MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIKATPOLICY SOCIAL HÄLSO YRKESCERTIFIKAT

för yrkescertifikat för social- och hälsovården

OID: 1.2.246.517.1.10.206

23.9.2022

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Dokumenthantering

Ägare	
Utarbetats av	Tuire Saaripuu
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Godkänd version 1.0., dokument förenligt med eIDAS-förordningen	3.5.2018/TS
v 1.1	Godkänd version 1.1, Befolkningsregistercentralens namnbyte	1.1.2020/TS
v 1.2	Uppdaterad version, tillgänglighetsegenskaper, namnändring av lagen 661/2009	6.5.2021
v 1.3	Tillagd information om loggdata	1.10.2021/VA
v 1.4	Uppdaterade versionen och länkarna till CPS dokument	23.9.2022/SK

Innehållsförteckning

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.

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.

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

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

Ett yrkescertifikat består av ett certifikatpar som har två särskilda användningsändamål: ett autentiserings- och krypteringscertifikat och ett signeringscertifikat som är förenligt med lagen om stark autentisering och betrodda elektroniska tjänster.

1 Tillämpning

I detta dokument fastställs de krav på förfarande som gäller certifikatutfärdare som utfärdar signeringscertifikat. Kraven ställs på verksamheten och förvaltningspraxisen hos dem som utfärdar signeringscertifikat 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.

I kraven på förfaringssätt:

a) Två till varandra nära knutna signeringscertifikatpolicyer specificeras för signeringscertifikat som utfärdas för allmänheten; den ena certifikatpolicyn förutsätter användning av en säker anordning för signaturframställning.

b) Specifikationsramar läggs fram för sådana signeringscertifikatpolicyer som förbättrar ovan nämnda förfaringssätt för certifikat eller som gäller signeringscertifikat som utfärdas för andra användargrupper än sådana som betraktas höra till allmänheten.

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 ges inga krav på utfärdarcertifikat, inte heller på relationen mellan 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 certifikat som utfärdas för allmänheten och som används för att stöda elektroniska signaturer.

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.

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

2 Referensförteckning

I detta dokument hänvisas 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 som knyter an 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:

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.

***ETSI* 8 Draft ETSI EN 319 411-2 V2.0.6 (2015-06)**

[ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

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

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

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

[Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider

Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Termbeskrivningar:

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].

3 Definitioner och förkortningar

3.1 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).

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 autentisering 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.

Rätt att utöva yrke: Med rätt att utöva yrke avses i denna certifikatpolicy rätt att utöva yrke som en legitimerad yrkesutbildad person, en yrkesutbildad person som beviljats tillstånd eller en yrkesutbildad person med skyddad yrkesbeteckning samt yrkesmässiga rättigheter för en studerande inom hälso- och sjukvården som en person kan få med stöd av 2 § i lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994). Rätten att utöva yrket kan vara obegränsad, begränsad eller frånta-gen i sin helhet. Rätten att utöva yrke inom hälso- och sjukvården registreras i Terhikki, ett register som förs av Tillstånds- och tillsynsverket för social- och hälsovården. Med rätt att utöva yrke avses i denna certifikatpolicy även en yrkesutbildad person inom socialvården som uppfyller behörighetsvillkoren enlig lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005).

Yrkescertifikat: Certifikatpar som Myndigheten för digitalisering och befolkningsdata utfärdat för en fysisk person. Specificeras längre fram i dokumentet.

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 är öppen och den andra hemlig. Ändamålet med nycklarna har fastställts på certifikatet (se certifikatinnehavarens signeringscertifikat samt autentiserings- och krypteringscertifikat).

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

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

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

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

Avancerad elektronisk signatur: en elektronisk signatur som uppfyller följande krav: den är entydigt knuten

a) 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.

Signeringscertifikat: ett certifikat som uppfyller kraven i Förordningen. Datainnehållet i signeringscertifikatet har fastställts i lagen om stark autentisering och betrodda elektroniska tjänster.

Signeringscertifikatpolicy: certifikatpolicy i vilken ingår de krav som föreskrivs i Förordningen.

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 bank-, 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.

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

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

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

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

Registreringsnummer: Registreringsnumret är en teknisk sifferserie som genereras för alla yrkesutbildade personer inom hälso- och sjukvården som registrerar sig eller redan har registrerat sig i centralregistret över yrkesutbildade personer inom hälso- och sjukvården, Terhikki. Registreringsnumret används bland annat för att identifiera yrkesutbildade personer till exempel i elektroniska recept.

Registreringsställe: Serviceställe där man kontrollerar identiteten hos den som ansöker om ett certifikat och att personen har rätt att utöva yrket. Registreringsstället ansvarar för distributionen av yrkeskort, certifikat och PIN-/PUK-koder till användarna i enlighet med certifikatpolicyn och certifieringspraxisen.

RSA-algoritm och RSA-nyckel: RSA-algoritmen är en allmänt använd öppen nyckelalgoritm. Hemliga och öppna nycklar i anslutning till yrkescertifikat är RSA-nycklar.

Yrkesutbildad person inom social- och hälsovården: En person som med stöd av lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994) har erhållit rätt att utöva yrke (legitimerad yrkesutbildad person) eller tillstånd att utöva yrke (yrkesutbildad person som beviljats tillstånd) eller en person som med stöd av nämnda lag har rätt att använda i förordning av statsrådet avsedd yrkesbeteckning för en yrkesutbildad person inom hälso- och sjukvården (yrkesutbildad person med skyddad yrkesbeteckning) och som registrerat sig i centralregistret över yrkesutbildade personer inom hälso- och sjukvården samt en person som uppfyller i kraven i lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005).

Tillstånds- och tillsynsverket för social- och hälsovården (Valvira): Valvira är tillstånds- och tillsynsmyndighet för social- och hälsovården. Genom styrning och övervakning förbättrar Valvira hanteringen av hälsoriskerna i livsmiljön, verkställandet av rättsskyddet och kvaliteten på tjänsterna inom social- och hälsovården. Till Valviras

uppgifter hör vidare att överaka att anordningar och förnödenheter inom social- och hälsovården överensstämmer med kraven samt att främja en säker användning av dem.

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

Spärrtjänst: Teknisk leverantör som för certifikatutfärdarens räkning tar emot och förmedlar begäranden om spärrning av certifikat till certifikatsystemet.

