MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

CERTIFIERINGSPRAXIS SOCIAL HÄLSO YRKESCERTIFIKAT

för yrkescertifikat inom social- och hälsovården

OID: 1.2.246.517.1.10.206.1

6.5.2021

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Dokumenthantering

Ägare	
Utarbetats av	Saaripuu Tuire
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
1.0	Godkänd version 1.0	3.5.2018/TS
1.1	Godkänd version 1.1, Befolkningsregistercentralens namnbyte	1.1.2020/TS
1.2	Uppdaterad version, tillgänglighetsegenskaper	6.5.2021

Innehållsförteckning

1 Inledning

I certifikatpolicyn definieras Myndigheten för digitalisering och befolkningsdatas - här efter certifikatutfärdaren (Certification Authority) – förutsättningar för certifieringsfunktioner enligt öppet nyckelsystem (Public Key Infrastructure; PKI) samt tillämpningsområde och begränsningar. I denna certifieringspraxis fastställs de principer som ingår i certifikatpolicyn på praktisk nivå.

Alla de parters som avses i denna certifieringspraxis ska förutom denna certifieringspraxis 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.

Syftet med denna certifieringspraxis är att beskriva de metoder som säkerställer att certifikat som utfärdas av Myndigheten för digitalisering och befolkningsdata (nedan MDB) är tillförlitliga. I denna certifieringspraxis fastställs förfaringssätten hos utfärdaren och användarna av certifikaten och de allmänna säkerhetskraven med vilka de funktionella, ekonomiska och juridiska hot och risker som anknyter till öppet nyckelsystem, ska minimeras.

Certifikatet kopplar samman den offentliga nyckeln och en mängd uppgifter som identifierar objektet, såsom en person, en organisation, en webbplats eller en apparat. Certifikatet utnyttjas av en yrkesutbildad person inom social- och hälsovården och en förlitande part som litar på att certifikatet är riktigt och som behöver certifikatet till exempel för autentisering av elektronisk signatur.

Detta kapitel definierar certifieringspraxisen och dess lämplighet. I kapitlet definieras också den administrativa organisationen för certifieringspraxisen och dess kontaktinformation.

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

1.1 Bakgrund

MDB beviljar certifikat för yrkesutbildade personer inom hälso- och sjukvården i enlighet med lagen om yrkesutbildade personer inom hälso- och -sjukvården (559/1994). MDB beviljar yrkescertifikat för personer inom socialvården som uppfyller de förutsättningar som beskrivs i lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005) för att arbeta med uppgifter som räknas upp i lagen.

Myndigheten för digitalisering och befolkningsdata erbjuder signatur- och identifieringscertifikat med hög datasäkerhetsnivå samt därtill relaterade tjänster. Med hjälp av certifikat säkerställs certifikatinnehavarens identitet samt riktigheten, enhetligheten och ursprungligheten av de uppgifter som certifikatet innehåller. En elektronisk signatur som gjorts med signaturcertifikat samt en stark elektronisk personidentifiering med en metod för stark elektronisk autentisering ger medborgarna möjlighet till trygg och flexibel nätkommunikation, oberoende av tid och plats. Certifikatutfärdare av

signaturcertifikat och leverantörer av autentiseringstjänster för stark elektronisk autentisering övervakas i Finland av Traficom.

I detta dokument fastställs förfarandekrav som gäller utfärdare av signaturcertifikat samt Myndigheten för digitalisering och befolkningsdata som utfärdar elektroniska identifieringsmedel. Förfarandekrav ställs på verksamheten av utfärdare av certifikat för att beställare, signerare som verifierats av utfärdaren samt parter som litar på certifikatet kan lita på att elektroniska signaturer kan bekräftas med certfikatet.

Utfärdandet av medlet för stark elektronisk autentisering som utfärdas av Myndigheten för digitalisering och befolkningsdata sker i samma produktionsmiljö, med samma tekniska och funktionella lösningar och samma förfarandesätt tillämpas på det som på utfärdandet av signaturcertifikatet som utfärdas av Myndigheten för digitalisering och befolkningsdata.

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.

Myndigheten för digitalisering och befolkningsdata har sedan 1.12.2010 varit lagstadgad certifikatutfärdare för social- och hälsovården med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården, lagen om elektroniska recept samt lagen om befolkningsdatasystemet och Myndigheten för digitalisering och befolkningsdatas certifikattjänster. Från och med 1.4.2015 är Myndigheten för digitalisering och befolkningsdata även lagstadgad certifikatutfärdare för socialvården till följd av ändringar som gjorts i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården.

I skapandet av MDB:s PKI har man utgått från följande bestämmelser, standarder och anvisningar:

- Lag om elektroniska recept
- Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården
- Lag om yrkesutbildade personer inom hälso- och sjukvården
- Lag om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005)
- Lag om stark autentisering och betrodda elektroniska tjänster
- Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)
- Lag om offentlighet i myndigheternas verksamhet (621/1999)

- Lag om säkerhetsutredningar (177/2002)
- IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)
- IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (4/2002)
- ETSI TS 101 456, v 1.4.3: Policy requirements for certification authorities issuing qualified certificates (5/2007)
- ISO/IEC 17090-3: Health informatics - Digital Certificates in Healthcare - Part 3: Policy management of certification authority
- Traficoms föreskrift Kommunikationsverket 72/2016 M Föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster
- Vahti 2/2013 Toimitilojen tietoturvaohje VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen

Vid tolkningen av dokumentet iakttas följande principer:

1. Rubriker och underrubriker i certifieringspraxisen är i huvudsak översättningar av rekommendationer i internationella standarder [RFC 3647]. Vid tolkning av dokumentet ska själva texten prioriteras framför rubrikerna.
2. Ett allmänt krav för certifikatutfärdare är att de uppfyller samtliga krav på utfärdare av certifikat i denna certifikatpolicy.
3. Märket "—" betyder att det inte finns sådana ytterligare villkor för ämnet i fråga som inte skulle ha fastställts i certifikatpolicyn.

1.2 Koder för certifieringspraxisen

Denna certifieringspraxis heter Certifieringspraxis för yrkescertifikat för yrkesutbildade personer inom social- och hälsovården vars OID är 1.2.246.517.1.10.206.1.

Denna certifieringspraxis syftar till Certifikatpolicyn för yrkescertifikat för yrkesutbildade personer inom social- och hälsovården, OID 1.2.246.517.1.10.206.

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 signaturcertifikat enligt Förordningen. I förfarandekrav som fastställs i detta dokument beskrivs användning av medel för skapande av säker signatur.

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 ETSI EN 319 411-1 [2], enligt QSCD; OID: 0.4.0.194112.1.2. Identifierings- och 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.

1.3 Parter och lämplighet

Detta kapitel beskriver de parter som producerar certifikat, utnyttjar certifikat eller är leverantörer av systemet.

1.3.1 Certifikatutfärdare

Utfärdaren uppfyller följande villkor:

- Utfärdaren förbinder sig till att följa villkoren för denna certifieringspraxis.
- Utfärdaren utarbetar certifikatpolicyn och certifieringspraxisen samt andra riktlinjer som kompletterar dessa dokument.
- Certifikatutfärdaren ska ha tillräcklig ekonomisk beredskap för att trygga den verksamhet som anges här. Utfärdaren svarar för certifikatverksamheten och anknytande risker och utgår från att leverantörerna inom certifikatsystemet garderar sig mot risker i verksamheten med hjälp av lämpliga metoder för riskhantering.
- Certifikatutfärdaren för register över registrerare som är godkända av utfärdaren.
- Utfärdaren beslutar om korscertifiering i samråd med övriga utfärdare.
- Certifikatutfärdaren svarar för livscykeln hos nyckelpar som är genererade av utfärdaren (generering, lagring, säkerhetskopiering, publicering och återkallande).

Certifikatutfärdaren förbinder sig att:

1. erbjuda certifikat- och registertjänster som definieras i denna certifieringspraxis;
2. erbjuda hanterings- och uppföljningsfunktioner enligt vad som beskrivs i kapitel 4 till 6 i denna certifieringspraxis;
3. förplikta registreringsstället att utföra ett identifieringsförfarande enligt kapitlen 3–4 i denna certifieringspraxis;
4. bevilja certifikat i enlighet med denna certifieringspraxis;
5. efterleva gällande lagar och förordningar och bestämmelser och riktlinjer enligt dessa samt främja rättigheterna för användare av certifikat och förlitande parter;
6. erbjuda en spärrtjänst enligt kapitlen 3-4 i denna certifieringspraxis;

7. se till att tillräckliga och oberoende kontroller i enlighet med certifieringspraxis utförs;

8. svara för att certifikatutfärdarens verksamhet fungerar; och

9. följa alla villkor för denna certifieringspraxis och certifikatpolicyn.

Utfärdaren kan välja att erbjuda extra funktioner eller tjänster som anknyter till certifikatsystemet.

Utfärdaren svarar för att informationen i certifikatet överensstämmer med denna certifieringspraxis.

Utfärdaren inspekterar och godkänner registrerarna och deras personal.

1.3.2 Registrerare

Registrerare som stöder sig på denna certifieringspraxispraxis ska uppfylla följande villkor:

- Registreraren förbinder sig till att uppfylla kraven i denna certifieringspraxis.
- Registreraren ska vara godkända och registrerad av utfärdaren.
- Registreraren ansvarar för identifiering av certifikatsökande.
- Registreraren ansvarar för att man kan lita på personalen som arbetar vid registreringsinstansen. Registreraren införskaffar utredningar om personal som anställs enligt utfärdarens krav för att säkerställa att de går att lita på och ser till att ständigt försäkra sig om att man kan lita på den personal man befullmäktigat. Utfärdaren godkänner personalen vid registreringsinstansen utgående från registrerarens utredningar.

Registrerare ska enligt denna certifieringspraxis förbinda sig till att:

1. efterleva gällande lagstiftning samt bestämmelser och riktlinjer enligt denna;

2. erbjuda hanterings- och uppföljningsfunktioner enligt vad som fordras i kapitel 4 till 6 i denna certifieringspraxis;

3. utföra identifieringsförfarande för certifikatsökanden enligt kapitel 3 till 4 i denna certifieringspraxis;

4. fullfölja avtalade uppdrag och stödja certifikatanvändares och förlitande parters rättigheter; och

5. följa alla villkor för denna certifieringspraxis och de villkor som anknyter till registreringstjänsten.

Registreraren kan erbjuda extra funktioner eller tjänster som har godkänts av certifikatutfärdaren.

Registreraren svarar för alla registreringstjänster som tillhandahålls av registreraren.

1.3.3 Innehavare av certifikat

Innehavaren av yrkescertifikat inom hälsovården kan vara en yrkesutbildad person inom hälso- och sjukvården som har registrerats i centralregistret för yrkesutbildade personer inom hälso- och sjukvården (Terhikki). Innehavare av yrkescertifikat inom socialvården kan vara en yrkesutbildad person inom socialvården som uppfyller behörighetsvillkoren för en yrkesutbildad person inom socialvården. Yrkesrättigheterna inom socialvården kontrolleras på det sätt som Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) har fastställt[1].

En yrkesutbildad person inom social- och hälsovården ska bevisa sin identitet vid ansökan om certifikat på det sätt som beskrivs i punkt 3.2.3 Identifiering av personen och verifiering av giltig yrkesrättighet.

