MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIERINGSPRAXIS SOCIAL HÄLSO TILLFÄLLIGA CERTIFIKAT

för tillfälligt certifikat för yrkesutbildade personer inom social- och hälsovården

OID: 1.2.246.517.1.10.307.1
OID: 1.2.246.517.1.10.357.1

15.9.2023

15.9.2023

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio, Anniina Tamminen
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Version 1.0	1.6.2021/VA
v 1.1	Uppdaterade versionen och länkarna till CPS dokument	3.10.2022/SK
v 1.3	Uppdaterade versionen till 1.3 för att vara i linje med de andra samtidigt uppdaterade policydokumenten. Ändrade validitetsdatum till en referens till pärmsidan. Ersatte termen ’PUK-kod’ med termen ’aktiveringskod’. Raderade föråldrad information angående användning av körkort som dokument för identifiering.	15.9.2023/AT

Innehållsförteckning

1 Inledning 12
1.1 Allmänt 13
1.2 Identifikationsuppgifter 14
1.3 Certifikatutfärdare och tillämpningsområden för certifikat 15
1.3.1 Certifikatutfärdare 15
1.3.2 Registrerare 15
1.3.3 Tillverkare och specificerare av reservkort eller chips 16
1.3.4 Spärrtjänst 16
1.3.5 Publicering av uppgifter om tillfälliga certifikat 16
1.3.6 Innehavare av certifikat 16
1.3.7 Förlitande part 17
1.3.8 Användning av certifikatet 17
1.4 Kontaktuppgifter 17
1.4.1 Organisation som administrerar certifieringspraxisen 17
1.4.2 Kontaktperson 17
2 Allmänna villkor 18
2.1 Skyldigheter 18
2.1.1 Certifikatutfärdarens skyldigheter 18
2.1.2 Registrerarens skyldigheter 19
2.1.3 Certifikatinnehavarens skyldigheter 19
2.1.4 Den förlitande partens skyldigheter 20
2.1.5 Skyldigheter vid publicering av certifikatet 20
2.2 Ansvar 21
2.2.1 Certifikatutfärdarens ansvar 21
2.2.2 Registrerarens ansvar 21
2.2.3 Certifikatinnehavarens ansvar 21
2.2.4 Den förlitande partens ansvar 22
2.2.5 Begränsning av ansvar 22
2.3 Ekonomiskt ansvar 23
2.3.1 Certifikatutfärdare 23
2.3.2 Andra parter 23
2.3.3 Utfärdarens ekonomiförvaltning 23
2.4 Tolkning och verkställighet 23
2.4.1 Lagstiftning som tillämpas 23
2.4.2 Avgörande av meningsskiljaktigheter 24

2.5 Avgifter 24
2.5.1 Beviljande och förnyelse av ett tillfälligt certifikat 25
2.5.2 Avgifter som hänför sig till användningen av tillfälligt certifikat 25
2.5.3 Avgifter som hänför sig till markering av tillfälligt certifikat på spärrlistan 25
2.5.4 Övriga avgifter 25
2.6 Publicering och tillgänglighet av uppgifter 25
2.6.1 Publicering av utfärdarens uppgifter 25
2.6.2 Publiceringsfrekvens 25
2.6.3 Uppgifternas tillgänglighet 26
2.6.4 Dataförvaring 26
2.7 Dataskyddsinspektion 26
2.7.1 Frekvens av inspektioner 26
2.7.2 Inspektör 26
2.7.3 Målen för och omfattningen av inspektionen 26
2.7.4 Åtgärder vid avvikelser 28
2.7.5 Information om resultatet av inspektionen 28
2.8 Publicering av uppgifter 28
2.8.1 Uppgifter som publiceras av utfärdaren 28
2.8.2 Offentliga uppgifter 28
2.8.3 Uppgifter som anknyter till upphörande eller avbrott av det tillfälliga certifikatets giltighet 28
2.8.4 Uppgifter som lämnas ut till myndigheter 29
2.8.5 Övriga uppgifter 29
2.8.6 Överlåtelse av uppgifter på certifikatinnehavarens begäran 29
2.8.7 Övriga principer för överlåtelse av uppgifter 29
2.9 Immaterialrättigheter 29
3 Identifiering av certifikatsökande 30
3.1 Registrering 30
3.1.1 Namngivningspraxis 30
3.1.2 Leverans av privata nycklar till certifikatinnehavaren 32
3.2 Förnyelse av nyckelpar 32
3.3 Förnyelse av nyckelpar efter införande av certifikat på spärrlista 32
3.4 Identifiering av den person som gjort begäran om spärrning 32
4 Funktionella krav 33
4.1 Ansökan om certifikat 33
4.2 Beviljande av certifikat 33
4.3 Mottagning av certifikat 33

4.4 Upphörande och avbrott av certifikatets giltighet 33
4.4.1 Förutsättningar för spärrning av ett certifikat 33
4.4.2 Person som gör begäran om spärrning 34
4.4.3 Spärrning 34
4.4.4 Tidpunkten för spärrning 35
4.4.5 Krav på avbrott av certifikatets giltighet 35
4.4.6 Person som gör begäran om avbrott 35
4.4.7 Begäran om avbrott 35
4.4.8 Begränsningar av avbrottstid 35
4.4.9 Publiceringsfrekvens för spärrlista 35
4.4.10 Krav på kontroll av spärrlista 35
4.4.11 Kontroll av certifikatets status online 35
4.4.12 Krav på kontroll av certifikatets status online 35
4.4.13 Särskilda krav gällande avslöjande av certifikatinnehavarens privata nyckel 36
4.5 Övervakning av systemet 36
4.6 Arkivering av uppgifter om certifikat 36
4.6.1 Material som sparas 36
4.6.2 Skydd av arkiv 37
4.6.3 Säkerhetsförfaranden för arkiverat material 37
4.6.4 Metoder för införskaffning och tryggande av arkiverat material 37
4.7 Hantering av kontinuerlig verksamhet och undantagsfall 37
4.7.1 Utfärdarens privata nyckel har röjts eller Utfärdarens certifikat har spärrats 37
4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof 38
4.8 Då utfärdarens verksamhet upphör 38
5 Krav på fysisk, funktionell och personalsäkerhet 38
5.1 Arrangemang kring fysisk säkerhet 39
5.1.1 Läge och lokalernas egenskaper 39
5.1.2 Fysisk tillgång till verksamhetslokalen 39
5.1.3 Elmatning och luftkonditionering 39
5.1.4 Brandsäkerhet 39
5.1.5 Förvaring av uppgifterna 39
5.1.6 Hantering av onödigt informationsmaterial 39
5.1.7 Vattenskador 39
5.1.8 Reservarrangemang 40
5.2 Funktionella krav 40
5.2.1 Ansvarsfördelning 40
5.2.2 Antal personer som behövs för uppgifterna 40

5.2.3 Uppgiftsspecifik autentisering 41
5.3 Personlig säkerhet 41
5.3.1 Utförande av bakgrundskontroll av personalen 41
5.3.2 Förfarande vid utförande av bakgrundskontroll 41
5.3.3 Krav på utbildning 42
5.3.4 Underhåll av expertis och kompetens 42
5.3.5 Krav på uppgiftsrotation 42
5.3.6 Åtgärder vid avvikelser 42
5.3.7 Personal som representerar organisationen 42
5.3.8 Handlingar som tillhandahålls personalen 42
6 Tekniska säkerhetsarrangemang 43
6.1 Skapande och sparande av nyckelpar 43
6.1.1 Skapande av nyckelpar 43
6.1.2 Överlåtelse av en privat nyckel till certifikatinnehavaren 43
6.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren 43
6.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren 44
6.1.5 Nycklarnas längder 44
6.1.6 Nycklarnas användningsändamål: 44
6.2 Skydd av privat nyckel 44
6.2.1 Standarder som gäller den kryptografiska modulen 44
6.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel 45
6.2.3 Överlåtelse av en privat nyckel till förlitande part 45
6.2.4 Säkerhetskopia av en privat nyckel 45
6.2.5 Arkivering av en privat nyckel 45
6.2.6 Administration av en privat nyckel i kryptografiska moduler 45
6.3 Andra faktorer som anknyter till nyckeladministration 45
6.3.1 Arkivering av en publik nyckel 45
6.3.2 Användningstid för publika och privata nycklar 45
6.4 Aktiveringsuppgift 46
6.4.1 Skapande och ibruktagande av aktiveringsuppgift 46
6.4.2 Skydd av aktiveringsuppgift 46
6.4.3 Andra faktorer som anknyter till aktiveringsuppgiften 46
6.5 Säkerhetskrav som gäller användning av datorer och tillgång till dessa 46
6.5.1 Utrustningssäkerhet 46
6.6 Livscykeladministration av certifikatsystemet 46
6.6.1 Övervakning som gäller systemutvecklingen 47
6.6.2 Hantering av säkerhet 47