Elektronisk signatur: En 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.

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

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

Annan personal inom social- och hälsovården: Annan person som arbetar på en verksamhetsenhet inom social- och hälsovården eller som utför en sådan persons uppgifter, och som inte är en yrkesutbildad person inom social- och hälsovården.

Tillhandahållare av tjänster inom social- och hälsovården: en verksamhetsenhet inom social- och hälsovården eller en yrkesutbildad person som arbetar som självständig yrkesutövare.

Aktörskort för social- och hälsovården: Ett aktivkort som innehåller ett certifikat som utfärdats för en annan aktör inom social- och hälsovården.

Terhikki-registret: Ett rikstäckande register över yrkesutbildade personer inom hälso- och sjukvården och deras rätter att utöva yrke som Valvira för i enlighet med lagen om yrkesutbildade personer inom hälso- och sjukvården /559/1994).

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

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.

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

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

Certifikatbeskrivning: Dokumentet innehåller de centrala delarna av 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. 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.

Mer information om den inbördes relationen mellan certifikatpolicyer och certifieringspraxisen ges i 4.3.

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

Certifikatregister: Ett register som 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 utgörs av certifikatsystem, datatrafik, certifikatregister och spärrlista, rådgivnings- och spärrtjänst samt hantering 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: Certifikatutfärdande organisation som svarar för produktionen av certifikat samt utarbetar certifikatpolicy och certifieringspraxis som beskriver organisationens verksamhet. En eller flera parter kan förlita sig på utfärdarens verksamhet. Utfärdare är den tillhandahållare av certifikattjänster som utfärdar certifikat. Den mer exakta beskrivningen grundar sig på ITU-T:s rekommendation X.509. Begreppet certifikatutfärdare förtydligas i punkt 4.2.

Certifikatutfärdarens certifikat (utfärdarcertifikatet): 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 yrkescertifikat 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: Aktör som beställer en tjänst av utfärdaren för en eller flera undertecknares räkning. Undertecknaren kan vara en beställare som agerar för egen räkning.

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

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

3.2 Förkortningar

ISO 27001	ISO IEC 27001
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
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
PUK	PIN Unblocking Key, PUK-kod
QCP	Qualified Certificate Policy: signeringscertifikatpolicy
RSA	Rivest, Shamir, Adleman, RSA-kod, en algoritm för den öppna nyckeln, en asymetrisk algoritm
SATU	Elektronisk kommunikationskod
SIM	Subscriber Identity Module
SSCD	Secure Signature Creation Device: Säker anordning för signaturframställning
MDB	Myndigheten för digitalisering och befolkningsdata

4 Allmänna begrepp

4.1 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 4.2. 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 de certifikat som utfärdas för allmänheten.

Certifikatutfärdaren är en tillhandahållare av certifikattjänster som avses i Förordningen.

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

Myndigheten för digitalisering och befolkningsdata (MDB) hör till finansministeriets förvaltningsområde. MDB är en myndighet som upprätthåller personregister. Enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster 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 och sedan 1.4.2015 för socialvården till följd av de ändringar som gjordes i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården. (lag om elektronisk behandling av klientuppgifter inom social- och hälsovården, lag om elektroniska recept och lag om yrkesutbildade personer inom hälso- och sjukvården). 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.

I detta dokument fastställs kraven på förfaranden som gäller utfärdare av signeringscertifikat samt Myndigheten för digitalisering och befolkningsdata i egenskap av tillhandahållare 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.

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.

Om identitetskort föreskrivs i lagen om identitetskort (829/1999) och om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster.

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 yrkescertifikat har registrerats av Myndigheten för digitalisering och befolkningsdata.

Denna certifikatpolicy beskriver de detaljerade kraven på utfärdandet och produktionen av signeringscertifikat, vilka grundar sig på Förordningen och är förenliga med lagen om stark autentisering och elektroniska betrodda tjänster, samt de detaljerade kraven på ansvarsfördelningen vid utfärdandet och produktionen.

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 yrkescertifikat och är förenligt med lagen om stark autentisering och elektroniska betrodda tjänster.

Ett yrkescertifikat består av ett certifikatpar som har två särskilda användningsändamål. Autentiserings- och krypteringscertifikatet 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.

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

4.2 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 befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster.

Ett yrkescertifikat 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 yrkescertifikat 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 de yrkescertifikat 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 yrkescertifikat 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 yrkescertifikat 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. Uppgifter om ett certifikats giltighet fås även via en OCSP-tjänst.

- **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.

Förlitande part: En förlitande part är en person eller en organisation som litar på innehållet i certifikatet och som använder certifikatet för att autentisering, kryptering och elektroniska signaturer. En förlitande part ska kontrollera att det certifikat som används är i kraft. Detta kan göras genom att man kontrollerar certifikatets status antingen i en OCSP-tjänst eller kontrolleraratt certifikatet inte finns på spärrlistan.

4.3 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.

4.3.1 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 som föreskrivits i Förordningen och i den nationella lagstiftningen. 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 yrkescertifikat. Certifikatinnehavare och förlitande parter bör handla i enlighet med denna certifikatpolicy.

Yrkescertifikat som är förenliga med denna certifikatpolicy kan användas för stark autentisering av en person, kryptering av information och för elektroniska signaturer. Yrkescertifikat 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.

4.3.2 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 befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster har Myndigheten för digitalisering och befolkningsdata till uppgift att producera tjänster inom certifierad elektronisk kommunikation.

4.3.3 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.

4.3.4 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 yrkescertifikat har nämns i ansökningshandlingen och i den allmänna bruksanvisningen som ges innan ansökan om yrkescertifikat undertecknas. Ansökan och bruksanvisningen utgör avtalet med den som ansöker om yrkescertifikat. Den organisation som ansöker om yrkescertifikat ansöker om certifikat för sina egna medlemmar. Dessa identifieras på ett personligt sätt vid ansökan. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter. Den som ansöker om ett yrkescertifikat godkänner de allmänna bruksvillkoren i samband med ansökan.

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

4.4 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.

Sökanden, dvs. organisationen ansöker om yrkescertifikat för sina medlemmar. Dessa är fysiska personer som identifierats på ett personligt sätt.

5 Inledning till certifikatpolicyer för signeringscertifikat

5.1 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 som är förenliga med Förordningen. Därför kallas dessa dokument signeringscertifikatpolicyer.