Genom att underteckna certifikatansökan förbinder sig den yrkesutbildade personen inom social- och hälsovården att följa användningsvillkoren för certifikatet. De gällande användningsvillkoren ges till den yrkesutbildade personen inom social- och hälsovården i samband med överlåtelsen av certifikatet.

1.3.4 Part som litar på certifikatet

Förlitande part kan vara ägare av ett sådant datasystem vars dataskyddsmekanismer har byggts för att utnyttja yrkescertifikat för yrkesutbildade personer inom social- och hälsovården.

Den förlitande parten är skyldig att följa de skyldigheter som gäller den förlitande parten i denna certifieringspraxis.

Den förlitande parten förbinder sig att genomföra alla de delar i sitt system som krävs i certifikatpolicyn och certifieringspraxisen (bl.a. kontroll av elektroniska signaturer, kontroll av certifikatleden, kontroll av certifikatets giltighet, antingen kontroll av spärrlistan eller OCPS-tjänsten spärrlistan) och ändra sitt system enligt de uppdateringar som görs i certifikatpolicyn och certifieringspraxisen.

1.3.5 Andra parter

Utfärdaren kan anlita underleverantörer och samarbetspartners som verkar i Finland för att producera certifikattjänster.

1.4 Användningsändamål för certifikat

I detta kapitel fastställs de användningsändamål som certifikatet typiskt används för och som certifieringspraxisen stödjer. Denna certifieringspraxis gäller utfärdaren, registrerarna, certifikatinnehavarna och de förlitande parterna.

De huvudsakliga ändamålen med användningen av certifikat regleras i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården och lagen om

[1] I RP 354/2014 rd föreslås att lagen om yrkesutbildade personer inom socialvården kommer att ersätta lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005) från och med 1.1.2016. Enligt regeringens proposition kontrolleras yrkesrättigheterna hos en yrkesutbildad person inom socialvården i registret över yrkesutbildade personer inom socialvården som upprätthålls av Valvira.

elektroniska recept. Dessutom kan certifikat användas i andra datasystem inom hälsovården och apoteksväsendet.

1.4.1 Tillåtna användningsändamål för certifikat

Yrkescertifikatet består av ett certifikatpar med två användningsändamål som avviker från varandra. Verifikations- och krypteringscertifikatet uppfyller kraven på starkt elektroniskt identifieringsmedel. Signaturcertifikatet som enbart är avsett för signatur uppfyller kraven för signaturcertifikatet. Myndigheten för digitalisering och befolkningsdata garanterar riktigheten av certifikatsökandens identitet.

Denna certifieringspraxis beskriver de detaljerade krav som gäller utfärdande, produktion och ansvarsfördelning gällande signaturcertifikat för elektronisk signatur enligt Förordningen och lagen om stark elektronisk autentisering och betrodda elektroniska tjänster.

Detta dokument beskriver också de lösningar och förfaringssätt som anknyter till utfärdande, produktion och lagring av uppgifter gällande identifikationscertifikatet som utfärdas som ett medel för stark elektronisk autentisering enligt lagen om stark elektronisk autentisering och betrodda elektroniska tjänster och som ingår i yrkescertifikatet genom att följa kraven i produktionsmiljön för signaturcertifikatet.

1.4.2 Förbjudna användningsändamål för certifikat

Enligt social- och hälsovårdsministeriets beslut om ”Användning av e-post inom hälso- och sjukvården” rekommenderas det inte att känsliga, sekretessbelagda patient- och vårduppgifter skickas per e-post. Utgångspunkten är att sekretessbelagd information inte får skickas per e-post ens med patientens uttryckliga samtycke. Det är således inte tillåtet att använda yrkescertifikat för hälsovården för att kryptera eller underteckna e-postmeddelanden som innehåller patientuppgifter.

1.5 Kontaktuppgifter

1.5.1 Den administrativa organisationen för certifieringspraxisen

Denna certifieringspraxis som beskriver utfärdandet av yrkescertifikat inom social- och hälsovården är registrerad av Myndigheten för digitalisering och befolkningsdata.

1.5.2 Kontaktuppgifter

Utfärdarens kontaktuppgifter

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

Myndigheten för digitalisering och befolkningsdata (MDB) Certifikattjänster

PB 123

00531 Helsingfors

www.fineid.fi

1.5.3 Certifieringspraxisens förhållande till certifikatpolicyn

Certifieringspraxisen ska motsvara certifikatpolicyn. Innehållet i certifikatpolicyn är alltid primärt avgörande med avseende på certifieringspraxisen. Kontrollrutinerna gällande certifikatpolicyn och certifieringspraxisen fastställs i kapitel 8.

1.5.4 Förfarande vid godkännande av certifieringspraxis

MDB:s Certifikattjänster fastställer och godkänner certifieringspraxisdokumenten.

1.6 Definitioner och förkortningar

Yrkesrättighet: Med yrkesrättighet avses i denna certifieringspraxis de registrerade yrkesrättigheter som en legitimerad yrkesutbildad person och yrkesutbildad person som beviljats tillstånd samt en studerande kan få med stöd 2 § i lagen om yrkesutbildade personer inom hälso- och sjukvården. Yrkesrättigheten kan vara obegränsad, begränsad eller fråntagen. Yrkesrättigheterna sparas i Terhikki-registret som upprätthålls av Tillstånds- och tillsynsverket för social- och hälsovården (Valvira). Med yrkesrättighet inom socialvården avses i denna certifieringspraxis de yrkesmässiga rättigheter hos innehavare av befattningar i olika yrkesgrupper enligt lagen om behörighetsvillkoren för yrkesutbildad personal inom socialvården (272/2005).

Returnering av nyckel *(Key recovery)***:** Med key recovery avses en situation där en privat nyckel returneras när yrkeskorte gått sönder eller försvunnit. Privata nycklar för yrkeskort inom social- och hälsovården kan inte returneras om nyckeln går sönder eller försvinner.

Hantering av nycklar (Key management)**:** Med hantering av nycklar avses hanteringsförfaranden och -lösningar för utfärdarens nycklar och certifikatinnehavarens verifikations- och krypterings- samt signaturnycklar under deras livscykel. Faser livscykeln är beställning, skapande, utdelning, förvaring, användning, spärrning, förnyelse, arkivering och förstöring av nyckeln.

Integritet (*Integrity*)**:** 1) Uppgifterna eller datasystemet är autentiskt, oförfalskat, har inga interna konflikter, är täckande, aktuellt, riktigt och användbart 2) uppgifterna eller meddelandet har inte ändrats utan befogenhet och eventuella ändringar kan verifieras i registreringskedjan.

Öppet nyckelsystem (PKI Public Key Infrastructure) Den utfärdare som utnämnts i det öppna nyckelsystemet producerar nyckelpar för användare, verifierar dem med sin digitala underskrift, säkerställer certifikatinnehavarens identitet och delar ut certifikaten till användarna, upprätthåller certifikatregistret och spärrlistan samt ger eventuella andra tjänster som anknyter till användningen av systemet. I det öppna nyckelsystemet har varje användare två nycklar som är sammankopplade. Den ena nyckeln är publik och den andra nyckeln är en privat nyckel som endast användaren innehar. Autenticiteten av en uppgift som undertecknats elektroniskt med privat nyckel kan endast autentiseras med en motsvarande publik nyckel, och på motsvarande sätt kan en uppgift som krypterats med mottagarens publika nyckel vid förmedling av information endast ändras till klartext med mottagarens privata nyckel.

Oavvislighet (*Non-repudiation*)**:** Oavvislighet betyder att parternas delaktighet i händelsen eller handlingen kan efteråt bevisas. Oavvislighet säkerställer att den andra parten inte efteråt kan förneka sin verksamhet, till exempel sin elektroniska signatur. Målet med oavvislighet är juridisk bundenhet.

Användbarhet (*Availability*)**:** En egenskap som avspeglar hur säkert ett system, en apparat, ett program eller en tjänst är tillgänglig vid behov.

Konfidentialitet (*Confidentiality*)**:** Endast behöriga personer, organisationer eller processer har tillgång till uppgiften.

Serviceleverantörers personaktör En person som arbetar hos en serviceleverantör inom social- och hälsovården men som inte är en yrkesutbildad person inom social- och hälsovården eller annan anställd inom social- och hälsovården. I gruppen i fråga ingår övriga personer och specialgrupper som använder riksomfattande datasystem, såsom dataskyddsansvariga samt datasystemleverantörer, konsulter osv.

PIN *(Personal identification number)***:** Kod som används för att säkerställa användningsrätten till yrkeskortets nyckelpar. Yrkeskort etinom social- och hälsovården för hälso- och sjukvården har två koder, den ena för verifikation och kryptering och den andra för elektronisk signatur.

Process (Process): En serie av händelser med en viss riktning, ett visst syfte, en viss verkan eller ett visst resultat, till exempel processen för beviljande av certifikat.

PUK (*Pin unblocking key*): En öppningskod som upplåser PIN-koden för ett låst yrkeskort i en situation där PIN-koden har matats fel för många gånger i rad.

Registrerare *(RA, Registration Authority)***:** En berodd instans i det öppna nyckelsystemet som befullmäktigad och auditerad av utfärdaren genomför uppgifter som registrerare. Registreraren upprätthåller ett eller flera registreringsställen för utfärdarens räkning.

Registreringsnummer: Registreringsnummer är en teknisk nummerserie som bildas för alla yrkesutbildade personer inom hälso- och sjukvården som registreras eller har redan registrerats i centralregistret över personer inom hälso- och sjukvården Terhikki. Registreringsnumret används bland annat som identifikationskod för yrkesutbildade personer i elektroniska recept.

Registreringsställe: Ett registreringsställe som kontrollerar certifikatsökandens identitet och yrkesrättigheter inom social- och hälsovården och som ansvarar för utdelningen av yrkeskort, certifikat och PIN-/PUK-koder till användarna enligt certifikatpolicyn och certifieringspraxisen.

Tillstånds- och tillsynsverket för social- och hälsovården (*Valvira*): Valvira är tillstånds- och tillsynsmyndigheten inom social- och hälsovården. Valvira främjar genom styrning och tillsyn tillgodoseendet av rättsskyddet och tjänsternas kvalitet inom social- och hälsovården samt hanteringen av hälsorisker i livsmiljön och hos befolkningen. I Valviras uppgifter ingår också tillsyn över produkter och utrustning för hälso- och sjukvård samt främjande av säker användning av dessa.

Yrkesutbildad person inom social- och hälsovården I denna certifieringspraxis avses med yrkesutbildad person inom social- och sjukvården enligt lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994) en yrkesutbildad person inom hälso- och sjukvården eller en yrkesutbildad person inom socialvården samt en studerande som avses i 2 § 3 mom. i lagen om yrkesutbildade personer inom hälso- och sjukvården och en studerande inom socialvården.

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

Personalkort för social- och hälsovården: Ett aktivkort som beviljats övrig personal inom social- och hälsovården (andra än yrkesutbildade personer inom social- och hälsovården) och som innehåller ett certifikat.

Annan person inom social- och hälsovården: En annan person som arbetar i en verksamhetsenhet inom social- och hälsovården eller en person som utför uppgifter vid en sådan, men som inte är yrkesutbildad person inom social- och hälsovården.

Serviceleverantör inom social- och hälsovården: En verksamhetsenhet inom social- och hälsovården eller en yrkesutbildad person inom social- och hälsovården som arbetar som självständig yrkesutövare.