6.7 Datanätets säkerhet 47
6.8 Övervakning av användning av kryptografisk modul 47
7 Profiler för certifikat och spärrlistor 48
7.1 Tekniska uppgifter om certifikat 48
7.2 Profil för spärrlistor 48
8 Hantering av dokument innehållande bestämmelser 48
8.1 Ändring av bestämmelser 48
8.2 Publicering och information 48
8.3 Förfarande för ändring och godkännande av certifikatpolicy 48

CERTIFIERINGSPRAXIS SOCIAL HÄLSO TILLFÄLLIGA CERTIFIKAT
Definitioner och förkortningar

Definitioner

Aktiveringsuppgift: En sådan konfidentiell uppgift (PIN-kod) som behövs för aktivering av privata nycklar med chips och användning av dessa med en öppen nyckelmetod.

Aktiveringskod: Aktiveringsuppgift, som används för att aktivera och fastställa egna, personliga PIN-koder. En aktiveringskod kan också användas för att öppna en låst PIN-kod.

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

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

Publik nyckel: Den publika delen av nyckelparet som används för icke-symmetrisk kryptering med en öppen nyckelmetod. Certifikatutfärdaren bekräftar med sin digitala signatur att den publika nyckeln innehas av certifikatets innehavare. Den publika nyckeln är en del av certifikatets datainnehåll.

Öppet nyckelsystem: Dataskyddsinfrastruktur där dataskyddstjänster produceras med en öppen nyckelmetod.

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

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

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

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

Organisationscertifikat: Ett kvalificerat certifikat som Myndigheten för digitalisering och befolkningsdata beviljat en fysisk person. Certifikatparets datainnehåll har fastställts i lagen om stark autentisering och betrodda elektroniska tjänster.

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

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

RSA-algoritm och RSA-nyckel: RSA-algoritm är en allmänt använd algoritm för publik nyckel. I organisationscertifikatet ingår privata och publika RSA-nycklar.

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

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

Terhikki-registret: Centralregister över yrkesutbildade personer inom hälso- och sjukvården.

Yrkesutbildad person inom hälso- och sjukvården En yrkesutbildad person inom hälso- och sjukvården som med stöd av lagen har erhållit rätt att utöva yrke (legitimerad yrkesutbildad person) eller tillstånd att utöva yrke (yrkesutbildad person som beviljats tillstånd) samt som med stöd av denna 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 har registrerats i centralregistret övre yrkesutbildade personer inom hälso- och sjukvården.

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

Personal inom hälso- och sjukvården: i lagen om yrkesutbildade personer inom hälso- och sjukvård (559/1994) avsedd personal som tillhandahåller hälsovårdstjänster, men som inte är yrkesutbildade personer inom hälso- och sjukvården. Till denna personalgrupp hör till exempel stöd-, kansli- och informationstjänstpersonal vid en verksamhetsenhet inom hälso- och sjukvården. En person som arbetar i en organisationen som erbjuder hälsovårdstjänster, men som inte är yrkesutbildad person inom hälso- och sjukvården.

Personalkort för social- och hälsovården (personalkort): Ett aktivkort som MDB beviljat övrig personal inom social- och hälsovården (andra än yrkesutbildade personer inom hälso- och sjukvården) och som innehåller ett certifikat.

Studerande inom hälso- och sjukvården: Under de förutsättningar som föreskrivs i statsrådets förordning kan den som studerar för yrket i fråga tillfälligt sköta en legitimerad yrkesutbildad persons uppgifter under ledning och tillsyn av en legitimerad yrkesutbildad person med rätt att självständigt utöva yrket i fråga. I fråga om en sådan studerande iakttas då i tillämpliga delar vad som föreskrivs om yrkesutbildade personer inom hälso- och sjukvården. Studerande inom medicin, odontologi och farmaci får ett yrkeskort inom hälso- och sjukvården. Den som studerar för ett annat yrke inom

hälso- och sjukvården och som uppfyller förutsättningarna i förordningen får ett organisationsspecifikt personalkort inom hälso- och sjukvården.

Aktörer inom social- och hälsovården: anställda hos serviceleverantörer inom social- och hälsovården som inte är yrkesutbildade personer inom social- och hälsovården eller personal inom social- och hälsovården. I gruppen i fråga ingår övriga personer och specialgrupper som använder riksomfattande datasystem, såsom dataskyddsansvariga samt datasystemleverantörer, konsulter osv.

Aktivkort inom social- och hälsovården (aktivkort): Ett aktivkort som MDB beviljat övrig personal inom social- och hälsovården och som innehåller ett certifikat.

Tillfälligt certifikat: Ett certifikat som Myndigheten för digitalisering och befolkningsdata beviljat en fysisk person och som kan användas för verifikation och kryptering eller verifikation och kryptering samt elektronisk signatur.

Reservkort: Ett reservkort för organisationens certifikatkort som har en teknisk del, ett chips, är försett med certifikat som kortinnehavaren behöver i när denne använder reservkortet. Av särskilt skäl kan reservkort också beviljas personer som inte har organisationens aktivkort.

Certifikat: Ett elektroniskt intyg med hjälp av vilket personen kan verifieras och med vilket information kan krypteras och som kopplar uppgifterna om verifieringen av en signatur till den som gjort signaturen och bekräftar signeraren. Certifikatet innehåller en medföljande unik kod enligt certifieringspraxis.

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

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

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

Certifikatregister: Register som utfärdaren som erbjuder certifikat för allmänheten upprätthåller. Uppgifterna förvaras i minst 5 år från tidpunkten då certifikatet upphört att gälla.

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

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

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

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

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

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

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

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

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

Användning och användningssyfte för certifikat: I detta dokument avses med användning av certifikat såväl användning av själva certifikatet som användning av medföljande nycklar.

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

Lista över förkortningar

CA	Certification Authority, certifikatutfärdare
CP	Certificate Policy, certifieringspolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, kryptografisk modul
HST	Elektronisk identifiering av person
HTTP	Hypertext Transport Protocol

ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, onlinetjänst för återställande av certifikatets status
OID	Object Identifier, identifierande kod
PDS	PKI Disclosure Statement, certifikatbeskrivning
PIN	Personal Identification Number, PIN-kod
PKI	Public Key Infrastructure, öppet nyckelsystem
RSA	Rivest, Shamir, Adleman, en algoritm för publik nyckel, icke-symmetrisk algoritm
MDB	Myndigheten för digitalisering och befolkningsdata

Referenser

I detta dokument refereras till bestämmelser och bestämningar som anges i följande dokument och som är bindande i anknytning till de funktioner som beskrivs i detta dokument.

- De använda referenserna till publiceringsdatumet och anläggningens eller versionens nummer är exakta eller av allmän natur.
- I fråga om exakta referenser tillämpas inte senare kontroller av källan.
- I fråga om referenser av allmän natur tillämpas den senaste versionen av källan.

Material gällande detta dokument finns tillgänglig bland annat på adressen http://docbox.etsi.org/Reference. ETSI garanterar inte att länken fungerar på lång sikt.

