CERTIFIERINGSPRAXIS

för serviceleverantörers kort för personaktörer

OID 1.2.246.517.1.10.203.4

SERTIFIOITU inspecta ORGANISAATIO
ISO 9001

SERTIFIOITU inspecta ORGANISAATIO
ISO/IEC 27001

Väestörekisterikeskus

VRK/TS/Keh

3.5.2018

HANTERING AV DOKUMENT	
Ägare	
Upprättat av	
Granskat av	
Godkänt av	

VERSIONSHANTERING		
version nr	åtgärder	datum/person
1.0	Godkänd version, dokument enligt eIDAS-förordningen	3.5.2018

VRK/TS/Keh

3.5.2018

Innehållsförteckning

VRK/TS/Keh

3.5.2018

Inledning

I certifikatpolicyn definieras Befolkningsregistercentralens - här efter certifikatutfärdaren (Certification Authority) – förutsättningar för certifieringsfunktioner enligt öppet nyckelsystem (Public Key Infrastructure; PKI) samt tillämpningsområde och begränsningar för detta dokument. 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 Befolkningsregistercentralen (nedan BRC) 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 certifikatinnehavaren och den förlitande parten 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.

1.1 Bakgrund

BRC beviljar personaktörscertifikat till personaktörer som är anställda hos serviceleverantörer inom hälsovården och som inte är yrkesutbildade personer inom hälso- och sjukvården (nedan personaktör). I gruppen i fråga ingår övriga personer och specialgrupper som använder riksomfattande datasystem, såsom dataskyddsansvariga samt datasystemleverantörer, konsulter osv.

Befolkningsregistercentralen erbjuder signatur- och identifieringscertifikat med hög datasäkerhetsnivå samt därtill relaterade tjänster för den offentliga och privata sektorn. 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 Kommunikationsverket.

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.

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som gjorts med certifikat.

Befolkningsregistercentralen har sedan 1.12.2010 varit lagstadgad certifikatutfärdare för hälsovården med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) samt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

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

- Lag om elektroniska recept (61/2007)
- Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007)
- Lag om yrkesutbildade personer inom hälso- och sjukvården (559/1994)
- Lag om stark autentisering och betrodda elektroniska tjänster (617/2009)
- Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)
- Lag om offentlighet i myndigheternas verksamhet (621/1999)
- Lag om säkerhetsutredningar (177/2002)
- Lag om stark autentisering och betrodda elektroniska tjänster (617/2009)
- 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 (5/2008)
- ETSI TS 101 456, v1.4.3: 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
- Kommunikationsverkets föreskrift Kommunikationsverket 72/2016 M Föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster
- VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
- 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 serviceleverantörers certifikat för personaktörer, vars OID är 1.2.246.517.1.10.203.4.

Denna certifieringspraxis syftar till Certifikatpolicyn för Befolkningsregistercentralens organisationscertifikat, OID 1.2.246.517.1.10.203.

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.

Befolkningsregistercentralen följer certifikatpolicyn som gäller signaturcertifikat som beviljas allmänheten enligt betrodda tjänster i Förordningen nr (EU) 910/2014. Dokumentets referensuppgifter är SÖK EN 319 411-1 [2], punkt 4.3.5. 3) enligt QSCD; OID: 0.4.0.194112.1.2. Signaturcertifikat som beviljas enligt denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar de godkända certifikat och medel för skapande som beskrivs i Förordningen såsom föreskrivs i 28 och 29 i Förordningen. Nivån av identifieringscertifikatet uppfyller kravnivån ”hög” enligt Förordningen och Säkerhetsnivåförordningen som utfärdats med stöd av den.

Parter och lämplighet

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

2.1.1 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 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. förplikta registreringsstället att spärra certifikat och 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.

2.1.2 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 certifikatsökandet enligt kapitel 3 till 4 i denna certifieringspraxis och enligt certifieringspraxisen;
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 i certifikatpolicyn.

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

Registreraren svarar för alla registreringstjänster som tillhandahålls av registreraren.

2.1.3 Innehavare av certifikat

Innehavaren av serviceleverantörers certifikat för personaktör kan vara en person som arbetar inom hälso- och sjukvården men som inte är en yrkesutbildad person inom hälso- och sjukvården eller annan anställd inom hälso- och sjukvården.

Sökanden av serviceleverantörers certifikat för personaktörer ska bevisa sin identitet vid ansökan om certifikat.

Genom att underteckna certifikatansökan förbinder sig sökanden att följa användningsvillkoren för certifikatet. De gällande användningsvillkoren ges till sökanden i samband med överlåtelsen av certifikatet.