Aktivkort för social- och hälsovården: Ett aktivkort som beviljats övrig personal inom social- och hälsovården och som innehåller ett certifikat.

Spärrlista *(CRL, Certificate Revocation List)***:** Spärrlistan är en lista över certifikat som spärrats. Ett certifikat spärras när innehavaren av certifikatet begär att certifikatet ska spärras, innehavaren av certifikatet förlorar sin yrkesrättighet som antecknats i certifikatet, yrkeskortet och öppningskoden har försvunnit eller stulits eller certifikatinnehavaren har dött.

Spärrtjänst: Utfärdarens tjänst som spärrar yrkescertifikat inom hälso- och sjukvården enligt begäran om spärrning.

Terhikki-registret: Ett riksomfattande register över yrkesutbildade personer inom hälso- och sjukvården och deras yrkesrättigheter som upprätthålls av Valvira med stöd av lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994).

Autentisering (*Authentication*)**:** Verifikation av autenticiteten av systemets användare (person, organisation, apparat eller system) eller en annan part vid kommunikationen. Allmänna metoder för autentisering av användare är: 1) användaren vet en unik sak, t.ex. ett lösenord) användaren har en unik egenskap, såsom fingeravtryck 3) användaren har ett unikt medel, t.ex. ett ett yrkeskort inom social- och hälsovården.

Identifiering *(Identification)***:** Ett förfarande med vilket till exempel användaren av datasystemet identifieras. Typiskt sker identifieringen genom att kontrollera om den angivna koden eller annan kod hör till de godkända koderna, t.ex. om en person som anmält sig vara användare finns i listan över befullmäktigade användare av datasystemet.

Skyddsnivå: Med skyddsnivå avses nivån av de säkerhetsåtgärder med vilka man förbereder sig för att en incident som hotar säkerheten prövas eller en sådan sker. Typiska uppföljningsobjekt på skyddsnivån är till exempel dataskyddsavvikelser.

System för reservnyckel *(Key escrow)***:** Key escrow är en metod där en säker deponering av verifikationsnycklar är obligatorisk och nyckeln i säker deponering är i vissa situationer användbar utan certifikatinnehavarens samtycke. Säker deponering av privata nycklar för yrkeskort inom social- och hälsovården är inte möjlig.

Certifikat *(Certificate)***:** En datahelhet som utgörs av en publik nyckel hos en aktör i servicenätverket såsom en yrkesutbildad person inom social- och hälsovården eller en serviceproducent inom ett öppet nyckelsystem och identifieringsuppgifter, som certifikatutfärdaren har skapat och signerat med sin privata nyckel. Certifikatets autenticitet kan verifieras med utfärdarens publika nyckel (utfärdarens certifikat).

Certifikatregister: Certifikatregistret är en publik databas dit utfärdaren sparar utfärdarens certifikat, verifikationscertifikaten för yrkesutbildade personer inom social- och hälsovården samt spärrlistorna.

Certifikatled: En kedja av certifikat som behövs för att en person som hör till certifikatförvaltningen kan säkert uträtta ärenden med en annan person som hör till certifikatförvaltningen. Detta görs antingen så att båda utfärdare har en gemensam utfärdare eller att utfärdarna har kommit överens om att de godkänner varandras certifikat.

Certifikatdatasystem (Vartti): Beställnings- och administrationssystem för certifikatkort och certifikat.

Utfärdare *(CA, Certification Authority)***:** En betrodd instans i det öppna nyckelsystemet som producerar nyckelparen för användare av systemet och producerar, undertecknar, utdelar och vid behov spärrar certifikat.

Befolkningsdatasystemet (BDS): Befolkningsdatasystemet är ett riksomfattande register som innehåller grundläggande uppgifter om finländska medborgare och i Finland fast bosatta utlänningar. Systemet innehåller också information om byggnader, byggprojekt och lägenheter samt fastigheter. Befolkningsdatasystemet upprätthålls av Myndigheten för digitalisering och befolkningsdata och magistraterna. Registreringen av uppgifter grundar sig på medborgarnas och myndigheternas lagstadgade anmälningar.

2 Publicering av uppgifter

2.1 Offentligt register

Utfärdaren ansvarar för upprätthållandet av certifikatregistret samt publiceringen av information som fastställs i punkt 2.2. Informationsinnehållet och strukturen i registret följer bestämningen FINEID S5 - Directory Specification.

Administratören av registret ansvarar för tjänster i anknytning till registret enligt avtalet och denna certifieringspraxis.

2.2 Uppgifter som publiceras av utfärdaren

Utfärdaren svarar för att certifieringspolicyn, certifieringspraxisen, certifieringsbeskrivningar och utfärdarens identifikationscertifikat är offentligt tillgängliga på adressen www.fineid.fi. Registertjänsten är en offentlig webbtjänst som innehåller certifikat beviljade av utfärdaren och avsedda för det offentliga registret samt utfärdarens certifikat och spärrlistan. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

2.3 Publiceringsfrekvens

Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen. Hanteringen av ändringar har beskrivits i punkt 9.12 i denna certifieringspraxis Hantering av ändringar i certifieringspraxisen.

Verifikationscertifikaten samt spärrlistorna publiceras i certifikatregistret genast när de har skapats.

2.4 Tillträdesrättigheter

Tillgängligheten av uppgifter som utfärdaren publicerat begränsas inte med tillträdesrättigheter.

3 Identifiering och verifikation

I detta kapitel fastställs den praxis och metoder med vilka personer identifieras och verifieras i beställningsprocessen för ett certifikat.

3.1 Utnämnande av certifikatinnehavare

3.1.1 Utnämnande

Utnämnandet av en yrkesutbildad person inom hälso- och sjukvården i verifikationscertifikatet och signaturcertifikatet har beskrivits i bestämningen THPKI - TS Myndigheten för digitalisering och befolkningsdatas CA-mall och certifikatens datainnehåll inom hälsovården.

Myndigheten för digitalisering och befolkningsdatas rotutfärdare är:

CN (Common name) = VRK Gov. Root CA - G2

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Utfärdaren för Myndigheten för digitalisering och befolkningsdatas yrkescertifikat inom social- och hälsovården är:

CN (Common name) = VRK CA for Social Welfare and Healthcare Prof. Certs

OU (Organizational unit) = Sosiaali- ja terveydenhuollon ammattivarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Certifikatinnehavarens namngivningspraxis:

TITLE (Title) = Titel

O (Organization) = Organisationens namn

SN (Surname) = Efternamn

G (Given name) = Förnamn

SERIALNUMBER (Serial Number) = Enskild tagg

C (Country) = FI

Valfria

CN (Common Name) = Service Namn

Pseudonym (Pseudonum) = Enskild tagg

UPN (User Principal Name) = OID, information

3.1.2 Betydelse av utnämnande

Vid utnämnandet av certifikatinnehavaren används en fysisk persons för- och efternamn som registrerats i Terhikki-registret.

Gruppen av attribut som bildar objektets namnpost i certifikatet är unik och specificerar den yrkesutbildade personen inom hälso- och sjukvården i fråga. Registernumret ges av Valvira som upprätthåller Terhikki-registret. Samtliga yrkesutbildade personer inom social- och hälsovården ska verka under sina egna namn.

3.1.3 Anonym eller pseudonym

Anonyma certifikat beviljas inte heller och certifikat beviljas inte heller för pseudonym, artistnamn eller smeknamn.

3.1.4 Innehåll av namnfälten

Innehållet av namnfälten har fastställts i punk 3.1.1 i denna certifieringspraxis.

3.1.5 Namnpostens unicitet

Namnposten som fastställs i punkt 3.1.1 specificerar den registrerade yrkesutbildade personen inom hälso- och sjukvården. Personens identifikationskod specificerar en yrkesutbildad person inom social- och hälsovården på ett unikt sätt.

3.1.6 Användningsrättighet till produktnamn

—

3.2 Verifikation av personlighet

3.2.1 Metod för att bevisa innehavet av en privat nyckel

De privata nycklarna för en yrkesutbildad person inom social- och hälsovården skapas alltid med hjälp av chipset på yrkeskortet. Yrkeskortet som innehåller de privata nycklarna överlåts till den yrkesutbildade personen inom social- och hälsovården efter att personens identitet har tillförlitligt verifierats på det sätt som avses i punkt 3.2.3 Identifiering av personen och verifikation av giltig yrkesrättighet och efter att certifikatet har registrerats och skapats.

3.2.2 Autentisering av organisation som företräder certifikatsökanden

När det gäller yrkesutbildade personer inom social- och hälsovården krävs inte verifikation av de organisationer som de representerar. Yrkesutbildade personer inom social- och hälsovården kan arbeta vid flera verksamhetsenheter inom social- och

hälsovården, så yrkescertifikatet och yrkeskortet för social- och hälsovården är inte organisationsbundna.

3.2.3 Identifiering av personen och verifikation av giltig yrkesrättighet

Vid ansökan om certifikat kontrolleras identiteten mot ett giltigt dokument som utfärdats av polisen och som styrker personens identitet, till exempel ett ID-kort och pass eller ett körkort som utfärdats efter den 1 oktober 1990. Godtagbara identifieringshandlingar är ett giltigt pass eller identitetskort som beviljats av myndighet i en medlemsstat inom EES, Schweiz eller San Marino, ett giltigt körkort som beviljats efter 1.10.1990 av myndighet i en medlemsstat inom EES och ett giltigt pass som beviljats av myndighet i något annat land. Om sökanden inte har ovannämnda dokument, identifierar polisen sökandens identitet på något annat sätt.

Giltigheten av yrkesrättigheten hos en yrkesutbildad person inom hälso- och sjukvården kontrolleras i centralregistret över yrkesutbildade personer inom hälso- och sjukvården (Terhikki) som upprätthålls av Valvira. Om sökanden av certifikat inom hälso- och sjukvården inte har en giltig yrkesrättighet i Terhikki-registret, beviljas inte certifikatet. Om uppgifter om den yrkesutbildade personen inom hälso- och sjukvården inte har registrerats i Terhikki, ska personen kontakta Valvira för att hans eller hennes yrkesrättigheter ska registreras. Vid kontrollen av uppgifter om yrkesutbildade personer inom socialvården följs Valviras anvisningar tills det riksomfattande registret över yrkesutbildade personer inom socialvården som upprätthålls av Valvira har tagits i bruk. I yrkescertifikatet och yrkeskortet inom social- och hälsovården antecknas endast en yrkesrättighet som sökanden har valt, även om sökanden skulle ha flera giltiga yrkesrättigheter.

3.2.4 Certifikatsökandens uppgifter som utfärdaren inte kontrollerar

Samtliga personuppgifter som behövs i certifikatansökan för en yrkesutbildad person inom hälso- och sjukvården kan hämtas från Terhikki-registret.

3.2.5 Förutsättningar för beviljande av certifikat

Endast en yrkesutbildad person inom hälso- och sjukvården som registrerats av Valvira har rätt att ansöka om yrkescertifikat. Samma krav på Valviras registrering som förutsättning för rätten att ansöka om yrkescertifikat gäller också yrkesutbildade personer inom socialvården efter att centralregistret över yrkesutbildade personer inom socialvården har tagits i bruk. Certifikatsökanden måste ha en giltig yrkesrättighet inom social- och hälsovården för att certifikatet kan beviljas. Eventuella begränsningar av yrkesrättigheten förhindrar inte beviljandet av certifikatet.