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 två signeringscertifikatpolicyer:

1. certifikatpolicy för signeringscertifikat som utfärdas för allmänheten, där 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.

2. Signeringscertifikatpolicy för signeringscertifikat som utfärdas för allmänheten.

I punkt 8 behandlas specifikationsförutsättningarna för andra signeringscertifikatpolicyer,

a) vilka effektiviserar eller begränsar ovan nämnda policyer och/eller

b) vilka eventuellt gäller signeringscertifikat för andra än allmänheten.

De principer som tillämpas här definieras i publikationerna RFC 3647 och ANSI X9.79. I detta dokument eftersträvas så stor överensstämmelse som möjligt med principerna och kraven i ovan nämnda dokument.

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 yrkescertifikat för social- och hälsovården, OID 1.2.246.517.1.10.206.

Certifikatpolicyn hänvisar till certifikatutfärdarens certifikatpolicy, OID 1.2.246.517.1.10.201.

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

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

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

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 för certifikatförvaltning vid Myndigheten för digitalisering och befolkningsdata besvarar frågor som gäller certifikatpolicyn och ansvarar för 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 yrkescertifikaten och dokumentationen i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata äger samtliga ägande- och användarrättigheter för denna certifikatpolicy.

5.2 Identifieringskoder

OID-identifierarna för de signeringscertifikatpolicyer som behandlas i detta dokument är de som följer:

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

Ett signeringscertifikat som utfärdats enligt denna policy uppfyller de krav som ställs på kvalificerade signeringscertifikat i Förordningen. Graden av tillförlitlighet på autentiseringscertifikatet är "hög" enligt Förordningen och i förordningen om tillitsnivåer som utfärdats med stöd av Förordningen.

I lagen om stark autentisering och betrodda elektroniska tjänster föreskrivs om betrodda tjänster som utförs med signeringscertifikat. Om elektroniska identitetskort föreskrivs i lagen om identitetskort och om certifikat utfärdade av Myndigheten för digitalisering och befolkningsdata i lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster.

Certifikatpolicyn träder i kraft 1.1.2020.

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.

5.3 Användarkrets och tillämpbarhet

5.3.1 Certifikatpolicyn för QCP/QSCD

Denna certifikatpolicy gäller certifikat

a) som uppfyller kraven i Förordningen

b) vars utfärdare uppfyller kraven i Förordningen

c) som utfärdas för allmänheten.

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

5.4 Överensstämmelse med krav

5.4.1 Allmänt

Certifikatutfärdaren har rätt att använda identifieraren för certifikatpolicyn bara

a) om certifikatutfärdaren uttrycker att den aktuella signeringscertifikatpolicyn följs och på beställarens eller de förlitande parternas begäran kan redogöra för överensstämmelsen med kraven.

b) om en behörig och oberoende part inom den senaste tiden har bedömt uppfyllandet av kraven i den specifika signeringscertifikatpolicyn hos utfärdaren.

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.

5.4.2 Certifikatpolicyn för QCP/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 kraven.

6 Skyldigheter och ansvar samt begränsningar av ansvaret

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

6.1 Certifikatutfärdarens skyldigheter

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

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

Certifikatutfärdaren tillhandahåller alla delområden av certifikattjänsten i enlighet med certifieringspraxisen.

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

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 yrkescertifikat liksom andra aspekter på användningen av organisationscertifikat 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 yrkescertifikat 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.

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.

6.2 Skyldigheter för den som ansöker om certifikat

Certifikatutfärdaren ålägger genom avtal sökanden att iaktta alla nedan nämnda skyldigheter (se 7.3.1, underpunkt i). Om undertecknaren och sökanden är olika aktörer ska beställaren informera undertecknaren om alla skyldigheter som gäller denne enligt förteckningen nedan:

a) Riktiga och fullständiga uppgifter ska lämnas till certifikatutfärdaren i enlighet med kraven i signeringscertifikatpolicyn, särskilt i samband med registreringen.

b) Ett nyckelpar får bara användas för elektroniska signaturer och i enlighet med eventuella begränsningar som meddelats beställaren (se 7.3.4).

c) Certifikatinnehavaren ska i sin verksamhet iaktta särskild omsorgsfullhet för att undertecknarens hemliga nyckel inte kan användas utan lov.

d) Om certifikatsökanden skapar undertecknarens nycklar:

   a. undertecknarens nycklar ska skapas med en algoritm som konstaterats lämplig för elektroniska signaturer
   b. som nyckellängd och algoritm ska användas en kombination som konstaterats lämpa sig för elektroniska signaturer under certifikatets giltighetstid.

Algoritmer och specifikationer och anvisningar beträffande deras parametrar har publicerats i dokumentet TS 102 176-1.

c. Undertecknaren kan ensam övervaka sin hemliga nyckel.

e) Om certifikatpolicyn förutsätter användning av en säker anordning för signaturframställning (dvs. signeringscertifikatpolitiken QCP public + SSCD tillämpas) får certifikatet bara användas i anslutning till elektroniska signaturer som skapats med en sådan anordning.

Ovan nämnda krav gäller inte signeringscertifikatpolitiken QCP public.

f) Om en utfärdare har utfärdat ett certifikat i enlighet med certifikatpolicyn QCP public + SSCD och undertecknarens nycklar skapas under övervakning av beställaren eller undertecknaren, ska undertecknarens nycklar skapas med en säker anordning för signaturframställning.

Ovan nämnda krav gäller inte signeringscertifikatpolitiken QCP public.

g) Certifikatutfärdaren ska underrättas utan skäligt dröjsmål om något av följande inträffar innan den på certifikatet meddelade giltighetstiden går ut:

a. Undertecknarens hemliga nyckel har försvunnit eller det har blivit omöjligt att använda den (till exempel om undertecknaren har glömt sin PIN-kod), den hemliga nyckeln har stulits, råkat i fel händer eller

b. Användningen av undertecknarens hemliga nyckel kan inte längre kontrolleras eftersom aktiveringsuppgifterna (till exempel PIN-koden) har råkat i fel händer eller av någon annan orsak, och/eller

c. Certifikatets innehåll stämmer inte med det som meddelats beställaren eller undertecknaren, eller innehållet har ändrats.

h) Om undertecknarens hemliga nyckel har råkat i fel händer ska den återkallas omedelbart och slutgiltigt.

