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

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

Lokaler där produktionsmässiga 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.

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 och service för utrustning som är oumbärlig för verksamheten har säkrats.

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

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

9.5.5 Hantering av verksamheten

Certifikatutfärdaren ska säkerställa att systemen är säkra och att de används på tillbörligt sätt så att risken för störningar i verksamheten enligt eIDAS Förordningen.

Myndigheten för digitalisering och befolkningsdata anlitar tekniska tjänsteleverantörer 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.

Den som ansvarar för säkerheten hos certifikatutfärdaren leder dessa ansvarsområden, men i den praktiska verksamheten är det driftspersonalen som genomför dem under övervakning i enlighet med tillämpliga anvisningar för säkerhetsförfarandena samt de dokument som fastställer rollerna och ansvarsområdena.

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

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.

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

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 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.

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

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 informerar Traficom om granskningsresultaten såsom föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i enlighet med Traficoms föreskrifter och rekommendationer.

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

Granskningen täcker Traficoms föreskrifter om informationssäkerheten i certifikatutfärdarens verksamhet.

9.5.6 Hantering av åtkomsten till systemen

Enligt eIDAS Förordningen ska certifikatutfärdaren säkerställa att endast personer med lämplig behörighet har åtkomst till utfärdarens system.

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

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

9.5.7 Driftsättning och underhåll av pålitliga system

Certifikatutfärdaren använder pålitliga system och produkter som är skyddade mot otillåtna ändringar i enlighet med eIDAS Förordningen.

9.5.8 Hantering av kontinuiteten i affärsverksamheten och störningar

Om en nödsituation uppstår, till exempel om certifikatutfärdarens hemliga signeringsnyckel äventyras, säkerställer certifikatutfärdaren att verksamheten så snart som möjligt återställs så att den motsvarar eIDAS Förordningen.

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.

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

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.

9.5.9 Nedläggning av certifikatutfärdarens verksamhet

Certifikatutfärdaren säkerställer att eventuella störningar som orsakas beställare och förlitande parter ifall tjänster som faller under certifikatpolicyn läggs ned minimeras och att sådan information med vilken bevis om certifieringen kan läggas fram vid rättsliga förfaranden enligt eIDAS Förordningen uppdateras ständigt.

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

9.5.10 Uppfyllandet av krav som grundar sig på lag

Certifikatutfärdaren ska säkerställa att de krav som grundar sig på lag iakttas.

När det gäller avtalsvillkor för certifikat som utfärdas för allmänheten beaktas även kraven i konsumentlagstiftningen, även direktiv 93/13/EEG om oskäliga villkor i konsumentavtal.

Ett signeringscertifikat som utfärdats i enlighet med denna certifikatpolicy uppfyller kraven i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS Förordningen).

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som görs med signeringscertifikat. Om elektroniska identitetskort föreskrivs i lagen om identitetskort och om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

Myndigheten för digitalisering och befolkningsdata iakttar tillämpliga delar av skadeståndslagen (412/1974) och av kraven i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet kan ärenden hanteras med ett signeringscertifikat i alla e-tjänster som tillhandahålls av myndigheter.

Myndigheten för digitalisering och befolkningsdata iakttar god informationshantering enligt dataskyddslagen och 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 (2007/223).

Om Myndigheten för digitalisering och befolkningsdatas ställning föreskrivs i lagen om Myndigheten för digitalisering och befolkningsdata (304/2019). I Finland utövar Traficom tillsyn över dem som utfärdar signeringscertifikat.

9.5.11 Förvaring av uppgifter som gäller signeringscertifikat

Certifikatutfärdaren säkerställer att alla uppgifter som gäller ett signeringscertifikat lagras för en viss, ändamålsenlig tid, särskilt av den anledningen att man ska kunna lägga fram bevis över certifieringen vid rättsliga förfaranden enligt eIDAS Förordningen.

På arkivering av medborgarcertifikat tillämpas som allmän lagbestämmelserna i arkivlagen (831/1994). Rätten att få information bestäms enligt 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 10 år från tidpunkten då certifikaten upphört att gälla.

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

Arkivuppgifterna förvaras enligt bestämmelserna för myndigheter som agerar som utfärdare.

Uppgifterna förvaras i lokaler med hög säkerhetsnivå och passagekontroll.