3.2.6 Förutsättningar och krav för samarbete mellan utfärdare

Förutsättningar och krav för samarbete mellan utfärdare fastställs i rotutfärdarens certifikatpolicy.

3.3 Identifiering och verifikation vid förnyelse av certifikat

3.3.1 Identifiering och verifikation vid förnyelse av certifikat

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

3.3.2 Identifiering och verifikation efter spärrning av certifikat

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

3.4 Identifiering av den person som gjort begäran om annullering

Begäran om spärrning av certifikat kan göras genom att ringa spärrtjänsten eller skriftligen till certifikatutfärdaren.

När begäran om spärrning görs per telefon eller skriftligen, registreras anmälarens och certifikatinnehavarens uppgifter i certifikatdatasystemet.

Om personen som gör spärrningsbegäran inte kan identifieras på ett tillräckligt pålitligt sätt och det finns en risk för missbruk av certifikatet, ställer utfärdaren spärrning av certifikatet i främsta rummet.

4 FUNKTIONELLA KRAV FÖR HANTERING AV CERTIFIKATETS LIVSCYKEL

Detta kapitel beskriver de krav som ställts för utfärdarens, registrerarens och den yrkesutbildade personen inom hälso- och sjukvården verksamhet. I kapitlet behandlas också spärrning av certifikat.

4.1 Ansökan om certifikat

Yrkescertifikat för social- och hälsovården ansöks personligen hos en organisation som är registrerare.

Uppgifterna i ansökan sparas i utfärdarens certifikatdatasystem.

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

- bevisar sin identitet på ett sätt som fastställs i kapitel 3
- företer sina personuppgifter enligt punkt 3.2.3 i kapitel 3.
- undertecknar ansökningsblanketten.

Registreraren anmäler sökanden om leveranssättet för yrkeskortet och kuvertet med koderna.

4.1.1 Vem som helst kan göra en certifikatansökan

Certifikatansökan kan göras av en yrkesutbildad person inom hälso- och sjukvården som registrerats av Valvira. Kravet på Valviras registrering gäller också yrkesutbildade personer inom socialvården efter att Valvira har fått centralregistret över yrkesutbildade personer inom socialvården färdigt. Fram till att centralregistret över yrkesutbildade personer inom socialvården blir färdigt, följs Valviras anvisningar för verifikation av yrkesutbildade personer inom socialvården.

4.1.2 Processen för beviljande av certifikat och ansvar

Registreringen av uppgifter i certifikatet som beviljas och yrkeskortet sker med ett system som säkerställer uppgifternas integritet.

Datakommunikationsförbindelserna mellan utfärdarens datasystem är skyddade. Personer som använder certifikatdatasystemet identifieras med certifikatkort som utfärdaren beviljat. Datainnehållet i certifikatet består av de uppgifter som angetts på ansökningsblanketten.

Registreraren beviljar certifikatet, när registreraren och sökanden har granskat och godkänt uppgifterna i ansökan med sin underskrift.

Utfärdaren lämnar till sökanden:

- ett yrkeskort som innehåller kortinnehavarens personliga nyckelpar och certifikat

- ett kodkuvert som innehåller de personliga PIN- och PUK-koderna som behövs för att använda yrkeskortet. Dessa är specificerade utifrån sökandens uppgifter.

Dessutom levererar registreraren bruksanvisningen för yrkeskortet till certifikatsökanden.

Registrerarens ansvar vid beviljande av certifikat har beskrivits i punkt 1.3.2.

4.2 Behandling av certifikatansökan

Certifikatansökan behandlas vid registreringsstället utan obefogat dröjsmål.

Registreraren sparar beställningsuppgifterna för certifikatet i utfärdarens certifikatdatasystem.

4.2.1 Identifiering och verifikation

Registreraren identifierar certifikatsökanden enligt kapitel 3 och kontrollerar att det finns en uppgift om personens yrkesrättighet registrerad i Terhikki-registret. Uppgiften om yrkesrättigheten hos en certifikatsökande inom socialvården kontrolleras enligt Valviras anvisningar tills Valviras centralregister över yrkesutbildade personer inom socialvården tas i bruk.

Uppgifterna på ansökningsblanketten kan hämtas från Terhikki-registret och Befolkningsdatasystemet. Det tilltalsnamn som sparas på certifikatet och som sökanden angett samt yrkesrättigheter som registrerats i Terhikki-registret har nämnts i ansökan. På blanketten anger registreraren också uppgifter om produktion och leverans av certifikatet samt de identifieringsdokument som använts för att identifiera sökanden. I fråga om socialvården följs Valviras anvisningar tills centralregistret över yrkesutbildade personer inom socialvården tas i bruk.

4.2.2 Godkännande eller underkännande av certifikatansökan

Ansökan om yrkescertifikat godkänns genom att bevilja certifikatet. Om sökanden saknar förutsättningar för beviljande av certifikatet, beviljas inte certifikatet och ansökan underkänns. Sökanden ska tilldelas beslutet utan dröjsmål och sökanden kan söka ändring i beslutet skriftligen hos utfärdaren.

4.2.3 Behandlingstiden för certifikatansökan

Certifikatansökan behandlas utan obefogat dröjsmål under registreringsställets öppettider.

4.3 Beviljande av certifikat

4.3.1 Utfärdarens uppgifter vid beviljande av certifikat

Tjänstemannen vid registreringsstället inleder processen för beviljande av certifikat. Användningen av certifikatsystemet förutsätter stark identifiering av tjänstemannen. Tjänstemannens åtgärder sparas i logguppgifterna i utfärdarens datasystem.

Uppgifterna vid beviljande av certifikat har beskrivits i punkterna 4.1 och 4.2 i denna certifieringspraxis.

4.3.2 Anmälan om beviljande av certifikat till sökanden

En separat anmälan om beviljande av yrkescertifikat för hälso- och sjukvården ges inte.

4.4 Godkännande av beviljat certifikat

4.4.1 Godkännandeförfarandet för beviljat certifikat ur certifikatsökandens synpunkt

Det förutsätts att certifikatinnehavaren granskar kortet och riktigheten av uppgifterna på certifikatet. Godkännandet av beviljat certifikat förutsätter inga andra åtgärder av certifikatinnehavaren. I problemsituationer ska certifikatinnehavaren kontakta registreringsstället eller stödtjänsttelefonen.

4.4.2 Publikation av certifikatet på uppdrag av utfärdaren

Utfärdaren publicerar de beviljade verifikationscertifikaten i certifikatregistret på det offentliga datanätet på det sätt som beskrivs i punkt 2.1. Signaturcertifikaten publiceras inte i registret.

4.4.3 Anmälan om beviljande av certifikat till andra parter

En separat anmälan om beviljande av yrkescertifikat för social- och hälsovården ges inte.

4.5 Användning av certifikat och nyckelpar

4.5.1 Användning av certifikat och nyckelpar på uppdrag av certifikatinnehavaren

Yrkescertifikat för social- och hälsovården och nyckelpar för dessa är avsedda att användas i datasystem och tjänster inom social- och hälsovården i Finland.

En yrkesutbildad person inom social- och hälsovården ska förbinda sig att agera enligt denna certifieringspraxis vid ansökan och användning av certifikatet.

En yrkesutbildad person inom social- och hälsovården ansvarar i första hand för den skada som han eller hon orsakar:

- genom ett förfarande som strider mot gällande lag, förordning eller bestämmelse eller anvisning som utfärdats med stöd av dessa;
- genom ett förfarande som strider mot certifikatpolicyn eller certifieringspraxisen;
- genom ett förfarande som strider mot användningsvillkoren för de certifikat som denne godkänt;
- genom annan avsiktlig eller vårdlös felaktig användning av certifikatet.

En yrkesutbildad person inom social- och hälsovården ska förvara och hantera sina egna certifikat och nyckelpar samt sina koder och sitt yrkeskort noggrant.

Certifikatinnehavaren ska förhindra att yrkeskortet försvinner eller att koderna avslöjas eller används olovligt.

Eget yrkeskort som finns i kortläsaren får inte lämnas utan övervakning eller ges till någon annan i något som helst fall.

En yrkesutbildad person inom social- och hälsovården ska anmäla spärrtjänsten:

- om yrkeskortet försvinner eller vid misstanke om missbruk.

Om yrkeskortet skadas, ska kortinnehavaren spärra certifikaten på det skadade kortet och hämta ett nytt yrkeskort från registreringsstället. Vid förnyelse av kort iakttas samma rutiner som vid första ansökan om kort och certifikat.

PIN-koder som används för aktivering av nycklar får inte förvaras på samma ställe med yrkeskortet. Certifikatinnehavaren ska byta PIN-koderna, om denne misstänker att koderna kan ha avslöjats för utomstående.

Om koden är låst och PUK-koden som behövs för att öppna den har försvunnit, ska kortinnehavaren besöka registreringsstället för att få öppningskoden. Vid förfrågan om öppningskoden kontrolleras identiteten av kortinnehavaren mot ett officiellt identitetsdokument som utfärdats av polisen. Tjänstemannen vid registreringsstället skriver ut ett nytt kodkuvert som innehåller öppningskoden. Öppningskoden lämnas inte per telefon eller brev av dataskyddsskäl.

4.5.2 Användning av certifikat och publika nycklar på uppdrag av en förlitande part

Den förlitande parten ansvarar när det gäller de egna datasystemen för att säkerställa att certifikatet används för det ändamål som fastställs i denna certifieringspraxis. Vid säkerställande av riktigt användningsändamål för certifikatet kan den förlitande parten stödja sig på den referens till denna certifieringspraxis som ingår i certifikatet.

Den förlitande parten ska säkerställa att de använda applikationerna uppfyller kraven i denna certifieringspraxis.

Den förlitande parten ansvarar för att kontrollera certifikatet på ett behörigt sätt genom hela certifikatvägen enligt bestämningen IETF RFC 3280. Om utfärdaren och den förlitande organisationen har kommit överens om extra tjänster som gäller användningen av certifikatet, förbinder sig den förlitande parten att följa villkoren för extra tjänster.

Innan ett certifikat godkänns ska den förlitande parten kontrollera att certifikatet gäller och inte är spärrat.

Den förlitande parten ansvarar för att kontrollera giltigheten av certifikatet, giltigheten av spärrlistan eller OCSP-tjänsten. Ett certifikat är inte tillförlitligt, om inte den förlitande parten inte kontrollerar de spärrade certifikaten på följande sätt:

1. Den förlitande parten ska kontrollera certifikatstigen för spärrlistan och äktheten av spärrlistan utifrån utfärdarens digitala underskrift.

2. Den förlitande parten ska kontrollera giltighetstiden av spärrlistan för att säkerställa att spärrlistan är giltig.

3. Certifikaten (den publika nyckeln) kan sparas lokalt i den förlitande partens system,. men certifikatets giltighet ska kontrolleras innan certifikatet godkänns.

Om en giltig spärrlista inte är tillgänglig på grund av en störning i systemet eller tjänsten, får certifikat enligt denna certifieringspraxis inte godkännas. Om den förlitande parten trots detta godkänner certifikatet, sker godkännandet på den förlitande partens eget ansvar.

4.6 Ny certifiering av en publik nyckel

Yrkescertifikat beviljas inte för tidigare certifierade publika nycklar.