Bestämmande 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".

Riktgivande 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 Di-rective 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 certifi-cation authorities issuing qualified certificates".

[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 Prac-tices Framework".

[Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the pro-tection 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 Con-formity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Terminologiska beskrivningar

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].

1 Inledning

Certifieringspraxis är en beskrivning av förfaringssätt och verksamhetsprinciper som efterlevs vid beviljande av certifikat, som utarbetas av utfärdaren. Certifieringspraxis är en mer detaljerad beskrivning av utfärdarens verksamhet än certifikatpolicy.

Denna certifieringspraxis tillämpas på Myndigheten för digitalisering och befolkningsdatas tillfälliga certifikat för yrkesutbildade personer inom social- och hälsovården.

Ett tillfälligt certifikat som stödjer användningen av certifikat för yrkesutbildade personer inom social- och hälsovården beviljat av Myndigheten för digitalisering och befolkningsdata, OID:1.2.246.517.1.10.306.1 och 1.2.246.517.1.10.356.1.

1.1 Allmänt

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

Ett tillfälligt certifikat är ett verifikations- och krypteringscertifikat samt signaturcertifikat. Myndigheten för digitalisering och befolkningsdata garanterar identitetens riktighet.

Ett tillfälligt certifikat för yrkesutbildade personer inom social- och hälsovården enligt denna policy kan beviljas en yrkesutbildad person inom social- och hälsovården. När en serviceleverantör inom social- och hälsovården registrerar tillfälliga certifikat för yrkesutbildade personer inom social- och hälsovården ska alla de parter som avses i denna certifikatpolicy följa lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

Myndigheten för digitalisering och befolkningsdata, som är certifikatutfärdare, specificerar innehavaren av certifikatet med hjälp av en unik kod, som även är en del av certifikatets datainnehåll. Koden är en teknisk identifieringskod som separat skapats för elektronisk ärendehantering. Den innehåller inte identifieringsuppgifter om personen.

Det tillfälliga certifikatet kan lagras på olika aktivkort.

Myndigheten för digitalisering och befolkningsdatas certifikatpolicy och certifieringspraxis har en egen unik kod (OID).

I utfärdarens funktioner ingår produktion av certifikat-, register- och spärrtjänster, registrering samt tillverkning och specificering av aktivkort. Dessa funktioner beskrivs närmare i kapitel 1.3.

Myndigheten för digitalisering och befolkningsdata skapar en separat certfikatpolicy för varje typ av certifikat som den utfärdat som för varje tekniskt underlag för certifieringspraxis. Certifikatpolicy beskriver de förfaringssätt, som används per certifikattyp användarvillkor och ansvarsfördelning och övriga aspekter av användningen av certifikat på ett allmänt plan. Certifieringspraxis beskriver de förfaringssätt som tillämpas på ett detaljerat plan.

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordning) tillämpas på signaturcertifikat för betrodda tjänster från och med 1.7.2016. I detta dokument fastställs förfarandekrav som gäller verksamheten och förvaltningspraxis av utfärdare av identifierings- och signaturcertifikat enligt Förordningen. I förfarandekrav som fastställs i detta dokument beskrivs användning av medel för skapande av säker signatur.

Utfärdaren är leverantör av certifikattjänster och beviljar certifikat enligt Förordningen.

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) är även Myndigheten för digitalisering och befolkningsdata leverantör av autentiseringstjänster då den producerar certifikatbaserade autentiseringsredskap för allmänheten. Leverantörer av autentiseringstjänster övervakas i Finland av Traficom.

Myndigheten för digitalisering och befolkningsdata har fungerat som lagstadgad certifikatutfärdare för hälsovården sedan 1.12.2010 och fungerar dessutom som lagstadgad certifikatutfärdare för socialvården sedan 1.4.2015 med stöd av ändringar i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) samt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019). Myndigheten för digitalisering och befolkningsdatas certifikattjänster ansvarar för verkets certifikatverksamhet.

1.2 Identifikationsuppgifter

Certifikatutfärdaren skapar en certifikatpolicy för varje typ av certifikat som den utfärdat och en certifieringspraxis för varje tekniskt underlag på vilket certifikatet kan användas.

Denna certifieringspraxis heter Certifieringspraxis för Myndigheten för digitalisering och befolkningsdatas tillfälliga certifikat för yrkesutbildade personer social- och hälsovården vars OID är 1.2.246.517.1.10.307.1 och 1.2.246.517.1.10.357.1.

Denna certifieringspraxis refererar till Certifikatpolicyn för tillfälliga certifikat för yrkesutbildade personer social- och hälsovården vars OID är 1.2.246.517.1.10.307 och 1.2.246.517.1.10.357.

Signaturcertifikatpolicyns OID-identifikationskoder som definieras i detta dokument är följande:

Myndigheten för digitalisering och befolkningsdata följer certifikatpolicyn som gäller signaturcertifikat som beviljas allmänheten enligt betrodda tjänster i Förordningen nr (EU) 910/2014. Dokumentets referensuppgifter är SÖK EN 319 411-1 [2], punkt QSCD; OID: 0.4.0.194112.1.2. Signaturcertifikat som beviljas enligt denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de godkända certifikat och medel för skapande som beskrivs i Förordningen såsom föreskrivs i 28 och 29 i Förordningen.

Nivån av identifieringscertifikatet uppfyller kravnivån ”hög” enligt Förordningen och Säkerhetsnivåförordningen som utfärdats med stöd av den.

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

1.3 Certifikatutfärdare och tillämpningsområden för certifikat

Utfärdaren producerar certifikattjänster enligt villkoren i denna certifieringspraxis och ansvarar för att de fungerar i innehavarens användning enligt 2.2.1 som beskriver utfärdarens ansvar. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifieringspraxis är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019) och lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) är att utöver övriga tjänster producera tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdatas certifikattjänst indelas operativt i följande delområden:

1.3.1 Certifikatutfärdare

Utfärdarens uppgift är att:

- utfärda certifikat- och registertjänster samt spärrtjänster enligt certifikatpolicyn och certifieringspraxisen
- personligen identifiera certifikatsökanden
- se till att datainnehållet i certifikaten är felfritt
- se till att certifikaten spärrs och att spärrlistorna för certifikat publiceras
- följa god dataskyddsnivå och god datahanteringssed vid hantering av certifikatinnehavarnas personuppgifter
- skapa en kommunikationskod för specificering av personen
- erbjuda ett beställnings- och administrationssystem för kort för registrering och spärrning.

1.3.2 Registrerare

Registreringen av et tillfälligt certifikat sker enligt förfarandet i lagen om stark autentisering och betrodda elektroniska tjänster och denna certifieringspraxis. Registreraren för tillfälliga certifikat på reservkort för yrkesutbildade personer inom social- och hälsovården är samarbetspartnern som ingått ett registreringsavtal med Myndigheten för digitalisering och befolkningsdata.

- Registreraren agerar på certifikatutfärdarens uppdrag och ansvar.
- Registreraren följer certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Registreraren identifierar certifikatsökanden enligt certifieringspraxisen.

- Registreringsstället lämnar till utfärdaren de uppgifter som anknyter till identifiering av personen och till ansökan av certifikatet, enligt vilka certifikatet skapas.
- Registreraren följer principer för god hantering av personuppgifter i sitt uppdrag.
- Myndigheten för digitalisering och befolkningsdata övervakar att kundorganisationen följer de villkor för registrering som nämns i avtalet och de bestämmelser som gäller registrering i lagen om stark autentisering och betrodda elektroniska tjänster.
- Registreraren använder det beställnings- och administrationssystem som certifikatutfärdaren erbjudit för registrering, beställning och spärrning av reservkort.

1.3.3 Tillverkare och specificerare av reservkort eller chips

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

1.3.4 Spärrtjänst

I fråga om reservkort används inte en likadan spärrtjänst för certifikat som med andra kort, utan spärrningen görs av registreraren i organisationen för certifikatinnehavaren i beställnings- och administrationssystemet för kort. Certifikat som spärras är certifikat som certifikatinnehavaren önskar innan certifikatets giltighetstid har löpt ut. De spärrade certifikaten införs i spärrlistan.