Om verksamheten hos den som utfärdade undertecknarens certifikat har äventyrats ska det säkerställas att undertecknaren inte använder certifikatet.

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

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

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

Innehavaren av yrkescertifikatet 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 yrkescertifikatet.

Organisationscertifikatet 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 yrkescertifikatet 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.

6.3 Information till de förlitande parterna

I de instruktioner som ges förlitande parter (se 7.3.4) ska det förklaras att parterna – för att kunna lita på certifikatet – förutsätts

a) verifiera med hjälp av en aktuell uppgift om spärrstatusen (se 7.3.4) att certifikatet är i kraft och inte har försatts i avbrottsläge eller återkallats. Beroende på certifikatutfärdarens praxis och sättet att distribuera information om spärrstatus kan det förekomma dröjsmål i informationen, dock högst med en (1) dag.

b) beakta eventuella begränsningar i användningen av certifikatet; om dessa informeras den förlitande parten på certifikatet eller i bruksvillkor som tillhandahållits enligt punkt 7.3.4

c) Iaktta villkoren som specificerats i avtal eller på annat sätt.

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

Yrkescertifikats identifikationscertifikat publiceras i ett offentligt register som är allmänt tillgänglig. Spärrade organisationscertifikat publiceras på en spärrlista. De förlitande parterna ska kontrollera mot spärrlistan att ett yrkescertifikat är giltigt.

Den förlitande parten är skyldig att säkerställa att certifikatet används i enlighet med användningsändamålet. Ett signeringscertifikat kan bara användas för elektroniska signaturer. För ett autentiserings- och krypteringscertifikat 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 ett yrkescertifikat efter att parten kontrollerat att **yrkescertifikatet är i kraft och inte finns på spärrlistan**. En part som förlitar sig på ett yrkescertifikat är skyldig att kontrollera certifikatet med hjälp av en spärrlista eller via en OCSP-tjänst. För att säkerställa tillförlitligheten hos yrkescertifikatet ska den förlitande parten utföra åtgärderna för att kontrollera yrkescertifikatets status.

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

6.4 Ansvar

Det ansvar som fastställs i 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.

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 yrkescertifikatet 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 yrkescertifikatet.

Myndigheten för digitalisering och befolkningsdata ansvarar för att yrkescertifikatet kan användas från tidpunkten från överlåtelsen till giltighetstidens utgång – förutsatt att det inte har införts på spärrlistan. Yrkescertifikatet överlåts till en person som identifierats på det sätt som förutsätts vid yrkescertifikat. Före undertecknandet av avtalet har certifikatinnehavaren fått bruksanvisningar för yrkescertifikatet.

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

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

Registrerarens ansvar

Registreraren av yrkescertifikat 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 yrkescertifikatet placeras på ett identitetskort – lagen om identitetskort.

Certifikatinnehavarens ansvar

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

Innehavaren av yrkescertifikatet 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 yrkescertifikatet. När en terminalsession avslutas eller terminalen lämnas utan tillsyn ska certifikatinnehavaren avlägsna chipet med yrkescertifikatet 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 yrkescertifikatet 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.

Den förlitande partens ansvar

En part som förlitar sig på ett yrkescertifikat kan inte i god tro lita på certifikatet och på att en elektronisk signatur är riktig ifall parten inte har kontrollerat att yrkescertifikatet är i kraft, Om yrkescertifikatet godkänns i en sådan situation frias Myndigheten för digitalisering och befolkningsdata från ansvar. Den förlitande parten ska kontrollera att det utfärdade certifikatet motsvarar användningsändamålet i den rättshandling där det används.

Begränsning av ansvar

Myndigheten för digitalisering och befolkningsdata ansvarar inte för eventuella skador som orsakas av att PIN-koden, 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 yrkescertifikatet 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 innehavaren av yrkescertifikatet.

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. Innehavare av yrkescertifikat eller förlitande parter ska i sådana fall svara för egna kostnaderna som följer av detta och utfärdaren är inte skyldig att ersätta tinnehavare 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 yrkescertifikatet eller för kostnaderna för detta fel.

Övriga parter

Förlitande parter kan lita på att yrkescertifikat eller elektroniska signaturer är korrekta efter att ha kontrollerat med en OCSP-tjänst att certifikatet är i kraft, att det inte har upptagits på någon spärrlista och att certifikatets giltighetstid inte har gått ut, och när det inte föreligger andra skäl att misstänka att certifikatet inte används korrekt.

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

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

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.

7 Krav på certifikatutfärdarens verksamhet

Denna punkt tillämpas på båda signeringscertifikatpolicyerna som specificerades i punkt 5 – QCP public- och QCP public + SSCD – om inte annat nämns separat.

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 (punkt 4.2). 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.

7.1 Certifieringspraxis

Certifikatutfärdaren intygar att tillhandahållandet av certifikattjänsterna uppfyller kraven på pålitlighet.

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

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

7.2.1 Skapande av certifikatutfärdarens nyckel

Inom en ändamålsenlig tid innan certifikatutfärdarens signeringsnyckel upphör att gälla 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.

7.2.2 Lagring, säkerhetskopiering och återställande av certifikatutfärdarens nyckel

Lagring av nycklar

Certifikatutfärdaren säkerställer att certifikatutfärdarens hemliga nycklar är fortsatt konfidentiella och intakta i enlighet med 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 ser till att utfärdarens hemliga nycklar inte kan röjas eller missbrukas.

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 yrkescertifikat tas inga kopior.

7.2.3 Distribution av certifikatutfärdarens öppna nyckel

Distribution av certifikat

Certifikatutfärdaren säkerställer att certifikatutfärdarens (öppna) nyckel som används för verifiering av signaturen samt de relaterade parametrarna hålls intakta och autentiska under distributionen till de förlitande parterna i enlighet med Förordningen.

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

Utfärdaren arkiverar alla certifierade öppna nycklar.

7.2.4 System med reservnyckel

Undertecknarens hemliga signeringsnycklar förvaras inte på ett sätt som möjliggör dekryptering och säkerhetskopiering, varvid de befullmäktigade instanserna i vissa fall skulle kunna dekryptera nycklar genom att använda uppgifter lämnade av en eller flera parter.

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

7.2.5 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 S2-specifikationerna.