4.7 Förnyelse av certifikat

4.7.1 Orsaker till förnyelse av certifikat

Certifikatet för yrkesutbildade personer inom social- och hälsovården kan förnyas när det föregående certifikatets giltighet upphör, om de förutsättningar för beviljande av certifikat som beskrivs i punkt 3.2.5 fortfarande är giltiga.

Certifikat kan också förnyas när uppgifter om yrkesrättigheten eller andra uppgifter som påverkar certifikatets datainnehåll ändras eller om yrkeskortet skadas. I sådana fall ska certifikatinnehavaren kontakta registreringsstället och ansöka om ett nytt yrkeskort och yrkescertifikat på det sätt som beskrivs i kapitel 4.

4.7.2 Ansökan om förnyelse av certifikat

Endast certifikatinnehavaren kan ansöka om förnyelse av certifikatet.

4.7.3 Hantering av begäran om förnyelse av certifikat

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

4.7.4 Anmälan om förnyelse av yrkeskort till certifikatsökanden

En separat anmälan om förnyelse av yrkescertifikat för social- och hälsovården ges inte.

4.7.5 Förfarande för godkännande av förnyat certifikat ur certifikatinnehavarens synpunkt

Det förnyade certifikatet godkänns enligt det förfarande som beskrivs i punkt 4.4.1.

4.7.6 Publikation av ett förnyat certifikat

Certifikaten publiceras enligt det förfarande som beskrivs i punkt 4.4.2.

4.7.7 Anmälan om beviljande av förnyat certifikat till andra parter

En separat anmälan om förnyelse av yrkescertifikat för social- och hälsovården ges inte.

4.8 Ändring av certifikat

Datainnehållet i ett certifikat kan inte ändras efter genereringen av certifikatet. När de uppgifter som påverkar datainnehållet i certifikatet ändras kan certifikatinnehavaren ansöka om ett nytt yrkescertifikat och yrkeskort enligt kapitel 4.7.

4.9 Spärrning och tillfällig spärrning av certifikat

Utfärdaren upprätthåller en spärrtjänst för certifikat som är tillgänglig 24 timmar per dygn, 7 dagar i veckan. Uppgifterna om spärrade certifikat upptas på en spärrlista som utfärdaren signerar och som publiceras i ett offentligt register. Certifikatet kan inte spärras tillfälligt.

Utfärdaren anmäler en yrkesutbildad person inom social- och hälsovården om spärrning av certifikat, när spärrningen beror på förlust av yrkesrättighet.

Spärrning av certifikatet annullerar inte de elektroniska signaturer som gjorts med certifikatet före spärrningstidpunkten.

4.9.1 Förutsättningar för spärrning av ett certifikat

Ett certifikat spärras om:

- innehavaren av certifikatet begär att certifikatet spärras
- certifikatinnehavaren förlorar en registrerad yrkesrättighet
- yrkeskortet har skadats, försvunnit eller stulits
- öppningskoden samt yrkeskortet har försvunnit eller stulits
- certifikatinnehavaren har dött.

Utfärdaren kan spärra certifikatet för yrkesutbildade personer inom social- och hälsovården, om certifikatet har använts i strid mot denna certifieringspraxis, lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården, lagen om elektroniska recept samt mot de författningar eller krav och anvisningar som utfärdats med stöd av dessa.

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

4.9.2 Behörig att begära spärrning

Behörig att begära spärrning av certifikat är:

- den yrkesutbildade personen inom social- och hälsovården eller hans eller hennes lagstadgade representant i fråga om personens eget certifikat;
- utfärdaren om förutsättningarna i punkt 4.9.1 uppfylls.

4.9.3 Spärrning av certifikat

Certifikatinnehavaren begär att spärrtjänsten spärrar certifikatet. Begäran görs:

1. Per telefon genom att ringa den avgiftsfria spärrtjänsten +358 800 162 622.

2. Skriftligen till certifikatutfärdaren.

Personen som gjort begäran om spärrning av certifikatet identifieras på det sätt som beskrivs i punkt 3.4.

Utfärdaren av certifikat spärrar certifikaten om:

- om innehavaren av certifikatet förlorar sin yrkesrättighet eller
- om innehavaren av certifikatet har dött.

Följande uppgifter antecknas om spärrningen av certifikat:

- personuppgifter som innehavaren av det spärrade certifikatet har tillgång till
  - efternamn och förnamn
  - registreringsnummer, personbeteckning
- personuppgifter om den person som gjort begäran om spärrning (om annan än certifikatinnehavaren)
- på vilket sätt den person som gör begäran om spärrning har identifierats
- tidpunkten för begäran om spärrning
- orsaken till begäran om spärrning antecknas när begäran om spärrning görs av någon annan än certifikatinnehavaren; certifikatinnehavaren behöver inte ange orsaken till begäran om spärrning
- personuppgifter för mottagaren av spärrningsbegäran
- eventuella övriga uppgifter som certifikatinnehavaren uppgett
  - tidpunkten då yrkeskortet har svunnit, certifikatinnehavarens dödstid eller motsvarande
- personuppgifter för den som spärrat certifikatet
- tidpunkten för spärrning av certifikatet.

Certifikatutfärdaren informerar certifikatinnehavaren om spärrat certifikat endast om spärrningen av certifikatet beror på förlust av yrkesrättighet. Certifikatet spärras genom certifikatsystemet och uppgifterna om spärrningen förvaras i 5 år efter spärrningstidpunkten.

4.9.4 Certifikatinnehavarens skyldighet att begära spärrning

Certifikatinnehavaren ska utan dröjsmål lämna en begäran om spärrning till spärrtjänsten, om de förutsättningar för spärrning som beskrivs i punkt 4.9.1 uppfylls.

4.9.5 Hanteringstid för begäran om spärrning av ett certifikat

Spärrtjänsten behandlar begäran om spärrning av certifikat utan dröjsmål.

4.9.6 Förlitande parters skyldighet att kontrollera giltigheten för certifikat

Innan ett certifikat godkänns ska den förlitande parten kontrollera att certifikatet gäller och inte är spärrat.

Den förlitande parten ansvarar för att kontrollera giltigheten av certifikatet antingen via OCSP-tjänsten eller den giltiga spärrlistan. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat spärrlistan.

4.9.7 Publiceringsfrekvens för spärrlista

En uppdaterad spärrlista publiceras varje timme

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

4.9.8 Maximal giltighetstid för spärrlista

Den uppdaterade spärrlistan är giltig i högst 72 timmar. I varje spärrlista anges när giltighetstiden går ut.

4.9.9 Kontroll av certifikatets status i realtid

Kontroll av certifikatets status i realtid är i bruk.

4.9.10 Krav för kontroll av certifikatets status i realtid

Certifikatets status kan kontrolleras i realtid i OCSP-tjänsten eller spärrlistan.

4.9.11 Andra kontrollåtgärder för certifikatets status

Certifikatets status kan kontrolleras i realtid i OCSP-tjänsten eller spärrlistan.

4.9.12 Spärrning av certifikat på grund av avslöjande av privat nyckel

Spärrning av certifikat på grund av avslöjande av privat nyckel avviker inte från spärrning av certifikat på andra grunder.

4.9.13 Spärrning av certifikat för en bestämd tid

Certifikat kan inte spärras för en bestämd tid.

4.9.14 Vem kan begära om spärrning för en bestämd tid

—

4.9.15 Förfaringssätt för spärrning av certifikat för en bestämd tid

—

4.9.16 Begränsningar för spärrning av certifikat för en bestämd tid

—

4.10 Möjlighet att kontrollera certifikatets status

Certifikatet status kontrolleras med hjälp av OCSP-tjänsten eller spärrlistan. Den förlitande parten ska också kontrollera att certifikatets giltighet inte har upphört.

4.11 Upphörande av certifikatets giltighet

Kortet är i kraft antingen under en allmänna giltighetstiden, en certifikatsspecifik frist eller tills det spärras när kriterierna för spärrning uppfylls.

4.12 System för reservnyckel och återlämning av nycklar

Säker deponering av krypteringsnycklar för yrkesutbildade personer är inte möjlig. Certifikaten kan således inte användas utan certifikatinnehavarens samtycke och privata nycklar kan inte återlämnas om kortet skadats eller försvunnit.

5 Hantering av fysisk, användnings- och personalsäkerhet

Myndigheten för digitalisering och befolkningsdatas datasäkerhet administreras i enlighet med Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och standarden ISO 27001:2005.

5.1 Hantering av fysisk säkerhet

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.

5.1.1 Placering och konstruktion av lokaler

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 tillgångskontroll

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 El och luftkonditionering

Systemen för certifikatproduktion ligger i maskinsalarna med eltillförsel och luftkonditionering som säkerställts med reservkraft. Om tillgång till bränsle i undantagssituationer ska det finnas ett leveransavtal.

5.1.4 Vattenskada

Systemen för certifikatproduktion ligger i maskinsalar med upphöjda golv och kabelupphöjningar under golvet samt med ett övervakningssystem som upptäcker vattenskadorna.

5.1.5 Eldsvåda

Systemen för certifikatproduktion ligger i maskinsalar försedda med automatisk släckning.

5.1.6 Förvaring av datamedier

Datamedier som används vid registreringsställen och certifikatproduktionen, såsom hårddiskar, disketter, flash-minnen och optiska minnen med sekretessbelagd information, ska hanteras och förvaras enligt samma krav som sekretessbelagt pappersdokument. En uppgift eller ett dokument är sekretessbelagt om så har föreskrivits i lagen om offentlighet i myndigheternas verksamhet.

5.1.7 Förstörande av datamedier

Datamedier som innehåller sekretessbelagd information och som använts vid registreringsställen och certifikatproduktionen förstörs i ett tillämpligt företag inom branschen. Intygen över förstörande av datamedier arkiveras.

5.1.8 Säkerhetskopiering över nätet

Säkerhetskopieringen av certifikatproduktionssystemet sker i certifikatsystemets interna datakommunikationsnät.

5.2 Hantering av användningssäkerhet

Utfärdaren har helhetsansvar för de administrativa och logistiska funktioner som anknyter till beviljande av certifikat och publikation av spärrlistor. Funktioner kan utföras också av en annan organisation på uppdrag av utfärdaren.

5.2.1 Roller i arbetsuppgifter

Arbetsuppgifterna för utfärdaren och de underleverantörer som utfärdaren anlitar har fördelats så att risken för oavsiktligt och avsiktligt missbruk av information och tjänster minskas. Arbetsuppgifterna i certifikatverksamheten har delats in i roller och var och en har endast de rättigheter till systemet som deras roller tillåter.

Roller i certifikatverksamheten är:

- huvudanvändare av systemet
- användare av systemet
- registrerare och
- auditerare.

5.2.2 Antal personer som behövs för arbetsuppgifter inom certifikatproduktion

Utsedda organisationer och personer som arbetar för utfärdaren.

I skapandet och administrationen av utfärdarens nyckelpar ska delta minst två personer. För ändringar som görs i certifikatsystemet på systemnivå krävs minst två personer. För identifiering och registrering av certifikatsökande behövs en person.

5.2.3 Identifiering och verifikation av personer för olika roller

Personer som arbetar med utfärdarens arbetsuppgifter som nämns i punkt 5.2.1 har ett personligt administrationskort som har skyddats med PIN-kod i sitt bruk. Personens rätt att använda certifikatsystemet eller andra system som anknyter till certifiering verifieras med hjälp av dessa administrationskort.

5.2.4 Roller som kräver separering av uppgifter

En registrerare kan inte ha rollen som huvudanvändare av systemet.