1.3.5 Publicering av uppgifter om tillfälliga certifikat

Registertjänsten är en offentlig webbtjänst som innehåller utfärdarens offentliga certifikat och spärrlistan. Tillfälliga certifikat publiceras inte i registret. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

1.3.6 Innehavare av certifikat

Ett organisationscertifikat enligt denna certifikatpolicy kan beviljas de personer som identifierats enligt lagen om stark autentisering och betrodda elektroniska tjänster och enligt kraven i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de förordningar som utfärdats med stöd av dessa. Innehavare av ett tillfälligt certifikat för yrkesutbildade personer inom social- och hälsovården kan vara en yrkesutbildad person inom social- och hälsovården.

Certifikatinnehavaren ska följa certifikatutfärdarens certifikatpolicy och certifieringspraxis.

1.3.7 Förlitande part

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

1.3.8 Användning av certifikatet

Myndigheten för digitalisering och befolkningsdata följer denna certifieringspraxis när den beviljar tillfälliga certifikat till yrkesutbildade personer inom social- och hälsovården. Certifikatinnehavare och parter som litar på certifikatet ska följa denna certifieringspraxis.

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

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

1.4 Kontaktuppgifter

1.4.1 Organisation som administrerar certifieringspraxisen

Denna certifikatpolicy är registrerad av Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019) är att utöver övriga tjänster producera tjänster inom certifierad elektronisk kommunikation. Myndigheten för digitalisering och befolkningsdata svarar för administrationen och uppdateringen av denna certifikatpolicy.

Upphovsrätten enligt denna certifieringspraxis tillfaller Myndigheten för digitalisering och befolkningsdata.

1.4.2 Kontaktperson

Frågor som gäller denna certifieringspraxis skickas till följande adress:

Myndigheten för digitalisering och befolkningsdata

PB 123 (Fågelviksgränden 2)	Tfn +358 295 535 001
00531 Helsingfors	Fax +358 9 876 4369
FO-nummer: 0245437-2	kirjaamo@dvv.fi

Frågor som gäller certifikatpolicyn besvaras av Myndigheten för digitalisering och befolkningsdatas Certifikattjänster.

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.dvv.fi/sv

2 Allmänna villkor

Certifikatpolicyn träder i kraft vid datumet som nämns på pärmsidan. Ändringsförfarandet för och publiceringen av certifieringspraxisen har beskrivits i punkt 8 i detta dokument.

2.1 Skyldigheter

2.1.1 Certifikatutfärdarens skyldigheter

- Myndigheten för digitalisering och befolkningsdata har ett lagstadgat uppdrag att fungera som certifikatutfärdare.
- Kundorganisationen ansvarar för sin del för spärrning av certifikat enligt avtalet mellan MDB och kundorganisationen.
- Kundorganisationen ska kontrollera riktigheten av uppgifter som gäller slutanvändarna enligt avtalet mellan MDB och kundorganisationen.
- Utfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser samt möjlighet att hantera 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 som man anlitar, t.ex. registrerare och korttillverkare.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning för beviljande av tillfälliga certifikat samt övriga aspekter av användningen av det tillfälliga certifikatet på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren följer certifikatpolicyn och certifieringspraxisen.

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

2.1.2 Registrerarens skyldigheter

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

2.1.3 Certifikatinnehavarens skyldigheter

- Användningsändamålet för certifikatet har fastställs i varje certifikattyps certifikatpolicy, certifieringspraxis och certifikatinnehavarens användningsvillkor. Certifikat får endast användas enligt dess användningsändamål för verifikation, kryptering eller elektronisk signatur.
- Innehavaren av det tillfälliga certifikatet ansvarar för att de uppgifter som uppges då man ansöker om det tillfälliga certifikatet är riktiga.
- Certifikatinnehavaren ansvarar för användningen av det tillfälliga certifikatet, de rättshandlingar som denne gör med certifikatet och deras ekonomiska följder.

- Innehavaren av det tillfälliga certifikatet förvarar de privata nycklar som finns på chipset och den kod som behövs för att använda dessa separat samt strävar efter att förhindra att de privata nycklarna försvinner, hamnar i utomståendes händer, ändras eller används olovligt. Att lämna chipset eller avslöja PIN-koden för en annan person, t.ex. genom att låna, frigör utfärdaren och parten som litar på det tillfälliga certifikatet från eventuellt ansvar som orsakas av användningen av chipset.

- Det tillfälliga certifikatet hanteras och skyddas med samma noggrannhet som andra motsvarande chips, kort eller dokument, såsom kreditkort, körkort och pass. Personliga PIN-koder ska förvaras fysiskt på annat ställe än chipset som innehåller det tillfälliga certifikatet och de privata nycklarna.

- Om chipset eller kortet försvinner eller om det finns möjlighet till missbruk, ska man omedelbart meddela registreraren i organisationen för certifikatinnehavaren, som spärrar certifikatet i beställnings- och administrationssystemet för kort.

2.1.4 Den förlitande partens skyldigheter

Den part som litar på certifikatet är skyldig att säkerställa att certifikatet används enligt dess användningsändamål. Användningsändamålet för verifierings- och krypteringscertifikatet är verifiering av person och kryptering av data. Användningsändamålet för signaturcertifikatet är elektronisk signatur.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan uppriktigt lita på det tillfälliga certifikatet då man kontrollerat att certifikatkedjan är hel, att det tillfälliga certifikatet är giltigt till exempel med hjälp av OCSP-tjänsten och att certifikatet inte har spärrats. Förlitande parter är skyldiga att kontrollera certifikaten på spärrlistan eller i OCSP-tjänsten. För att säkerställa att det tillfälliga certifikatet giltighet är tillförlitlig, ska den förlitande parten kontrollera de spärrade certifikaten på det sätt som beskrivs nedan.

Om den förlitande parten kopierar spärrlistan från registret, ska denna säkerställa spärrlistans autenticitet genom att kontrollera utfärdaren elektroniska signatur. Dessutom ska förlitande parter kontrollera spärrlistans giltighetstid.

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

2.1.5 Skyldigheter vid publicering av certifikatet

De spärrade tillfälliga certifikaten publiceras på spärrlistan i vilken den förlitande parten ska kontrollera att certifikatet är giltigt. Tillfälliga certifikat publiceras inte i registret.

2.2 Ansvar

2.2.1 Certifikatutfärdarens ansvar

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

Myndigheten för digitalisering och befolkningsdata svarar för att det tillfälliga certifikatet har skapats enligt de förfaranden som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster samt certifikatpolicyn och certifieringspraxisen. Dessutom ska det tillfälliga certifikatet skapas enligt de uppgifter som sökanden har lämnat och det ska uppfylla utfärdarens skadeståndsansvar som fastställs i lagarna. Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa. Myndigheten för digitalisering och befolkningsdata ansvarar endast för den information som man sparat i certifikatet.

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

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

Utfärdaren ansvarar för att de certifikat som spärrats av registreraren i certifikatinnehavarens organisation införs i spärrlistan i den tid som nämns i denna certifieringspraxis.

2.2.2 Registrerarens ansvar

Registreraren för det tillfälliga certifikatet är det registreringsställe som registrerar certifikatet för Myndigheten för digitalisering och befolkningsdata som är utfärdare enligt ett avtal som separat ingåtts för denna verksamhet. Registreraren ansvarar för den registrering som denne gjort och för spärrningen av certifikatet. Vad gäller registreringen följs de krav som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och certifieringspraxisen. Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

2.2.3 Certifikatinnehavarens ansvar

Certifikatinnehavaren ansvarar för användningen av det tillfälliga certifikatet, de rättshandlingar som denne gör med certifikatet och deras ekonomiska följder.