7.2.6 När certifikatutfärdarens nyckel går ut

Certifikatutfärdaren säkerställer att de hemliga signeringsnycklarna inte används efter att deras livscykel är till ända.

Myndigheten för digitalisering och befolkningsdata gör inga nycklar av de hemliga signeringsnycklarna.

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

Certifikatutfärdaren säkerställer att krypteringsutrustningen är säker under hela dess livscykel.

7.2.8 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.

Skapande av certifikat

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

Certifikatinnehavarens hemliga och öppna nycklar är minst 2048-bitars RSA-nycklar.

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

Certifikatutfärdarens certifikat:

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

Certifikatinnehavarens autentiserings- och krypteringscertifikat:

Ändamål: Verifiering av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signeringscertifikat:

Ändamål: Elektroniska signaturer

7.3 Säker anordning för signaturframställning

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.

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

7.4.1 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.

När en certifikatutfärdare utfärdar ett yrkescertifikat är det samtidigt ett godkännande av certifikatansökan. Utfärdaren ansvarar vid utfärdandet av yrkescertifikatet för att datainnehållet i certifikatet är riktigt vid tidpunkten för överlåtelsen av certifikatet.

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

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

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

Yrkescertifikat kan hämtas personligen från registreringsstället.

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

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

Korttillverkaren skapar aktiveringsuppgifterna som behövs för nycklarna, dvs. PIN-koderna.

PIN-koderna 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 PIN- och PUK-koder som behövs för att man ska kunna använda yrkescertifikatet 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 yrkescertifikatet användas för e-tjänster.

Innehavaren av ett yrkescertifikat informeras om möjligheten att byta de ursprungliga PIN-koderna till nya koder. Ett gratisprogram för byte av PIN-koder finns på https://dvv.fi/sv/.

Rättigheterna och skyldigheterna för den som ansöker om ett yrkescertifikat ingår i ansökningsdokumentet och i de allmänna bruksvillkoren, som utgör avtalet som ingås med sökanden.

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

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

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

En certifikatinnehavare som misstänker att det blivit möjligt att använda yrkescertifikatet i strid med avtalsvillkoren ska genast anmäla certifikaten för spärrning.

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

De hemliga nycklarna i anslutning till yrkescertifikatet som skapats på ett chip eller i en annan säker miljö levereras till innehavaren i samband med överlåtelsen. Det finns inga kopior av de hemliga signeringsnycklarna på chipet och sådana kan inte heller göras i ett senare skede.

I detta kapitel behandlas förfaringssätten för identifiering och autentisering av personer under processen för beställning av certifikat.

Hur en yrkesutbildad person inom social- och hälsovården benämns på autentiseringscertifikatet och signeringscertifikatet beskrivs i specifikationen THPKI - T2 (Väestörekisterikeskuksen CA-malli ja varmenteiden tietosisältö sosiaali- ja terveydenhuollossa).

För en Innehavare av ett certifikat för hälso- och sjukvården används det för- och efternamn som registrerats för den fysiska personen i Terhikki-registret.

Gruppen av attribut som bildar objektets namnpost i certifikatet är unik och individualiserar den yrkesutbildade personen i fråga. Registreringsnumret ges av Valvira, som upprätthåller Terhikki-registret. Alla yrkesutbildade personer inom social- och hälsovården ska agera i eget namn.

Certifikatutfärdaren utfärdar inga anonyma certifikat.

Den specificerade namnposten identifierar den yrkesutbildade personen. Personens identifieringskod är unik och individuell.

De hemliganycklarna för yrkesutbildade personer inom social- och hälsovården skapas alltid på yrkeskortets chip. Yrkeskortet, som innehåller de hemliga nycklarna, överlåts till certifikatinnehavarna efter att identiteten har verifierats på ett tillförlitligt sätt och certifikatet har skapats och registrerats.

När det gäller yrkesutbildade personer inom social- och hälsovården krävs ingen verifiering av de organisationer som de företräder. Yrkesutbildade personer inom social- och hälsovården kan arbeta på flera olika verksamhetsenheter och således är varken yrkescertifikatet eller yrkeskortet organisationsbundna.

Vid ansökan om certifikat kontrolleras identiteten med hjälp av en giltig, av polisen utfärdad identitetshandling, dvs. identitetskort eller pass, eller ett körkort som utfärdats efter 1.10.1990. Godtagbara identifieringshandlingar är också ett giltigt pass eller identitetskort som utfärdats av myndighet i en medlemsstat inom EES, Schweiz eller San Marino, ett giltigt körkort som utfärdats efter 1.10.1990 av myndighet i en medlemsstat inom EES och ett giltigt pass som utfärdats av en myndighet i någon annan stat. Om sökanden inte har nämnda handlingar ska polisen kontrollera sökandens identitet på annat sätt.

En inom socialvården yrkesutbildad persons rätt att utöva yrket kontrolleras i enlighet med Valviras vid var tid gällande anvisningar. När centralregistret över yrkesutbildade personer inom socialvården blir klart och rikstäckande, ska rätten att utöva yrke kontrolleras mot detta register.

Att en yrkesutbildad person inom hälso- och sjukvården har en gällande rätt att utöva yrket kontrolleras med hjälp av Valviras centralregister över yrkesutbildade personer inom hälso- och sjukvården (Terhikki). På ett yrkescertifikat och yrkeskort för hälso- och sjukvården antecknas bara en rätt att utöva yrke, ifall sökanden har flera giltiga yrkesrättigheter. Om rätten att utöva yrket inte finns registrerad i Terhikki, utfärdas inget certifikat.

Om en yrkesutbildad persons uppgifter inte har registrerats i Terhikki bör personen kontakta Valvira för registreringen av yrkesrättigheterna.

Alla personuppgifter som behövs för ansökan om certifikat för en yrkesutbildad person inom hälso- och sjukvården grundar sig på Terhikki-registret.

Bara yrkesutbildade personer inom hälso- och sjukvården som är registrerade hos Valvira har rätt att ansöka om yrkescertifikat. Sökanden ska ha en giltig rätt att utöva ett yrke för att yrkescertifikatet ska kunna utfärdas. Eventuella begränsningar i anslutning till rätten att utöva yrke utgör inget hinder för utfärdandet av certifikatet.

Förutsättningarna för och kraven på samarbetet mellan olika certifikatutfärdare definieras i rotcertifikatutfärdarens certifikatpolicy.