Säkerhetskopior förvaras i ett annat fysiskt utrymme än originalen.

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

9.6 Krav på organisationen

Certifikatutfärdaren ska säkerställa att dess organisation är tillförlitlig så som avses i eIDAS Förordningen.

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

Ett signeringscertifikat som utfärdats i enlighet med denna certifikatpolicy uppfyller kraven i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS Förordningen).

Myndigheten för digitalisering och befolkningsdata iakttar god informationshantering enligt dataskyddslagen och 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 (2007/223).

Myndigheten för digitalisering och befolkningsdata ansvarar för att medborgarcertifikatet har skapats med iakttagande av de förfaringssätt som lagts fram i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster, lagen om stark autentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet, certifikatpolicyn och certifieringspraxisen samt i enlighet med de uppgifter som sökanden av certifikatet har uppgivit.

Beträffande behandlingen av personuppgifter iakttar Myndigheten för digitalisering och befolkningsdata dataskyddslagen. 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.

Ett utfärdat identitetskort är ett bevis på ett positivt förvaltningsbeslut. Den som är missnöjd med ett beslut får söka ändring i det genom att anföra skriftligt besvär hos förvaltningsdomstolen. En besvärsanvisning bifogas ett negativt beslut till en sökande av ett identitetskort. Besvär ska riktas till den förvaltningsdomstol inom vars domkretspolisinrättningen är belägen. Polisinrättningarna registrerar uppgifter om förvaltningsrätten i respektive område på dokumentet, om kunden önskar anföra besvär. Besvärstiden börjar löpa från den tidpunkt när besvärsanvisningen på tillbörligt sätt har fogats till beslutet och delgivits kunden.

Vid utfärdandet av medborgarcertifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att medborgarcertifikatet uppfyller de krav som ställs på det i certifikatpolicyn. Eventuella tvister avgörs enligt rättssystemet i Finland.

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

Medborgarcertifikat som lagrats på andra chip prissätts enligt gällande prislista för Myndigheten för digitalisering och befolkningsdatas affärsekonomiska prestationer.

10 Specifikationer för andra certifikatpolicyer

Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat är signeringscertifikat. Därför tillämpas denna punkt inte i samband med tillhandahållandet av medborgarcertifikat.

10.1 Hantering av certifikatpolicyn

Myndigheten för digitalisering och befolkningsdata kan ändra specifikationerna med anledning av kraven i lagstiftningen eller funktionella krav. Ändringar i specifikationerna införs i dokumenten över certifikatpolicyn och certifieringspraxisen såsom beskrivs i denna punkt.

Myndigheten för digitalisering och befolkningsdata publicerar certifikatpolicyn och certifieringspraxisen på sin webbplats och på https://dvv.fi/sv/certifikatpolicydokument.

Myndigheten för digitalisering och befolkningsdatas 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.

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för medborgarcertifikat. 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 både till Traficom och på sin egen 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.

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

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

10.2 Undantag till certifikatpolicyerna som gäller signeringscertifikat för andra än allmänheten

Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat består av ett signeringscertifikat och ett identifieringsverktyg för stark autentisering. Därför tillämpas denna punkt inte i samband med tillhandahållandet av medborgarcertifikat.

10.3 Ytterligare krav

Beställare och förlitande parter ska informeras om kravuppfyllelsen

a) ifall certifikatpolicyn inte gäller allmän användning och om undantag tillämpas

b) ifall certifikatpolicyn innehåller krav på användningen av säkra anordningar för signaturframställning

c) på vilket sätt certifikatpolicyn i fråga ökar eller skärper kraven i den certifikatpolicy som behandlats i detta dokument.

10.4 Överensstämmelse med krav

Certifikatutfärdaren får uppge att verksamheten är förenlig med detta dokument och certifikatpolicyn bara om certifikatutfärdaren uttrycker att den aktuella certifikatpolicyn följs och på beställarens eller de förlitande parternas begäran kan redogöra för överensstämmelsen med kraven.

Redogörelsen kan till exempel vara en granskningsberättelse där granskaren försäkrar att utfärdaren iakttar kraven i en viss certifikatpolicy. Det kan handla om en intern granskare som hör till utfärdarens organisation, men granskaren får inte vara över- eller underordnad den avdelning som driver utfärdarens verksamhet.