Om ett kort med chips lämnas i läsaren, kan det finnas risk för missbruk av det tillfälliga certifikatet. När certifikatinnehavaren slutar terminalsessionen, är denne ansvarig för att avlägsna chipset som innehåller det tillfälliga certifikatet ur läsaren och stänga de använda applikationerna tillbörligt eller annars koppla av den tekniska uppkopplingen som behövs för att använda certifikatet.

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

2.2.4 Den förlitande partens ansvar

Den förlitande parten kan inte uppriktigt lita på det tillfälliga certifikatet om man inte kontrollerat det tillfälliga certifikatets giltighet på spärrlistan. Om det tillfälliga certifikatet trots detta godkänns frias Myndigheten för digitalisering och befolkningsdata från ansvar. Den förlitande parten ska kontrollera att certifikatkedjan är hel och att det beviljade certifikatet motsvarar användningssyftet i den rättshandling det används för.

2.2.5 Begränsning av ansvar

Vid produktion av certifikattjänster fastställs Myndigheten för digitalisering och befolkningsdatas ansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och i tillämpliga delar enligt bestämmelserna i skadeståndslagen (412/1974).

Myndigheten för digitalisering och befolkningsdata svarar inte för eventuella skador som orsakas av att PIN-koden och certifikatinnehavarens privata nyckel röjs, om inte röjningen direkt har orsakats av Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdatas ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder, dock högst 15 procent av den ifrågavarande kundorganisationens certifikatfakturering under de föregående tre månaderna (MDB:s andel).

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

Myndigheten för digitalisering och befolkningsdata är inte ansvarig 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 kortläsare 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 eller underhåll av spärrlistan meddelas på förhand.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Certifikatinnehavare eller förlitande parter ska i sådana fall svara för egna kostnader som följer av detta

och utfärdaren är inte skyldig att ersätta certifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

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

2.3 Ekonomiskt ansvar

2.3.1 Certifikatutfärdare

Vid produktion av certifikattjänster fastställs Myndigheten för digitalisering och befolkningsdatas ansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och i tillämpliga delar enligt bestämmelserna i skadeståndslagen (412/1974).

I fråga om den förlitande parten ansvarar Myndigheten för digitalisering och befolkningsdata för högst orsakade direkta skador enligt punkten ansvarsbegränsningar.

2.3.2 Andra parter

Den förlitande parten kan lita på riktigheten av det tillfälliga certifikatet, om denne har kontrollerat att certifikatkedjan är hel, att det tillfälliga certifikatet inte finns på spärrlistan och att certifikatets giltighetstid inte har upphört och denne inte har andra grundade orsaker att misstänka riktigheten av användningen av certifikatet.

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

2.3.3 Utfärdarens ekonomiförvaltning

Myndigheten för digitalisering och befolkningsdatas certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Myndigheten för digitalisering och befolkningsdata är ett ämbetsverk underställt finansministeriet. Myndigheten för digitalisering och befolkningsdata ekonomiska förvaltning utgår från lagar och förordningar om statens ekonomi samt finansministeriets och Statskontorets bestämmelser. Statens revisionsverk sköter granskningen av ekonomin. Utöver detta beskrivs verksamhetens resultat med fokus på effekter, ekonomi och lönsamhet.

2.4 Tolkning och verkställighet

2.4.1 Lagstiftning som tillämpas

Vid produktion av certifikattjänster fastställs Myndigheten för digitalisering och befolkningsdatas ansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och i tillämpliga delar enligt bestämmelserna i skadeståndslagen (412/1974). Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

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

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

Myndigheten för digitalisering och befolkningsdata skaffar de uppgifter som krävs för registrering och identifiering av person med ett separat privaträttsligt avtal som gäller registreringsåtgärder. Myndigheten för digitalisering och befolkningsdata kan skaffa tjänsten till exempel genom att följa bestämmelserna i lagen om samservice inom den offentliga förvaltningen (223/2007).

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

Myndigheten för digitalisering och befolkningsdata svarar för att de tillfälliga certifikaten har skapats enligt de förfaranden som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster samt certifikatpolicyn och certifieringspraxisen och enligt de uppgifter certifikatsökanden har uppgett. Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

Myndigheten för digitalisering och befolkningsdatas verksamhet övervakas av Kommunikationsverket som är ett tillsynsorgan enligt lagen om stark autentisering och betrodda elektroniska tjänster och som ger nödvändiga bestämmelser och rekommendationer om verksamheten.

I fråga om hantering av personuppgifter följer Myndigheten för digitalisering och befolkningsdata personuppgiftslagen. Myndigheten för digitalisering och befolkningsdata samarbetar kontinuerligt med Dataombudsmannen i fråga om hanteringen av personuppgifter.

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

2.4.2 Avgörande av meningsskiljaktigheter

Vid beviljandet av certifikat ansvarar Myndigheten för digitalisering och befolkningsdata för att certifikaten uppfyller de krav som ställs i denna certifieringspraxis och i certifikatpolicyn som gäller tillfälliga certifikat. Eventuella tvister löses enligt rättssystemet i Finland.

2.5 Avgifter

I detta kapitel fastställs de avgifter som hänför sig till användningen av tillfälliga certifikat.

2.5.1 Beviljande och förnyelse av ett tillfälligt certifikat

Ett tillfälligt certifikat ansöks enligt vad som beskrivs i certifieringspraxisen.

Priset på reservkortet fastställs enligt finansministeriets vid var tid gällande förordning om avgifterna för Myndigheten för digitalisering och befolkningsdatas prestationer.

Tillfälliga certifikat prissatts enligt Befolkningscentralens giltiga prislista för företagsekonomiska prestationer.

2.5.2 Avgifter som hänför sig till användningen av tillfälligt certifikat

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

2.5.3 Avgifter som hänför sig till markering av tillfälligt certifikat på spärrlistan

Det är avgiftsfritt att anmäla att ett tillfälligt certifikat ska införas på spärrlistan. Även avhämtning av spärrlistor från registret och kontroll av det tillfälliga certifikatets giltighet är avgiftsfritt.

2.5.4 Övriga avgifter

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

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

Användningsvillkoren för det tillfälliga certifikatet lämnas till innehavaren av det tillfälliga certifikatet i samband med mottagningen av det tillfälliga certifikatet.

2.6 Publicering och tillgänglighet av uppgifter

2.6.1 Publicering av utfärdarens uppgifter

Utfärdaren publicerar utfärdarens offentliga certifikat och spärrlistor i ett allmänt tillgängligt, offentligt register som kan användas utan avgift. Tillfälliga certifikat publiceras inte. Utfärdaren publicerar certifikatpolicy, certifieringspraxis, certifikatbeskrivning (PDS) samt övriga offentliga handlingar med anknytning till produktionen av certifikattjänster på sin webbplats.

2.6.2 Publiceringsfrekvens

Utfärdaren publicerar en spärrlista som är giltig 72 timmar efter publikationen. Denna spärrlista uppdateras en gång per timme med en ny spärrlista.

2.6.3 Uppgifternas tillgänglighet

Uppgifterna i registret och spärrlistan är offentligt tillgängliga. Offentliga FINEID-bestämmelser som publicerats av utfärdaren finns på utfärdarens webbplats. Certifikatpolicyn och certifieringspraxisen finns även tillgängliga på certifikatutfärdarens webbplats.

2.6.4 Dataförvaring

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

2.7 Dataskyddsinspektion

Traficom som övervakar leverantörer av identifieringstjänst kan inspektera leverantörens verksamhet under de förutsättningar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster.

2.7.1 Frekvens av inspektioner

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

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

2.7.2 Inspektör

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

2.7.3 Målen för och omfattningen av inspektionen

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

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

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

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

Spärrtjänst:

- Datakommunikationssäkerhet
- Personalsäkerhet
- Fysisk säkerhet

Certifikatproduktion:

- Arbetsfördelning och varje persons uppgifter – personalsäkerhet
- Fysisk säkerhet
- Säkerhet i anknytning till utfärdarens nycklar
- Produktionssystemet för certifikat och reservsystemet
- Datakommunikationssäkerhet

Kortproduktion:

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

Registertjänst:

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

- datakommunikationssäkerhet
- fysisk säkerhet

HelpDesk-verksamhet:

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

2.7.4 Åtgärder vid avvikelser

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

2.7.5 Information om resultatet av inspektionen

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

Myndigheten för digitalisering och befolkningsdata informerar bland annat Traficom om resultaten av inspektionen.