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

Vid utfärdandet av ett nytt certifikat iakttas samma rutiner som vid första ansökan om certifikat.

Ansökan om ett yrkescertifikat inom social- och hälsovården förutsätter ett personligt besök hos en organisation som fungerar som registrerare.

Uppgifterna i ansökan registreras i certifikatutfärdarens certifikatdatasystem.

Ansökan om ett yrkescertifikat för social- och hälsovården förutsätter att sökanden:

- Intygar sin identitet på det sätt som redogjorts för i kapitel 3
- lägger fram sina personuppgifter enligt det som beskrivits i kapitel 3.2.3
- undertecknar ansökningsformuläret.

Registreraren meddelar sökanden hur yrkeskortet och kuvertet med PIN-koden kommer att levereras.

Certifikatansökan kan göras av en yrkesutbildad person inom hälso- och sjukvården som registrerats hos Valvira. En yrkesutbildad person inom socialvården kan göra ansökan enligt Valviras vid var tid gällande anvisningar tills dess att centralregistret för yrkesutbildade personer inom socialvården är klart och i bruk.

Registreringen av uppgifterna om certifikatet som ska utfärdas och det relaterade yrkeskortet sker med ett system som säkerställer integriteten i uppgifterna.

Datakommunikationsförbindelserna mellan certifikatutfärdarens datasystem är skyddade. Personer som använder certifikatdatasystemet identifieras med hjälp av certifikatkort utfärdade av certifikatutfärdaren. Datainnehållet i ett certifikat uppkommer av de uppgifter som lämnades på ansökan.

Registreraren utfärdar certifikatet när registreraren och sökanden har kontrollerat och med sin underskrift godkänt uppgifterna på ansökan.

Certifikatutfärdaren levererar följande till sökanden:

- ett enligt sökandens uppgifter specificerat yrkeskort som innehåller kortinnehavarens hemliga nyckelpar och certifikat
- ett kuvert som innehåller de hemliga PIN- och PUK-koder som behövs för användningen av yrkeskortet.

Dessutom ger registreraren certifikatsökanden en bruksanvisning för yrkeskortet.

Registrerarens ansvar i anslutning till utfärdandet behandlades i kapitel 1.3.2.

Certifikatansökan handläggs på registreringsstället utan obefogat dröjsmål.

Registreraren inför beställningsuppgifterna i certifikatutfärdarens certifikatdatasystem.

Registreraren identifierar sökanden i enlighet med kapitel 3 och kontrollerar att en uppgift om sökandens rätt att utöva yrke finns i Terhikki-registret. Uppgifterna för ansökningsformuläret fås från Terhikki-registret och befolkningsdatasystemet. I ansökan nämns det tilltalsnamn som sökanden uppgett att ska införas på certifikatet samt den yrkesrättighet som finns upptagen i Terhikki-registret. Utöver dessa uppgifter fyller

registreraren i de uppgifter som behövs för produktionen och leveransen av certifikatet samt vilken identifieringshandling som användes för att identifiera sökanden.

En ansökan om yrkescertifikat godkänns i och med utfärdandet av certifikatet. Om förutsättningar för att utfärda certifikatet saknas för sökandens del, kan certifikatet inte utfärdas och ansökan avslås. Sökanden delges beslutet omedelbart och sökanden kan då göra en skriftlig yrkan på ändring av beslutet som riktas till certifikatutfärdaren.

En certifikatansökan handläggs utan obefogat dröjsmål under registreringsställets öppethållningstider. Om utfärdandet av ett yrkescertifikat för social- och hälsovården ges inget separat meddelande.

Tjänstemannen på registreringsstället startar processen för utfärdandet av certifikatet. För att tjänstemannen ska kunna använda certifikatsystemet förutsätts stark autentisering. Tjänstemannens åtgärder sparas i en logg i certifikatutfärdarens datasystem.

Det förutsätts att certifikatinnehavaren kontrollerar att kort- och certifikatuppgifterna är korrekta. För att godkänna ett utfärdat certifikat behöver innehavaren inte vidta några andra åtgärder. Om problem uppstår bör certifikatinnehavaren kontakta registreringsstället eller stödtjänsten,

Certifikatutfärdaren publicerar utfärdade autentiseringscertifikat i ett certifikatregister som finns i ett offentligt datanät. Signeringscertifikat publiceras inte i register.

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

Certifikatutfärdaren säkerställer att begäranden om certifikat som ska utfärdas för en tidigare registrerad undertecknare är fullständiga, korrekta och behöriga. Begärandena kan gälla förnyelse av certifikat, byte av nyckelpar efter ett återkallande eller innan giltighetstiden går ut samt uppdatering som beror på att undertecknarens attribut har ändrats.

Ett certifikat för en yrkesutbildad person inom social- och hälsovården kan förnyas när det föregående certifikatet går ut, om förutsättningarna för utfärdande fortfarande gäller.

Certifikatet kan också förnyas om uppgifterna om rätt att utöva yrke eller andra uppgifter som påverkar certifikatets datainnehåll har ändrats eller om yrkeskortet har gått sönder. Då bör certifikatinnehavaren kontakta registreringsstället och ansöka om ett nytt yrkeskort och ett nytt yrkescertifikat.

Endast certifikatinnehavaren kan ansöka om förnyelse av certifikatet.

Vid förnyelse av certifikat, förfarandet för godkännande och publiceringen av certifikatet iakttas samma rutiner som vid första ansökan om certifikat.

Om förnyelse av ett yrkescertifikat för social- och hälsovården ges inget separat meddelande.

7.4.3 Skapande av certifikat

Certifikatutfärdaren säkerställer att certifikaten utfärdas säkert så att deras autenticitet bevaras.

Certifikatinnehavarnas hemliga nycklar skapas säkert på ett sätt som uppfyller kraven på yrkescertifikat. 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.

7.4.4 Distribution av bruksvillkor

Utfärdaren säkerställer att bruksvillkoren och -anvisningarna ställs till förfogande för beställarna och de förlitande parterna.

Ett signeringscertifikat som utfärdats enligt denna policy uppfyller de krav som ställs i Förordningen.

Informationen kan ges som en del av avtalet med certifikatsökanden 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 yrkescertifikatet användas för e-tjänster.

Ansökan om ett yrkescertifikat görs enligt beskrivningen i certifieringspraxisen.