5.3 Hantering av personalsäkerhet

5.3.1 Bakgrunds-, förtjänst-, erfarenhets- och utredningskrav

Systemanvändarnas arbetsuppgifter är kritiska med tanke på säkerheten, eftersom de skapar och hanterar certifikat- och nyckeluppgifter. En person som arbetar med systemanvändarens uppgifter ska vara lämplig för arbetsuppgifterna och förstå betydelsen av säkerheten i sitt vardagliga arbete. Organisationer som utfärdaren befullmäktigat sörjer för tillförlitligheten hos sin personal.

En säkerhetsutredning av personer som arbetar med utfärdarens arbetsuppgifter utförs.

5.3.2 Förfarande för kontroll av bakgrund

Organisationer som utfärdaren befullmäktigat sörjer och ansvarar själva för kontrollen av bakgrunden samt tillförlitligheten hos sin personal.

5.3.3 Utbildningsfrekvens och -krav

Utfärdaren och organisationer som arbetar för utfärdaren sörjer själva för att personalen får tillräcklig utbildning. Utfärdaren ordnar utbildning för registrerare som arbetar vid registreringsställen.

5.3.4 Fortutbildningsfrekvens och -krav

—

5.3.5 Frekvens och ordning av rotation av arbetsuppgifter

—

5.3.6 Följder av olovliga åtgärder

Förutom lagstadgade påföljder förlorar en person som agerat olovligt permanent användningsrättigheterna till utfärdarens system.

5.3.7 Krav på underleverantörers personal

Personalen i organisationer som utfärdaren befullmäktigat ska uppfylla kraven i punkt 5.3.1.

5.3.8 Dokument som levereras till personalen

Personalen som deltar i certifikatverksamheten har förutom denna certifieringspraxis också certifikatpolicyn och nödvändiga verksamhetsanvisningar till sitt förfogande.

5.4 Uppföljning av certifikatsystemets säkerhet

De förfaranden för uppföljning av säkerheten som beskrivs i detta kapitel binder alla anläggnings- och systemhelheter som förknippas med processen för beställning och beviljande av certifikat.

5.4.1 Händelser som arkiveras

Utfärdaren förvarar följande uppgifter för säkerhetsuppföljning:

1. Skapande av användningsrättigheter på systemnivå och försök att bryta mot befogenheterna.

2. Åtgärdsbegäran gällande uppdatering och upprätthållande av systemet.
3. Installering av ett nytt program eller uppdatering av ett program.
4. Klockslaget och datumet för alla säkringar samt andra beskrivande uppgifter.
5. Stängning, start och stopp av certifikatsystemet.
6. Klockslaget och datumet för alla uppdateringar av anläggningar.

I fråga om certifikat och certifikatsystemet förvarar utfärdaren:

1. Alla händelser som förknippas med skapande och spärrning av certifikat, även certifikat som utfärdaren använder i sin verksamhet.
2. Alla händelser som förknippas med hantering av signaturnycklar för certifikat.
3. Alla meddelanden från registreringstjänsten, utdelningstjänsten för certifikat och extra tjänster som inte förknippas med hanteringen av systemet
4. Start och nedkörning av loggsystemet.
5. Ändringar i inställningarna för loggsystemet.

5.4.2 Analyseringsfrekvensen av logguppgifter

Logguppgifter analyseras vid behov.

5.4.3 Förvaringstiden för logguppgifter

Logguppgifterna förvaras i enlighet med gällande arkivbestämmelser.

5.4.4 Skydd av logguppgifter

Endast separat berättigade personer har tillgång till logguppgifterna.

Logguppgifterna skyddas mot ändring, förstörelse, skador och osaklig användning.

5.4.5 Säkerhetskopiering av logguppgifter

Logguppgifterna säkerhetskopieras varje dag.

5.4.6 Genomförande av insamlingssystemet för logguppgifter (intern/extern)

Utfärdaren ansvarar för insamlingssystemet för logguppgifter.

5.4.7 Anmälan om logghändelse

Systemanvändaren får ingen separat anmälan om logghändelser.

Personer som ansvarar för övervakningen av logguppgifter underrättas separat om följande händelser:

- försök att bryta mot befogenheterna;
- stängning, start och stopp av systemet;
- installering eller uppdatering av ett program.

5.4.8 Utvärdering av sårbarheter

Utfärdaren utvärderar och uppföljer sårbarheten av certifikatsystemet och produktionsmiljön med hjälp av en riskanalys och strävar efter att minimera risker som anknyter till dessa.

5.5 Material som arkiveras

5.5.1 Dokument, filer och medier som arkiveras

Utfärdaren arkiverar följande uppgifter:

- certifikatansökningar
- undertecknade godkännanden av certifikatansökan eller annan ansökan
- avtal om certifikattjänster
- beviljade certifikat
- korscertifieringsdokument, inklusive motiveringar till korscertifiering och beslut samt vidtagna åtgärder
- begäran om spärrning av certifikat
- gällande och föregående certifikatpolicy och certifieringspraxis
- avtal mellan utfärdaren och registreringsställen och
- avtal om upprätthållande, användning och administration av certifikatsystemet

5.5.2 Förvaringstiden för arkiv

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Vid arkivering tillämpas också bestämmelserna i lagen om elektronisk kommunikation i myndigheternas verksamhet.

5.5.3 Skydd av arkiv

Endast separat berättigade personer har tillgång till arkivuppgifterna. Dokumenten, filerna och de övriga medierna förvaras i en brandsäker lokal försedd med passagekontroll dit endast personer befullmäktigade av utfärdaren har tillgång till.

Arkivuppgifterna skyddas mot ändring, förstörelse, skador och osaklig användning.

5.5.4 Säkerhetskopiering av arkiven

Endast arkivuppgifter i elektronisk form säkerhetskopieras.

5.5.5 Tidsstämpel för arkivuppgifter

Dokument som arkiveras är daterade. Tidsstämpeltjänsten är för tillfället inte i bruk.

5.5.6 Insamlingssystemet för arkivuppgifter (intern/extern)

Utfärdaren har inget insamlingssystem för arkivuppgifter.

5.5.7 Tillgängligheten och integriteten av arkivuppgifterna

Endast separat berättigade personer har tillgång till arkivuppgifterna. Arkivuppgifterna skyddas mot ändring, förstörelse, skador och osaklig användning.

5.6 Byte av utfärdarens nyckelpar

Utfärdaren skapar ett nytt nyckelpar och utfärdarens certifikat senast fem år och tre månader innan det föregående certifikatets giltighetstid löper ut. Utfärdarens certifikat förs in i det offentliga registret enligt kapitel 2. Dessutom har utfärdarens certifikat sparats på chipset på yrkeskortet.

5.7 Förberedelse inför störningssituationer

5.7.1 Plan för funktionsstörningar och äventyrande av verksamheten

Utfärdaren har en kontinuitets- och återhämtningsplan som möjliggör en störningsfri kontinuitet i verksamheten och återhämtning av utfärdarens system från olyckor. Det finns tydliga ansvar, planer och anvisningar för störnings- och undantagssituationer.

5.7.2 Skada på certifikatsystemet, programmen eller uppgifterna

I undantagssituationer följer utfärdaren kontinuitets- och återhämtningsplanen.

5.7.3 Förfaranden vid avslöjande av certifikatinnehavarens privata nyckel

Certifikatinnehavarens privata nycklar är skyddade mot fysisk intrång och avslöjande av nycklar. Om certifikatinnehavarens privata nyckel har avslöjats, spärras certifikatet. Ett nytt yrkeskort med nya privata nycklar skapas för certifikatinnehavaren.

5.7.4 Kontinuiteten av verksamheten efter störningssituation

Utfärdaren strävar efter att få kärnfunktionerna i systemet att fungera utan dröjsmål. 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.

5.8 Nedläggning

5.8.1 Nedläggning av utfärdarens verksamhet

Nedläggning av utfärdarens verksamhet är en situation där utfärdarens verksamhet läggs ned permanent. En situation där utfärdarens tjänster överförs från en organisation till en annan eller där utfärdaren beviljar en ny utfärdares certifikat anses inte som nedläggning av utfärdarens verksamhet.

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

- Samtliga gällande certifikat annulleras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast annullerade certifikatets giltighetstid har löpt ut.

- Utfärdaren upphäver samtliga avtalspartners befogenheter för att utföra åtgärder med anknytning till hantering av livscykeln av certifikat för utfärdarens del.
- Utfärdaren ser till att tillgången till utfärdarens arkiv enligt punkt 5.5.7 bevaras även efter att utfärdarens verksamhet har upphört.
- Spärrlistorna finns tillgängliga på angivet sätt under deras giltighetstid.

5.8.2 Nedläggning av registrerarens verksamhet och rättigheter

Nedläggning av registrerarens verksamhet och rättigheter är en situation där den rättighet att registrera yrkescertifikat för social- och hälsovården som utfärdaren beviljat en organisation inom hälso- och sjukvård upphör permanent.

Nedläggningen av registrerarens verksamhet sker enligt avtalet mellan registreraren och utfärdaren.

6 Hantering av teknisk säkerhet

I detta kapitel behandlas villkoren för hantering av publik och privat nyckel för utfärdaren, registreraren och den yrkesutbildade personen inom social- och hälsovården och motsvarande tekniska bestämningar.

Nyckelparet för den yrkesutbildade personen inom social- och hälsovården kan skapas av utfärdaren eller en annan organisation befullmäktigad av utfärdaren. I alla fall uppföljer utfärdaren hur villkoren för skapande av nyckelpar uppfylls och ansvarar för att nyckelparet fungerar.

6.1 Skapande och leverans av nyckelpar till certifikatinnehavaren

6.1.1 Skapande av nyckelpar

Utfärdarens nyckelpar skapas och förvaras i kryptografiska moduler som är i enlighet med allmänt erkända standarder som Europeiska gemenskapernas kommission har bekräftat och som publicerats i Europeiska unionens officiella tidning, såsom godkännande på nivå FIPS 140-1 eller 140-2 level 3.

Nyckelparen för certifikatinnehavaren skapas med yrkeskortets chips.

Den trygga processen för att skapa och lagra nyckelpar förhindrar att nyckeln röjs utanför det system som används för att skapa nyckeln.

6.1.2 Leverans av en privat nyckel till en yrkesutbildad person inom hälso- och sjukvården

Yrkeskortet som innehåller de privata nycklarna och koderna som behövs för att använda det levereras till den yrkesutbildade personen inom hälso- och sjukvården på så vis att det inte är möjligt för utomstående att komma åt dem.

6.1.3 Leverans av certifikatsökandens publika nyckel till utfärdaren

Certifikatsökandens publika nyckel överförs mellan utfärdarens system genom att använda en säker dataförbindelse.

6.1.4 Leverans av utfärdarens publika nyckel till förlitande parter

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren. Utfärdarens certifikat sparas också på yrkeskort för hälso- och sjukvården.

6.1.5 Nycklarnas längd

Utfärdarens nycklar är RSA-nycklar med 4096 bitar.

Signaturnycklarna för yrkesutbildade personer inom social- och hälsovården samt verifikationsnycklarna är RSA-nycklar med 2048 bitar.

6.1.6 Skapande och kvalitet av parametrar för publik nyckel

Vid skapande av nyckelpar används standardiserade, högklassiga, kända och testade metoder och kryptografiska moduler.