2.8 Publicering av uppgifter

2.8.1 Uppgifter som publiceras av utfärdaren

Uppgifterna i certifikatsystemet är konfidentiella, om de inte grundar sig på bestämmelser om överlåtelse av uppgifter enligt personuppgiftslagen, lagen om elektronisk kommunikation i myndigheternas verksamhet och lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster (304/2019) eller lagen om stark autentisering och betrodda elektroniska tjänster eller de ändamål som fastställs i certifikatpolicyn eller certifieringspraxisen.

2.8.2 Offentliga uppgifter

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

2.8.3 Uppgifter som anknyter till upphörande eller avbrott av det tillfälliga certifikatets giltighet

Start- och sluttiden för det tillfälliga certifikatets giltighet har antecknats i det tillfälliga certifikatet. Certifikat som spärrats under giltighetstiden publiceras på spärrlistan som är tillgänglig för alla.

2.8.4 Uppgifter som lämnas ut till myndigheter

Uppgifter som lämnas ut till myndigheter fastställs enligt gällande lagstiftning.

2.8.5 Övriga uppgifter

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

2.8.6 Överlåtelse av uppgifter på certifikatinnehavarens begäran

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

2.8.7 Övriga principer för överlåtelse av uppgifter

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

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

2.9 Immaterialrättigheter

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

3 Identifiering av certifikatsökande

3.1 Registrering

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

I ansökningsdokumentet nämns tydligt att sökanden av tillfälliga certifikat intygar riktigheten hos uppgifterna med sin signatur samt godkänner att de tillfälliga certifikaten skapas. Samtidigt godkänner sökanden reglerna och villkoren för användning av de tillfälliga certifikaten samt sörjer för förvaringen av det tillfälliga certifikaten och PIN-koderna samt för anmälan om eventuellt missbruk eller försvunnet kort.

Utfärdaren, registreraren, korttillverkaren samt leverantörer av övriga delområden av certifikattjänsterna har ingått avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheterna för samtliga parter. Sökanden av tillfälliga certifikat svarar för att samtliga uppgifter som är väsentliga för de tillfälliga certifikaten och som sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren av tillfälliga certifikat ska endast använda sina tillfälliga certifikat i enlighet med deras användningssyfte.

Då utfärdaren beviljar det tillfälliga certifikatet, godkänner utfärdaren samtidigt certifikatansökan.

Innehavaren av tillfälliga certifikat ansvarar för att förhindra att de privata nycklar som denne har och PIN-koderna används i strid mot användningsvillkoren genom att sörja för dessa på det sätt som nämns i användningsvillkoren.

Certifikatinnehavaren ska omedelbart anmäla om behovet av att spärra det tillfälliga certifikatet till registreraren i certifikatinnehavarens organisation, om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

3.1.1 Namngivningspraxis

Befolkningsregistercentalens rotutfärdare är:

CN (Common name) = DVV Gov. Root CA – G3 RSA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

S (State) = Finland

C (Country) = FI

och

CN (Common name) = DVV Gov. Root CA – G3 ECC

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

S (State) = Finland

C (Country) = FI

Myndigheten för digitalisering och befolkningsdatas utfärdare av tillfälliga certifikat är:

CN (Common name) = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R

OU (Organizational unit) = Sosiaali- ja terveydenhuollon tilapaisammattivarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

och

CN (Common name) = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E

OU (Organizational unit) = Sosiaali- ja terveydenhuollon tilapaisammattivarmenteet

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Certifikatinnehavarens namngivningspraxis för tillfälliga certifikat för yrkesutbildade personer inom social- och hälsovården:

2.5.4.5 (Serial Number) = Registreringsnummer

SN (Surname) = Efternamn

G (Given name) = Förnamn

T (Title) = Titel

Pseudonum= Identifikationskod (före detta SF-nummer)

UPN (Universal Principal Name) = UPN-namn

CN (Common name) = Efternamn Förnamn Registreringsnummer

C (Country) = FI

Utfärdarens publika nyckel är en del av utfärdarens certifikat. Utfärdarens certifikat är tillgängligt i det offentliga registret. Om det tillfälliga certifikatet finns på ett reservkort, placeras också utfärdarens certifikat på chipset på reservkortet.

Uppgifterna om certifikatinnehavaren anger entydigt certifikatinnehavaren. Utfärdaren utreder vid behov certifikatinnehavarens officiella identitet.

3.1.2 Leverans av privata nycklar till certifikatinnehavaren

En privat nyckel som anknyter till ett tillfälligt certifikat och som skapats med chips eller i en annan säker miljö levereras till certifikatinnehavaren i samband med överlåtelsen.

Reservkortet som innehåller det tillfälliga certifikatet överlåts till certifikatinnehavaren personligen när denne besöker en registrerare som representerar utfärdaren. Innehavaren av det tillfälliga certifikatet ska bevisa sin identitet på ett sätt som motsvarar det förfarande som följs i ansökningsfasen. Identifieringssättet antecknas på mottagningskvittot och förutom kunden ska också den registrerare som överlåter reservkortet underteckna mottagningskvittot.

3.2 Förnyelse av nyckelpar

Publika nycklar på tillfälliga certifikat och privata nycklar på chips kan inte förnyas. För att skapa ett nytt nyckelpar krävs ett nytt tillfälligt certifikat.

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

3.3 Förnyelse av nyckelpar efter införande av certifikat på spärrlista

Publika nycklar på tillfälliga certifikat och privata nycklar på chips kan inte förnyas. Vid förnyelse av tillfälliga certifikat iakttas samma rutiner som vid första ansökan om certifikat.

3.4 Identifiering av den person som gjort begäran om spärrning

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

Begäran om spärrning görs av registreraren i certifikatinnehavarens organisation när denne märker att certifikatet har försvunnit eller om missbruk av certifikatet har varit möjligt.

Certifikatet ska spärras omedelbart när det finns anledning att misstänka missbruk av certifikatet på grund av att det har försvunnit eller stulits.

Alla elektroniska åtgärder vid spärrning arkiveras.

4 Funktionella krav

4.1 Ansökan om certifikat

Rättigheterna och skyldigheterna för certifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden. Ansökningsdokumentet innehåller information om varje parts rättigheter och skyldigheter. När sökanden av det tillfälliga certifikatet söker certifikat, godkänner denne samtidigt de allmänna användningsvillkoren.

I ansökningsdokumentet och användarvillkoren nämns tydligt att sökanden av det tillfälliga certifikatet med sin signatur intygar riktigheten hos uppgifterna samt godkänner att certifikatet skapas och publiceras i det offentliga registret. Samtidigt godkänner sökanden reglerna och villkoren för användning av det tillfälliga certifikatet samt sörjer för förvaringen av det tillfälliga certifikaten och PIN-koderna samt för anmälan om eventuellt missbruk eller försvunnet certifikat/chips.

Man ansöker om ett tillfälligt certifikat genom att personligen besöka ett registreringsställe som är registrerare. Vid ansökan om certifikat kontrolleras identiteten mot ett giltigt dokument som utfärdats av polisen och som styrker personens identitet, till exempel ett ID-kort som utfärdats efter den 11 mars 1999 och pass. Godtagbara identifieringshandlingar är ett giltigt pass eller identitetskort som beviljats av myndighet i en medlemsstat inom EES, Schweiz eller San Marino och ett giltigt pass som beviljats av myndighet i något annat land. Uppgiften om identifieringssättet antecknas på ansökningsblanketten. Vid ansökan om certifikat kontrolleras personens yrkesrättigheter inom hälso- och sjukvården i Terhikki-registret. Tjänstemannen vid registreringsstället bekräftar med sin underskrift att identiteten och yrkesrättigheterna inom social- och hälsovården har kontrollerats.