Certifikat 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 yrkescertifikaten, spärrlistan eller det offentliga registret. Enskilda tillhandahållare

av e-tjänster kan debitera för användningen av sin egen tjänst. Användningen av yrkescertifikat förutsätter ingen särskild anmälan eller särskilt tillstånd av utfärdaren.

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

För rådgivningstjänsten debiteras en särskild avgift enligt gällande prislista.

Om en tjänsteleverantör vill tillhandahålla en informationsförsörjningstjänst mellan yrkescertifikatens 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 yrkescertifikatet innan avtalet om certifikatet ingås och beslut om utfärdande träffas, både på registreringsstället och på Myndigheten för digitalisering och befolkningsdatas webbplats.

7.4.5 Distribution av certifikat

Certifikatutfärdaren säkerställer att certifikaten ställs till förfogande för beställarna, undertecknarna och de förlitande parterna.

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

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

Ett yrkescertifikat levereras enligt överenskommelse och publiceras i det offentliga registret genast då det skapats och det finns i registret under hela dess giltighetstid. Certifikatutfärdaren publicerar en spärrlista som är i kraft i två timmar efter publiceringen. Spärrlistan uppdateras med en ny spärrlista en gång i timmen.

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

7.4.6 Återkallande av certifikat och avbrott i giltigheten

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

Certifikatutfärdaren kan spärra ett yrkescertifikat för en yrkesutbildad person inom social- och hälsovården om certifikatet har använts i strid med denna certifikatpolicy,

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

Det är inte tillåtet att använda eller försöka använda ett certifikat efter att begäran om spärrning har gjorts.

Följande kan kräva spärrning av ett certifikat:

- en yrkesutbildad inom social- och hälsovården eller dennes lagstadgade företrädare vad gäller den yrkesutbildades eget certifikat
- utfärdaren av certifikatet om förutsättningarna i 4.9.1 uppfylls.

Certifikatinnehavaren riktar begäran om spärrning till spärrtjänsten eller till utfärdaren. Begäran görs:

1) per telefon

2) skriftligen till certifikatutfärdaren.

Certifikatutfärdaren spärrar certifikat på eget initiativ:

- om rätten att utöva yrke upphör att gälla
- om certifikatinnehavaren avlider.

Följande uppgifter antecknas om spärrningen av certifikat:

- personuppgifterna som innehavaren av certifikatet har tillgång till
- förnamn och efternamn
- registreringsnummer, personbeteckning
- personuppgifter om den som gjorde begäran om spärrning (om en annan person än certifikatinnehavaren)
- sättet att identifiera den som gjorde begäran om spärrning
- tidpunkten för begäran om spärrning
- personuppgifter om den som tog emot begäran om spärrning
- eventuella övriga uppgifter som certifikatinnehavaren uppgett
- när ett yrkeskort försvunnit, när en certifikatinnehavare avlidit osv.
- personuppgifter om den som spärrade certifikatet
- tidpunkten för spärrning av certifikatet.

Myndigheten för digitalisering och befolkningsdata tillhandahåller ingen tjänst för att försätta ett certifikat i avbrottsläge.

Begäran om spärrning kan göras per telefon till spärrtjänsten eller skriftligt till utfärdaren.

När en begäran om spärrning görs per telefon eller skriftligt antecknas uppgifterna om anmälaren och certifikatinnehavaren i certifikatdatasystemet.

Om den som begär spärrning inte kan identifieras tillräckligt tillförlitligt och det finns risk för att certifikatet missbrukas, ger utfärdaren en spärrning företräde.

Orsaken till begäran som spärrning antecknas om någon annan än certifikatinnehavaren gör begäran; certifikatinnehavaren behöver inte uppge någon orsak till begäran om spärrning.

Certifikatutfärdaren skickar ingen separat bekräftelse till certifikatinnehavaren om att certifikatet har spärrats förutom i fall där spärrningen beror på förlorad rätt att utöva yrke. Certifikatet spärras via certifikatsystemet och uppgifterna om spärrningen förvaras i fem år från tidpunkten för spärrningen.

Certifikatinnehavaren ska utan dröjsmål lämna en begäran om spärrning till spärrtjänsten, om förutsättningarna för spärrning uppfylls.

Spärrtjänsten handlägger omedelbart begäranden om spärrning av certifikat.

Innan ett certifikat godkänns ska den förlitande parten kontrollera att certifikatet är i kraft och inte har spärrats.

Den förlitande parten ansvarar för kontrollen av certifikatets giltighet. Om den förlitande parten inte har kontrollerat spärrlistan eller uppgiften om giltighet via en OCSP-tjänst, är certifikatet inte att lita på.

En uppdaterad spärrlista publiceras varje timme

Av spärrlistan ska framgå den planerade publiceringstidpunkten för nästa spärrlista. En ny spärrlista kan också publiceras tidigare än planerat.

En uppdaterad spärrlista gäller i högst 72 timmar. I varje spärrlista anges när giltighetstiden går ut.

Om ett certifikat måste spärras på grund av att en hemlig nyckel har röjts avviker förfarandet inte från spärrning av andra orsaker.

Certifikat spärras inte för en viss tid.

Statuset på ett certifikat kan kontrolleras i realtid.

Ett certifikats status kontrolleras mot spärrtjänsten eller med hjälp av en OCSP-tjänst. Den förlitande parten ska också kontrollera att certifikatets giltighetstid inte har gått ut.

Ett certifikat i kraft antingen under en allmän giltighetstid, en viss tid som är certifikatbestämd eller tills det spärras om förutsättningarna för spärrning uppfylls.

Certifikatutfärdaren lagrar inte yrkesutbildade personers krypteringsnycklar utanför kortet. På det sättet kan certifikaten inte användas utan certifikatinnehavarens samtycke, och hemliga nycklar kan inte återställas ifall kortet går sönder eller kommer bort.

Det är i första hand certifikatinnehavaren som ska begära spärrning av ett yrkescertifikat. 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.

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 två 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 spärrade certifikat.

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 omedelbart i samband med begäran om spärrning.

Förnyelse av nyckelpar efter att ett certifikat införts på spärrlistan

De öppna nycklarna på yrkescertifikatet och de hemliga nycklarna på chipet kan inte förnyas. Ett spärrat yrkescertifikat kan inte tas i bruk på nytt.