6.1.7 Nycklarnas användningsändamål:

Användningsändamålen för utfärdarens nyckelpar är signatur av certifikat och signatur av spärrlista.

Användningsändamålen för nyckelparet för en yrkesutbildad person inom hälso- och sjukvården är verifikation av certifikatinnehavaren och kryptering av information samt utvecklad elektronisk signatur.

6.2 Skydd av privat nyckel och hantering av kryptografiska moduler

6.2.1 Använda standarder

Utfärdarens privata nycklar förvaras krypterade i kryptografiska moduler (HSM) som förvaltas av utfärdaren och som uppfyller kraven enligt FIPS 140-1 eller 140-2 level 3. Utfärdarens privata nycklar är skyddade mot röjning och missbruk.

Utfärdaren säkerställer att den privata nyckeln på certifikatkortet för en yrkesutbildad person inom social- och hälsovården levereras till den yrkesutbildade personen inom social- och sjukvården enligt förfaranden i denna certifieringspraxis.

Yrkeskortet för en yrkesutbildad person inom social- och hälsovården är i enlighet med giltiga tillämpliga standarder, såsom ISO/IEC 7816 och IAS ECC v 1.01.

Yrkeskortets chips och dess operativsystem är säkerhetscertifierat. Godkända säkerhetscertifikat är FIPS 140-1 eller 140-2 level 3 eller det högre Common Criteria EAL4+ och ISO/IEC 15408.

6.2.2 Privat nyckel i flera personers besittning

För hantering av utfärdarens privata nycklar krävs åtminstone två personer som är berättigade för hantering av nycklar.

Den privata nyckeln för registreraren och en yrkesutbildad person inom social- och hälsovården kan hanteras och användas endast av innehavaren av nyckeln.

6.2.3 System för reservnyckel för privata nycklar

Reservkortsystemet för yrkeskort för social- och hälsovården är inte i bruk.

6.2.4 Säkerhetskopiering av en privat nyckel

Det görs en säkerhetskopia på certifikatutfärdarens privata nyckel.

Säkerhetsegenskaperna och förvaringen av certifikatutfärdarens säkerhetskopierade privata nyckel motsvarar säkerhetskraven för utfärdarens privata originalnyckel i samtliga situationer.

Kopior av privata nycklar för yrkesutbildade personer inom social- och hälsovården tas eller förvaras inte.

En privat nyckel för yrkesutbildade personer inom social- och hälsovården röjs inte för utomstående i någon fas av yrkeskortets livscykel, och privata nycklar för yrkesutbildade personer inom social- och hälsovården förvaras inte någon annanstans än på yrkeskortet för social- och hälsovården.

6.2.5 Arkivering av privata nycklar

Utfärdarens privata nycklar förstörs efter att deras giltighetstid har upphört.

Privata nycklar för yrkesutbildade personer inom social- och hälsovården arkiveras inte. Utfärdaren har inte tillgång till certifikatinnehavarnas privata nycklar.

6.2.6 Hantering av privata nycklar i kryptografiska moduler

Utfärdaren har rätt att flytta utfärdarens privata nycklar till en annan kryptografisk modul vid service eller byte av originalutrustningen.

6.2.7 Förvaring av privata nycklar

Utfärdarens privata nycklar förvaras krypterade i kryptografiska moduler.

Certifikatinnehavarens privata nycklar förvaras på yrkeskortets chips så att de inte kan läsas, ändras, kopieras eller överföras.

6.2.8 Aktivering av privata nycklar

Aktivering av utfärdarens privata nycklar utförs av för uppdraget befullmäktigade personer med kontrollkort i de kryptografiska modulerna.

Certifikatinnehavarens privata nycklar är skyddade mot röjning och olovlig användning med yrkeskortets chips. Bara interna kommandon som utförs med chipset ger tillgång till de privata nycklarna.

För att kommandot som gäller de privata nycklarna ska kunna utföras, måste nyckeln i fråga ha aktiverats med rätt PIN-kod.

PIN-koden på yrkeskortet låses efter att koden matats fel fem gånger.

Låsningen av PIN-koden på yrkeskort kan öppnas med rätt öppningskod.

6.2.9 Förhindrande av användning av privata nycklar

Användningen av certifikatutfärdarens privata nycklar kan förhindras av personer som är behöriga för uppgiften med hjälp av kontrollkort eller genom bortkoppling av strömmen till den kryptografiska modul som innehåller utfärdarens privata nycklar.

Användning av yrkeskortets privata nycklar förhindras genom att avlägsna yrkeskortet från kortläsaren.

6.2.10 Förstörande av en privat nyckel

Bara certifikatutfärdaren kan förstöra utfärdarens privata nycklar.

När certifikatutfärdarens verksamhet upphör, ska utfärdarens privata nycklar och kopiorna av dem förstöras.

Om en yrkesutbildad person inom social- och hälsovården vill förstöra sin egen privata nycklar, ska han eller hon anmäla spärrtjänsten om spärrningen av yrkeskortet i fråga och se till att informationen på yrkeskortets chips förstörs till exempel genom att klippa kortet itu.

6.2.11 Klassificering av säkerhetsnivån av yrkeskort och kryptografiska moduler

Yrkeskorten och de kryptografiska modulerna ska uppfylla de standarder och klasser som nämns i punkt 6.2.1.

6.3 Andra faktorer som påverkar hanteringen av nyckelparet

Om varje process vid skapande av nycklar samlas in information. I dessa uppgifter ingår uppgifter om yrkeskortbeställningen, kortnumren för tillverkade yrkeskort samt certifikat.

6.3.1 Arkivering av publika nycklar

Utfärdaren arkiverar de publika nycklar som den certifierat enligt punkt 5.5.

6.3.2 Giltighetstiden för certifikat och nycklar

Certifikat och nyckelpar för en yrkesutbildad person inom social- och hälsovården är giltiga i högst 60 månader. Giltighetstiden börjar från tidpunkten för beviljande av certifikatet. Certifikatet kan vid behov beviljas för en bestämd tid.

Giltighetstiden för utfärdarens certifikat och nyckelpar är 13 år från tidpunkten av skapandet av nycklarna. Nycklar används inte före giltighetstiden eller efter giltighetstiden för något ändamål.

6.4 Aktiveringsuppgifter

6.4.1 Skapande av aktiveringsuppgift

Aktiveringsuppgiften dvs. PIN-koden samt öppningskoden dvs. PUK-koden skapas i samband med specificeringen av yrkeskortet. Koderna grundar sig på slumptal. PIN-koden skyddar de privata nycklarna på yrkeskortet. Certifikatinnehavaren kan byta PIN-koden till ett siffra med minst 4 tecken.

PUK-koden som behövs för att öppna en låst PIN-kod är 8 tecken lång. PUK-koden förvaras i utfärdarens datasystem.

6.4.2 Skydd av aktiveringsuppgift

PIN-koderna levereras till certifikatinnehavaren i ett slutet kodkuvert och de är endast i certifikatinnehavarens kännedom. Certifikatinnehavaren kan byta PIN-koderna för sitt yrkeskort till siffror med minst 4 tecken. PUK-koden kan inte ändras.

6.4.3 Andra faktorer om aktiveringsuppgiften

—

6.5 Hantering av datorutrustningens säkerhet

Till hanteringen av säkerheten av utfärdarens system hör bland annat stark identifiering av användaren och spårbarheten av funktioner och uppgifter i anknytning till utfärdarens privata nycklar ända fram till personnivå samt insamling av logguppgifter. Datorutrustningen ligger i skyddade lokaler.

För säkerheten av registrerarens datorutrustning sörjer man genom att förhindra olaglig användning av utrustningen.

6.5.1 Särskilda krav

I fråga om säkerhetskrav för datorutrustningen följs anvisningen VAHTI 5/2004.

6.5.2 Klassificering av utrustningssäkerhet

—

6.6 Hantering av säkerhet under livscykeln

6.6.1 Hantering av systemutveckling

Utvecklingen av utfärdarens system sker i en utvecklingsmiljö som är separata från produktionssystemet.

Alla uppdateringar som görs i utfärdarens datasystem görs genom att först säkerställa att de fungerar i testmiljön. Uppdateringarna planeras från fall till fall och deras tidtabell planeras och om uppdateringarna informeras i förväg. Planen innehåller testplanen och kriterierna för godkännande.

Vid versionsbyte säkerställs att hela datahanteringskedjan i datasystemet fungerar. Ibruktagandefasen planeras så att snabb återgång till gammal version är möjlig inom ramen för en bestämd tid.

6.6.2 Hantering av säkerhet

I fråga om hanteringen av säkerheten av datorutrustningen följs anvisningen VAHTI 5/2004. Hanteringen av säkerheten grundar sig på:

- fördelning av arbetsuppgifter till olika personer enligt punkt 5.2;
- uppföljning av säkerhet;
- regelbundna säkerhetskontroller;
- tekniska skyddslösningar och -metoder; och
- förfarande för befullmäktigande och godkännande av applikationsändringar.

6.6.3 Säkerhetsklassificering av livscykeln

—

6.7 Hantering av datanätets säkerhet

Dataförbindelserna och datanäten i utfärdarens system är starkt krypterade och skyddade samt dedikerade. Utfärdaren svarar för övervakningen av datanätet.

I fråga om säkerhetskrav för dataförbindelserna följs anvisningen VAHTI 5/2004.

6.8 Tidsstämpel

Tidsstämpeltjänsten är för tillfället inte i bruk.

7 Profil för certifikat och spärrlista

7.1 Profil för certifikat

Profilen för yrkescertifikat för social- och hälsovården har beskrivits i bestämningen THPKI - T2: Myndigheten för digitalisering och befolkningsdatas CA-mall och certifikatens datainnehåll inom social- och hälsovården.

7.2 Profil för spärrlista

Profilen för spärrlistan för yrkescertifikat för social- och hälsovården har beskrivits i bestämningen FINEID S2 - VRK (PRC) CA-model and certificate contents.

7.3 Kontroll av spärrlista i realtid (OCSP)

OCSP-protokollet är tillgängligt.

8 Godkännandekontroll

Utfärdaren svarar för att dess certifieringsverksamhet följer denna certifieringspraxis samt certifikatpolicy.

8.1 Utförande av godkännandekontroller

Certifikatutfärdarens verksamhet inspekteras minst en gång om året. Med hjälp av inspektionen utreds om utfärdaren verkar i enlighet med certifikatpolicyn och certifieringspraxisen. Utfärdaren ansvarar för verkställandet av inspektionen.

8.2 Inspektör

Inspektionen kan utföras av en oberoende och välansedd inspektionsanläggning och som specialiserat sig på inspektion av datasystem och som ligger i Finland eller en annan stat i Europeiska ekonomiska samarbetsområdet.

8.3 Inspektörens förhållande till part som inspekteras

Inspektören är utomstående och obunden i förhållande till det objekt som inspekteras.

8.4 Inspektionens omfattning

Vid granskningen jämförs certifikatpolicyn och certifieringspraxisen med utfärdarens verksamhet som helhet. Till inspektionen hör också kontroll av datasäkerheten av datasystem som anknyter till utfärdarens certifiering och registrering.

Inspektionen gäller också utfärdarens underleverantörer och andra leverantörer.

Inspektionens resultat antecknas som ett utlåtande.

8.5 Åtgärder som ska vidtas vid avvikelser

Utfärdaren vidtar utan fördröjning korrigerande åtgärder vid upptäckta avvikelser.