4.2 Beviljande av certifikat

Utfärdaren beviljar det tillfälliga certifikatet då utfärdaren godkänner certifikatansökan.

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

4.3 Mottagning av certifikat

De tillfälliga certifikaten hämtas personligen från registreringsstället.

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

4.4 Upphörande och avbrott av certifikatets giltighet

4.4.1 Förutsättningar för spärrning av ett certifikat

Det tillfälliga certifikatet ska införas på spärrlista när det finns anledning att misstänka missbruk av certifikatet på grund av att det har försvunnit eller stulits.

4.4.2 Person som gör begäran om spärrning

Begäran om spärrning görs av registreraren i certifikatinnehavarens organisation.

4.4.3 Spärrning

Ett certifikat kan spärras via Myndigheten för digitalisering och befolkningsdatas beställnings- och administrationssystem för kort.

Uppgiften om införandet av certifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärrning har konstaterats vara behörig och godkänd. Spärrlistan gäller i högst 72 timmar.

Spärrning av tillfälliga certifikat

Certifikatinnehavaren ansvarar för spärrningen av certifikat. Ett tillfälligt certifikat kan spärras och då kan det inte längre användas. Däremot kan andra applikationer som eventuellt finns på kortets tekniska underlag användas enligt deras användningsändamål.

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

Spärrade certifikat kan inte tas i bruk igen.

Spärrning av certifikat på uppdrag av Myndigheten för digitalisering och befolkningsdata

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

- Myndigheten för digitalisering och befolkningsdata spärrar de certifikat som den beviljat om ett fel upptäcks i certifikatens datainnehåll.
- Myndigheten för digitalisering och befolkningsdata kan spärra certifikat som undertecknats med dess privata nyckel, om det finns anledning att misstänka att Myndigheten för digitalisering och befolkningsdatas privata nycklar har röjts eller hamnat i fel händer.
- Samtliga gällande servercertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.
- Om den privata 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 också spärra ett certifikat av ett annat särskilt skäl.

4.4.4 Tidpunkten för spärrning

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

4.4.5 Krav på avbrott av certifikatets giltighet

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.6 Person som gör begäran om avbrott

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.7 Begäran om avbrott

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.8 Begränsningar av avbrottstid

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.9 Publiceringsfrekvens för spärrlista

Uppgiften om införandet av certifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärrning har konstaterats vara behörig och godkänd. Spärrlistan gäller i högst 72 timmar.

Spärrlistan innehåller tidpunkten för publicering av nästa spärrlista.

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

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

4.4.10 Krav på kontroll av spärrlista

Den förlitande partens skyldigheter har beskrivits i kapitel 2.1.4.

4.4.11 Kontroll av certifikatets status online

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

4.4.12 Krav på kontroll av certifikatets status online

Utfärdaren erbjuder en onlinekontrolltjänst för certifikatets status.

4.4.13 Särskilda krav gällande avslöjande av certifikatinnehavarens privata nyckel

Certifikatinnehavaren ansvarar för att skydda användningen av sin privata nyckel genom att sörja för sitt chips eller kort och sina koder på det sätt som nämns i användningsvillkoren. Certifikatinnehavaren ska omedelbart anmäla om behovet av att spärra det tillfälliga certifikatet till registreraren i certifikatinnehavarens organisation, om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

4.5 Övervakning av systemet

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

4.6 Arkivering av uppgifter om certifikat

4.6.1 Material som sparas

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas för en del dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i minst 5 år från tidpunkten då certifikaten upphört att gälla. Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa. Utfärdaren arkiverar följande uppgifter:

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

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

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

d) Begäran om spärrning av certifikat.

e) Spärrlistor sparade i det offentliga registret och övrig information om spärrningen av certifikat.

f) Gällande certifikatpolicy och tidigare certifikatpolicyn och motsvarande certifieringspraxis.

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

h) Granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet.

Det arkiverade materialet förvaras enligt de bestämmelser som gäller myndigheten.

4.6.2 Skydd av arkiv

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

4.6.3 Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

4.6.4 Metoder för införskaffning och tryggande av arkiverat material

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

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

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

4.7 Hantering av kontinuerlig verksamhet och undantagsfall

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

4.7.1 Utfärdarens privata nyckel har röjts eller Utfärdarens certifikat har spärrats

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

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

a) Utfärdaren meddelar det inträffade till samtliga innehavare, förlitade parter och avtalskunder eller i övrigt har ett sådant förhållande till utfärdaren på grund av avtalsförhållande eller myndighetsverksamhet att utfärdaren måste informera om det inträffade.

b) Utfärdaren skapar en ny nyckel i enlighet med kapitel 6.

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

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

4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas säkerhetspolicy beaktas åtgärder som förorsakas av problem med den externa säkerheten. Myndigheten för digitalisering och befolkningsdata har fått ISO/IEC 27001-dataskyddscertifikatet, som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även utifall en eventuell katastrof. I samband med beviljande och underhåll av certifikat följer Myndigheten för digitalisering och befolkningsdata de förfaranden som nämns i kapitel 4.7.

4.8 Då utfärdarens verksamhet upphör

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

Utfärdaren meddelar de parter som nämns i punkt a) i kapitel 4.7.1 om att certifikattjänsterna upphör så snart som möjligt, dock minst en månad innan tidpunkten för detta.

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

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

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

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

d) Utfärdaren ansvarar för att uppgifterna enligt lagen om stark autentisering och betrodda elektroniska tjänster arkiveras samt följer också annars bestämmelserna i arkivlagen i fråga om arkivering av uppgifter. Förutom de ovannämnda följer man lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

5 Krav på fysisk, funktionell och personalsäkerhet

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

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. MDB svarar i egenskap av

certifikatutfärdare för säkerheten inom certifikatproduktionen och själva produktionen på ett ändamålsenligt sätt inom samtliga delområden.

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

5.1 Arrangemang kring fysisk säkerhet

5.1.1 Läge och lokalernas egenskaper

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

Säkerheten i verksamhetslokalerna är förverkligad på så vis att obehöriga inte har tillträde till lokalerna.

5.1.2 Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässig uppgifter inom certifikatsystemet utförs är försedda med passagekontroll. Passerkontrollsystemet upptäcker både tillåtet och otillåtet tillträde. Tillträde till maskinsal fordrar autentisering av personen, varvid personen identifieras och hans eller hennes passagerättigheter kontrolleras och händelsen registreras. Maskinsalarna övervakas dygnet runt.

5.1.3 Elmatning och luftkonditionering

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

5.1.4 Brandsäkerhet

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

5.1.5 Förvaring av uppgifterna

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

Uppgifterna har skyddats mot försvinnande, ändring och olovlig användning.

5.1.6 Hantering av onödigt informationsmaterial

Säkerhetsklassificerat informationsmaterial kasseras på ett pålitligt sätt genom att förstöra.

5.1.7 Vattenskador

Maskinsalarna har behöriga detektorer för fuktighet.

5.1.8 Reservarrangemang

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

Tillgången till reservdelar och service för viktig utrustning är säkrad.

5.2 Funktionella krav

5.2.1 Ansvarsfördelning

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

Utfärdarens uppgifter delas in i följande ansvarsområden:

- Datasäkerhetsansvarig
- Registreringsansvarig
- Administratör för systemet
- Användare av systemet
- Övervakare av systemet

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

5.2.2 Antal personer som behövs för uppgifterna

Skapande, aktivering, säkerhetskopiering och returnering av utfärdarens privata nyckel utförs kontrollerat med två personer som fungerar som administratörer för systemet närvarande.

Annullering av utfärdarens privata nyckel är endast möjligt med två berättiga personer närvarande.

Vid formateringen av den kryptografiska modulen för utfärdarens privata nyckel närvarar minst två personer som fungerar som administratörer för systemet.