För att ett nytt nyckelpar ska kunna bildas måste innehavaren ansöka om ett nytt yrkescertifikat.

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

Giltigheten för yrkescertifikat kan inte avbrytas tillfälligt, förutom när Myndigheten för digitalisering och befolkningsdata och kundorganisationen har avtalat separat om ett sådant förfarande.

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

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.

7.5 Utfärdarens lednings- och verksamhetspraxis

7.5.1 Hantering av säkerheten

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

I dokumenten i fråga (beskrivningarna av informationssäkerheten i systemet) specificeras alla objekt som hänför sig till tjänsterna samt eventuella hot och skyddsmetoder som tillämpas för att undvika att hoten blir verklighet eller begränsa följderna om hoten blir verklighet. I dokumenten beskrivs de regler, anvisningar och förfaranden enligt vika de specificerade tjänsterna och deras säkerhetsnivå genomförs och fastställs förfaringssätten vid eventuella kränkningar av informationssäkerheten och nödsituationer.

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

7.5.2 Klassificering och hantering av reserver

Certifikatutfärdaren säkerställer att nivån på skyddet av datalagren och informationen är ändamålsenlig.

Offentlig information som publiceras av Myndigheten för digitalisering och befolkningsdata i egenskap av utfärdare finns på utfärdarens webbplats. De konfidentiella uppgifterna i certifikatsystemet är sparade i utfärdarens egna, 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 personuppgiftslagen. Utfärdaren har även berett en registerbeskrivning i enlighet med personuppgiftslagen angående hanteringen av personuppgifter i certifikatsystemet.

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

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

Giltighetstiden för ett yrkescertifikat finns angivet på certifikatet. Yrkescertifikat 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 personuppgiftslagen och speciallagstiftning. Myndigheten för digitalisering och befolkningsdata har berett uppförandekoder både för utlämning av uppgifter och för den behandling av personuppgifter som sker inom certifikatverksamheten. Vid behandlingen av personuppgifter iakttas särskild omsorgsfullhet.

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.

7.5.3 Personal och informationssäkerhet

Certifikatutfärdaren säkerställer att personalen och rekryteringspraxisen främjar och stöder en tillförlitlig verksamhet.

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.

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 befolkningsdatas enhet Förvaltning och ledningsstöd 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.

7.5.4 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.

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

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

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

7.5.5 Hantering av verksamheten

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

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.

7.5.6 Hantering av åtkomsten till systemen

Certifikatutfärdaren säkerställer att endast personer med lämplig behörighet har åtkomst till utfärdarens system.

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

För certifikatsystemet används bara ändamålsenlig utrustning.

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

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 dubbla uppsättning.

7.5.7 Driftsättning och underhåll av pålitliga system

Certifikatutfärdaren använder pålitliga system och produkter som är skyddade mot otillåtna ändringar.

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 erhållit informationssäkerhetscertifikatet ISO 27001,

som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även vid en eventuell katastrof.

7.5.8 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 uppdateras ständigt.

7.5.9 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 enligt denna policy uppfyller de krav som ställs i Förordningen.

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som görs med signeringscertifikat och om verktyg för stark autentisering. I lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (661/2009) föreskrivs om certifikat som utfärdas av Myndigheten för digitalisering och befolkningsdata.

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. De skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet gäller Myndigheten för digitalisering och befolkningsdata. Vidare tillämpas lämpliga delar av skadeståndslagen (412/1974) och 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 personuppgiftslagen (523/1999) 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 (166/1996) och förordningen om registerförvaltningen (248/1996). I Finland utövar Traficom tillsyn över dem som utfärdar signeringscertifikat.

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

Vid utfärdandet av certifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att yrkescertifikaten för yrkesutbildade inom social- och hälsovården uppfyller kraven i denna certifikatpolicy. Eventuella tvister avgörs enligt rättssystemet i Finland av Helsingfors tingsrätt.

7.5.10 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.

På arkivering av yrkescertifikat tillämpas som allmän lag bestämmelserna 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 5 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.

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

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

7.6 Krav på organisationen

Certifikatutfärdaren ska säkerställa att dess organisation är tillförlitlig.

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare i denna certifikatpolicy. Om Myndigheten för digitalisering och befolkningsdatas ställning föreskrivs i lagen (166/1996) och förordningen om registerförvaltningen (248/1996).

Ett signeringscertifikat som utfärdats enligt denna policy uppfyller de krav som ställs i Förordningen.

Myndigheten för digitalisering och befolkningsdata iakttar god informationshantering enligt personuppgiftslagen (523/1999) och lagen om offentlighet i myndigheternas verksamhet. 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 yrkescertifikatet 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 personuppgiftslagen. Myndigheten för digitalisering och befolkningsdata samarbetar kontinuerligt med dataskyddsombudsmannen i frågor som gäller behandling av personuppgifter.

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

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

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

8 Specifikationer för andra signeringscertifikatpolicyer

Hantering av specifikationsdokument

I denna punkt fastställs de allmänna ramarna för andra certifikatpolicyer som gäller utfärdare av signeringscertifikat.

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

8.1 Hantering av signeringscertifikatpolicyn

Certifikatutfärdaren säkerställer att certifikatpolicyn är aktuell.

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 yrkescertifikat. 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.

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

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

8.2 Undantag till certifikatpolicyer som gäller signeringscertifikat för andra än allmänheten

Om certifikat utfärdas för andra än allmänheten, behöver signeringscertifikatpolicyn för verksamheten i fråga inte iaktta följande krav på förfarande i anslutning till signeringscertifikat:

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

8.3 Ytterligare krav

Beställare och förlitande parter ska informeras

a) ifall certifikatpolicyn inte gäller allmän användning

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 signeringscertifikatpolicy som behandlats i detta dokument.

8.4 Överensstämmelse med krav

Certifikatutfärdaren får uppge att verksamheten är förenlig med detta dokument och signeringscertifikatpolicyn bara

a) om certifikatutfärdaren uttrycker att den aktuella signeringscertifikatpolicyn 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 signeringscertifikatpolicy. 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.

b) om en behörig och oberoende part nyligen har bedömt uppfyllandet av kraven i den specifika signeringscertifikatpolicyn hos utfärdaren. Resultaten av granskningen ska på begäran göras tillgängligt för beställarna och de förlitande parterna.

[Yksikkö] / Aarnio Ville 1.4.2021