8.6 Information om resultat av inspektionen

Den inspekterade statusen för dokument och verksamhet beskrivs i den offentliga utlåtandedelen i inspektionsberättelsen. Inspektionsberättelsen överlåts i sin helhet på begäran till utfärdarens samarbetspartner enligt avtal.

9 Allmänna villkor

Detta kapitel innehåller skyldigheter och ansvar för utfärdaren, registreraren, den yrkesutbildade personen inom hälso- och sjukvården och andra parter som anknyter till certifikatsystemets verksamhet samt frågor som gäller utredningen av konflikter.

9.1 Avgifter och andra arvoden

Avgifter och andra arvoden fastställs enligt 22 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården och Finansministeriets förordning om avgifterna för Myndigheten för digitalisering och befolkningsdatas prestationer som är giltig vid respektive tidpunkt.

9.1.1 Avgift för beviljande av certifikat

—

9.1.2 Avgift för användning av certifikat

—

9.1.3 Avgift för spärrning av certifikat eller förfrågan om status

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

9.1.4 Avgifter för andra tjänster, såsom rådgivningstjänsten

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

9.1.5 Ersättningar

Ersättningar fastställs enligt avtalen med parterna för certifikatsystemet.

9.2 Ekonomiska skyldigheter

Utfärdaren svarar i enlighet lagen om stark autentisering och betrodda elektroniska tjänster att den har tillräckliga ekonomiska resurser för att arrangera certifikatverksamheten på ett ändamålsenligt sätt samt hantera eventuella krav på skadeersättning.

9.3 Konfidentialitet och dataskydd

I fråga om konfidentialitet och dataskydd följs lagar, förordningar, god datahantering och principer.

9.3.1 Privata uppgifter

Privata uppgifter kan endast avslöjas med stöd av en bestämmelse i lag eller en bestämmelse som grundar sig på lag eller certifikatinnehavarens samtycke.

Alla privata nycklar som utfärdaren använder eller hanterar i den verksamhet som denna certifieringspolicy gäller, är sekretessbelagda.

Insamlade register och logguppgifter publiceras endast om lagen eller förordningen eller en bestämmelse som utfärdats med stöd av dessa förutsätter detta.

9.3.2 Offentliga uppgifter

Publika nycklar för verifikationscertifikat och spärrlistan är offentlig information och tillgänglig för alla i det offentliga registret.

Identifieringsuppgifterna eller andra privata uppgifter eller uppgifter om företaget som ingår i det beviljade certifikatet är offentliga om inte annat bestäms i avtalen eller i lag, förordning eller bestämmelser som utfärdats med stöd av dessa.

9.3.3 Skydd av privata uppgifter

Alla parter i certifikatsystemet ska följa lagar, förordningar och rekommendationer som utfärdats om skydd av privata uppgifter.

9.4 Integritetsskydd

I fråga om integritetsskydd följs den gällande lagstiftningen.

9.4.1 Plan för skydd av privata uppgifter

Parterna i certifikatsystemet ska skapa och genomföra en plan för skydd av privata uppgifter.

9.4.2 Privata uppgifter som hanteras i utfärdarens system

Vid hanteringen av privata uppgifter i utfärdarens system följs lagstiftningen om hantering av personuppgifter och integritetsskydd.

9.4.3 Publika uppgifter som hanteras i utfärdarens system

Vid hanteringen av publika uppgifter i utfärdarens system följs lagen om offentlighet i myndigheternas verksamhet.

9.4.4 Ansvar för skydd av privata uppgifter

Utfärdaren ansvarar för att de privata uppgifter som hanteras i utfärdarens system är skyddade mot osaklig hantering.

9.4.5 Användning eller publicering av privata uppgifter med certifikatinnehavarens samtycke

Konfidentialiteten och dataskyddet av uppgifterna har fastställts i punkt 9.3.

9.4.6 Utlämning av uppgifter till myndigheter

Till myndigheter utlämnas uppgifter enligt lagar, förordningar eller bestämmelser som utfärdats med stöd av dessa.

9.4.7 Andra omständigheter där uppgifter kan publiceras

Utfärdaren lämnar inte ut uppgifter i några andra än ovannämnda omständigheter.

9.5 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 certifikatpolicy.

9.6 Parternas förbindelser

9.6.1 Utfärdarens förbindelser

Utfärdaren förbinder sig att producera, upprätthålla och utveckla certifikattjänster inom social- och hälsovården enligt denna certifieringspraxis och certifikatpolicy.

9.6.2 Registrerarens förbindelser

Registreraren ska för sin del förbinda sig att producera, upprätthålla och utveckla registreringstjänster inom social- och hälsovården enligt denna certifieringspraxis och certifikatpolicy.

9.6.3 Certifikatinnehavarens förbindelser

Certifikatinnehavaren förbinder sig att använda yrkescertifikatet för social- och hälsovården och yrkeskortet enligt denna certifieringspraxis, certifikatpolicy och de givna anvisningarna.

9.6.4 De förlitande parternas förbindelser

De förlitande parterna förbinder sig att ansvara för att de egna social- hälsovårdssystemen och yrkescertifikaten för social- och hälsovården är kompatibla.

9.6.5 Andra parters förbindelser

—

9.7 Ansvarsfrihetsklausul

De ansvarsfrihetsklausuler som ställts i avtalen mellan utfärdaren och utfärdarens avtalspartner samt för innehavaren av utfärdarens certifikat och den instans som utnyttjar certifikatsystemet förbinder utfärdarens avtalspartner, certifikatinnehavaren och den instans som utnyttjar certifikatsystemet på samma sätt som de ansvarsfrihetsklausuler och ansvarsbegränsningar som ingår i denna certifieringspraxis.

9.8 Ansvarsbegränsningar

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Myndigheten för digitalisering och befolkningsdata tillämpas utfärdarens skadeståndsansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och lagen om elektronisk kommunikation i myndigheternas verksamhet. I tillämpliga delar tillämpas också skadeståndslagen (412/1974).

Utfärdaren svarar inte för eventuella skador som orsakas av att PIN-koderna, PUK-koden och certifikatinnehavarens privata nycklar röjs, om inte röjningen direkt har orsakats av utfärdarens omedelbara åtgärder.

Utfärdarens ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på utfärdarens omedelbara åtgärder.

Utfärdaren svarar inte för indirekta skador eller följdskador som har orsakats certifikatinnehavaren. Utfärdaren svarar inte heller för eventuella indirekta skador eller

följdskador som orsakas förlitande parter eller andra avtalsparter för certifikatinnehavaren.

Utfärdaren 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. Certifikatinnehavarens ansvar för användningen av certifikatet upphör när han eller hon meddelat de uppgifter som behövs för att spärra certifikatet till spärrtjänsten och fått ett samtal av den funktionär som tog emot telefonsamtalet om att certifikatet har antecknats på spärrlistan. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

9.9 Skadestånd

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Myndigheten för digitalisering och befolkningsdata tillämpas utfärdarens skadeståndsansvar enligt lagen om stark autentisering och betrodda elektroniska tjänster och lagen om elektronisk kommunikation i myndigheternas verksamhet. I tillämpliga delar tillämpas också skadeståndslagen (412/1974).

9.10Giltighetstid och upphörande av giltighet

9.10.1 Giltighetstid för certifieringspraxis

Certifieringspraxisen är i kraft ända fram till att en ny version av certifieringspolicyn ersätter den.

9.10.2 Upphörande av giltighetstiden för certifieringspraxisen

Certifieringspraxisen har ingen separat bestämd giltighetstid.

9.10.3 Konsekvenser av upphörande av giltighetstiden för certifieringspraxisen

—

9.11Kommunikation mellan parterna för certifikattjänsten

Utfärdaren och de samarbetsinstanser som anknyter till certifikatverksamheten ska informera om ändringar som gäller deras verksamhet i alla fall. Informeringen om ändringar sker skriftligen till alla samarbetspartner.

9.12 Hantering av ändringar i certifieringspraxisen

Utfärdaren beslutar om ändringar i certifieringspraxisen.

9.12.1 Ändring av certifieringspraxisen

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för yrkescertifikatet. 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 till Traficom och 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.

9.12.2 Information om ändringar

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.

9.12.3 Ändring av koduppgift i certifieringspraxisen

Koduppgiften i certifieringspraxisen ändras inte även om innehållet i certifieringspraxisen ändras.

9.13 Avgörande av meningsskiljaktigheter

Avsikten är att eventuella tvister som gäller certifikattjänsten inom hälso- och sjukvården och denna certifieringspraxis hanteras i förhandlingar mellan parterna. Om en lösning inte nås, hanteras meningsskiljaktigheterna mellan parterna i tingsrätten i utfärdarens hemort i Finland.

9.14 Tillämplig lag

På certifikattjänsten inom social- och hälsovården och denna certifieringspraxis tillämpas finsk lag.

9.15 Att följa lagen

Vid ordnandet av certifikattjänster inom social- och hälsovården följs enbart finsk lag.

9.16 Övriga arrangemang

9.16.1 Avtal

Rättigheterna, ansvar och skyldigheterna mellan utfärdaren och certifikatinnehavaren fastställs i certifikatpolicyn och certifieringspraxisen. Genom att underteckna certifikatansökan förbinder sig den yrkesutbildade personen inom social- och hälsovården att följa användningsvillkoren för certifikatet. De gällande användningsvillkoren ges till den yrkesutbildade personen inom social- och hälsovården i samband med överlåtelsen av certifikatet.

Med sin underskrift förbinder sig den yrkesutbildade personen inom social- och hälsovården att omedelbart anmäla spärrtjänsten om försvunnet certifikatkort, misstanke om missbruk eller möjlighet till missbruk.

Utfärdaren ingår ett avtal med registrerare som befullmäktigats av utfärdaren. Av avtalet framgår båda parternas rättigheter, ansvar och skyldigheter.

Utfärdaren kan ingå avtal med förlitande parter eller andra parter. Av avtalen ska tydligt framgå båda avtalsparternas rättigheter, ansvar och skyldigheter.

Utfärdaren upprättar nödvändiga avtal med certifikattjänstleverantören och delleverantörerna.

9.16.2 Rättsöverlåtelse

Avtalsparterna för certifikattjänsten inom hälso- och sjukvården får inte överlåta sina rättigheter som fastställts i avtalen till andra parter utan att utfärdaren i förväg gett sitt godkännande för det.

9.16.3 Ogiltighet

Eventuell nullitet, ogiltighet eller icke-verkställbarhet av en enskild bestämmelse i denna certifieringspraxis inverkar inte på certifieringspraxisens giltighet till andra delar.

9.16.4 Verkställighet

Även om utfärdaren i ett enskilt avtalsbrottsärende skulle avstå från sin rätt till skadestånd eller annan ersättning, betyder det inte avstående från rätten till skadestånd för samma skada eller andra avtalsbrott i framtiden.

9.16.5 Oöverstigligt hinder

Utfärdaren ansvarar inte för skador som beror på naturkatastrofer eller andra motsvarande skador som beror på oöverstigliga omständigheter. Lägg till hinder

9.17Övriga villkor

Vid tolkning och tillämpning av dokument och handlingar som gäller certifikattjänster inom social- och hälsovården, denna certifieringspraxis samt förbindelser mellan parterna för certifikatsystemet och deras avtalspartner är de finskspråkiga versionerna av dokumenten i första hand avgörande.

[Yksikkö] / Aarnio Ville 1.4.2021