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

Registrering och autentisering av tillfälliga certifikat fordrar närvaron av en person.

5.2.3 Uppgiftsspecifik autentisering

Registrerare av tillfälliga certifikat:

Registreraren är den organisation med vilken Myndigheten för digitalisering och befolkningsdata har ingått ett avtal om registrering.

Administratör av certifikatsystemet:

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

Användare av certifikatsystemet:

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

5.3 Personlig säkerhet

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

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

5.3.1 Utförande av bakgrundskontroll av personalen

Myndigheten för digitalisering och befolkningsdata utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar med de tekniska leverantörernas certifikatdatasystem.

5.3.2 Förfarande vid utförande av bakgrundskontroll

Personalens arbetserfarenhet kartläggs vid rekryteringen och personen fyller i en blankett som lämnas till skyddspolisen. Med hjälp av denna utförs en säkerhetsutredning av personen.

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

- fylla i en blankett som lämnas in till skyddspolisen, som används för att utföra en säkerhetsutredning för personen
- avstå från uppgifter som strider mot deras skyldigheter och ansvarsområden
- vara personer som inte tidigare har avfärdats på grund av att de försummat eller misskött sina uppgifter

- ha lämplig utbildning för att utföra sina uppgifter.

5.3.3 Krav på utbildning

Personalen på Myndigheten för digitalisering och befolkningsdata ska ha sådan utbildning att de kan utföra sina uppgifter på bästa möjliga sätt. Vid Myndigheten för digitalisering och befolkningsdata finns en utbildningsplan. För förverkligandet av planen svarar Myndigheten för digitalisering och befolkningsdatas administrativa enhet.

5.3.4 Underhåll av expertis och kompetens

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

5.3.5 Krav på uppgiftsrotation

Då utfärdaren planerar arbetsrotation inom sin verksamhet ska uppgifterna organiseras på så vis att den anställda kan utföra sina nya uppgifter på bästa möjliga sätt. I genomförandet av arbetsrotationen beaktas iakttagande av god dataadministration och bevarande av tillräcklig kompetensnivå för de olika uppgifterna.

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

5.3.6 Åtgärder vid avvikelser

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

5.3.7 Personal som representerar organisationen

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

5.3.8 Handlingar som tillhandahålls personalen

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

6 Tekniska säkerhetsarrangemang

6.1 Skapande och sparande av nyckelpar

6.1.1 Skapande av nyckelpar

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

Certifikatutfärdare:

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

Innehavare av certifikat:

Nycklarna skapas i samband med certifieringen. Den privata nyckeln förvaras på reservkortet som läs- och skrivskyddad.

Utfärdaren skapar certifikatinnehavarens nycklar på ett säkert sätt.

6.1.2 Överlåtelse av en privat nyckel till certifikatinnehavaren

Det tillfälliga certifikatet som innehåller certifikatinnehavarens privata nyckel och för vilken den ursprungliga PIN-koden krävs som aktiveringsuppgift, ges till certifikatinnehavaren i samband med registreringen.

Innehavaren av det tillfälliga certifikatet ska bevisa sin identitet på ett sätt som motsvarar det förfarande som följs i ansökningsfasen. Identifieringssättet antecknas på mottagningskvittot och förutom kunden ska också den registrerartjänsteman som överlåter reservkortet underteckna mottagningskvittot.

6.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren

De publika nycklarnas integritet skyddas ända fram till certifieringen. Efter att nycklarna har skapats gör korttillverkaren certifikatbegäran till certifikatsystemet. Certifikatbegäran innehåller uppgifterna om den publika nyckeln och andra uppgifter om certifikatet. Teleförbindelsen mellan systemet för certifikatbegäran och systemet för skapande av begäran krypteras och de personer som startar systemet för certifikatbegäran identifieras med administrationskort som beviljats av Utfärdaren.

6.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren

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

6.1.5 Nycklarnas längder

Utfärdarens privata nyckel som används för att signera tillfälliga certifikat för yrkesutbildade personer inom social- och hälsovården samt den motsvarande publika nyckeln är RSA-nycklar med storleken 4096 bitar och 384 bitar ECC-nycklar.

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

6.1.6 Nycklarnas användningsändamål:

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

Certifikatutfärdarens certifikat:

Ändamål: Underskrift av certifikat och spärrlistor. Den tekniska beskrivningen finns i FINEID S 2-bestämmelserna.

Certifikatinnehavarens verifikations- och krypteringscertifikat

Ändamål: Verifikation av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signaturcertifikat

Ändamål: Elektronisk signatur.

6.2 Skydd av privat nyckel

6.2.1 Standarder som gäller den kryptografiska modulen

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

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

6.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel

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

6.2.3 Överlåtelse av en privat nyckel till förlitande part

Kortinnehavarnas privata nycklar skapas säkert på det sätt som förutsätts för certifikat. Nyckelpar som kortinnehavaren själv har skapat godkänns inte. En privat nyckel kan inte överföras eller kopieras från aktivkortet. Utfärdaren och korttillverkaren kan inte behandla privata nycklar för de personer som de certifierat.

Då nycklar skapas har de ännu inte riktats till en viss person.

6.2.4 Säkerhetskopia av en privat nyckel

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

6.2.5 Arkivering av en privat nyckel

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

6.2.6 Administration av en privat nyckel i kryptografiska moduler

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

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

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

6.3 Andra faktorer som anknyter till nyckeladministration

6.3.1 Arkivering av en publik nyckel

Utfärdaren arkiverar alla publika nycklar som den certifierat.

6.3.2 Användningstid för publika och privata nycklar

Det tillfälliga certifikatets användningstid är i enlighet med avtalet, dock högst tre (3) månader. Certifikatet kan spärras under dess giltighetstid.

6.4 Aktiveringsuppgift

6.4.1 Skapande och ibruktagande av aktiveringsuppgift

Korttillverkaren skapar aktiveringsuppgiften dvs. PIN-koden som möjliggör användningen av nycklarna. Den individuella PIN-koden räknas och överförs till kortet.

6.4.2 Skydd av aktiveringsuppgift

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

6.4.3 Andra faktorer som anknyter till aktiveringsuppgiften

För innehavaren av det tillfälliga certifikatet klargörs att denne har möjlighet att byta den ursprungliga PIN-koden till en ny kod. Utbytesprogrammet för PIN-koden kan avgiftsfritt användas av kortinnehavaren på adressen https://dvv.fi/sv.

Det tillfälliga certifikatet låser sig och användningen förhindras om fel PIN-kod ges tre gånger i rad. En låst PIN-kod kan inte upplösas. Då görs ett nytt reservkort för personen.

6.5 Säkerhetskrav som gäller användning av datorer och tillgång till dessa

6.5.1 Utrustningssäkerhet

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

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

Vid serviceförfarande är utomstående personals tillgång till system och lokaler som serviceproduktionen ansvarar för förhindrad. Servicebesök är endast möjligt för en teknisk leverantör som ingått ett tekniskt leveransavtal och sekretessavtal. Lista över godkända tekniska leverantörer upprätthålls.

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

Certifikatsystemets utrustning övervakas dygnet runt.

6.6 Livscykeladministration av certifikatsystemet

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

6.6.1 Övervakning som gäller systemutvecklingen

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

6.6.2 Hantering av säkerhet

Myndigheten för digitalisering och befolkningsdatas datasäkerhet administreras i enlighet med Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och standarden ISO/IEC 27001.

6.7 Datanätets säkerhet

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

6.8 Övervakning av användning av kryptografisk modul

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

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

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

7 Profiler för certifikat och spärrlistor

7.1 Tekniska uppgifter om certifikat

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

7.2 Profil för spärrlistor

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

8 Hantering av dokument innehållande bestämmelser

8.1 Ändring av bestämmelser

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

8.2 Publicering och information

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

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

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

8.3 Förfarande för ändring och godkännande av certifikatpolicy

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

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

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

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

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

15.9.2023