2.1.4 Förlitande part

Förlitande part kan vara ägare av ett sådant datasystem vars dataskyddsmekanismer har byggts för att utnyttja serviceleverantörers certifikat för personaktörer.

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 via OCPS-tjänsten eller kontroll av spärrlistan) och ändra sitt system enligt de uppdateringar som görs i certifikatpolicyn och certifieringspraxisen.

2.1.5 Andra parter

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

2.2 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.

Serviceleverantörers certifikat för personaktörer används i de nationella datasystemen inom hälso- och sjukvården. Med nationella datasystem inom hälso- och sjukvården avses system med vilka de uppgifter som ålagts Folkpensionsanstalten i lagen om elektroniska recept (61/2007) och lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) verkställs. Dessutom kan serviceleverantörers certifikat för personaktörer användas i andra datasystem inom hälso- och sjukvården och apoteksväsendet.

2.2.1 Tillåtna användningsändamål för certifikat

Ett certifikat förenar en person och en offentlig nyckel som ställts till personens förfogande och en med PIN-kod skyddad privat nyckel. Serviceleverantörers certifikat för personaktörer som beviljas enligt denna certifieringspraxis används för elektronisk identifiering av certifikatets innehavare, kryptering av data vid kommunikation eller lagring och för elektronisk signatur, dvs. för verifiering av äktheten, integriteten och obestridligheten av ett digitalt dokument eller någon annan digital uppgift (t.ex. anteckning i patientjournal, elektroniskt recept).

2.2.2 Förbjudna användningsändamål för certifikat

Enligt social- och hälsoministeriets beslut är det förbjudet att förmedla patientuppgifter per e-post. Det är således inte tillåtet att använda serviceleverantörers certifikat för personaktörer för att kryptera eller underteckna e-postmeddelanden som innehåller patientuppgifter.

2.3 Kontaktuppgifter

2.3.1 Den administrativa organisationen för certifieringspraxisen

Denna certifieringspraxis är producerad av Befolkningsregistercentralens certifikattjänster. BRC:s Certifikattjänster ansvarar för hanteringen och uppdateringen av detta dokument.a

2.3.2 Kontaktuppgifter

Utfärdarens kontaktuppgifter

Befolkningsregistercentralen (BRC) PB 123 (Fågelviksgränden 4) 00531 HELSINGFORS	www.fineid.fi E-post: vaestörekisterikeskus@vrk.fi Telefon +358 295 535 001 Fax +358 9 876 4369

2.3.3 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.

2.3.4 Förfarande vid godkännande av certifieringspraxis

BRC:s Certifikattjänster fastställer och godkänner certifieringspraxisdokumenten.

2.4 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 (559/1994). Yrkesrättigheten kan vara obegränsad, begränsad eller fråntagen. Yrkesrättigheterna sparas i Terhikki-registret som upprätthålls av Tillstånds- och tillsynsverket för social- och hälsovården.

Returnering av nyckel *(Key recovery)***:** Med key recovery avses en situation där en privat nyckel returneras när certifikatkortet gått sönder eller försvunnit. Privata nycklar för certifikatkort inom hälso- och sjukvården 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.

Korthanteringsapplikationen, KoHa: En databasapplikation som fungerar som en separat del av certifikatsystemet och som stödjer registreringstjänsten och spärrtjänsten. I applikationen har bland annat kortens och certifikatens livscykel- och innehavaruppgifter sparats.

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.

OCSP: Online Certificate Status Protocol, onlinetjänst för återställande av certifikatets status

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

Personifieringsprogram: Ett program som används i registreringsställen, med vilket kontakter med KoHa- och Terhikki-registren hanteras, tryckningar på certifikatkortet görs samt certifikat sparas på kortets chips. Med personifieringsprogrammet produceras också PIN-koderna och PUK-öppningskoderna.

PIN *(Personal identification number)*: Kod som används för att säkerställa användningsrätten till certifikatkortets nyckelpar. Certifikatet 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 certifikatkort 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.

Registreringsställe *(RA-piste)***:** Ett serviceställe där certifikatsökandens identitet samt yrkesrättigheterna hos yrkesutbildade personer inom hälso- och sjukvården och arbetsgivaruppgifter för andra personer kontrolleras. Registreringsstället ansvarar för utdelningen av certifikatkort, certifikat och PIN-/PUK-koder enligt certifikatpolicyn och certifieringspraxisen.

Spärrlista *(CRL, Certificate Revocation List)***:** Spärrlistan är en lista över certifikat som spärrats. Ett certifikat spärras när innehavaren av certifikatet begär att certifikatet spärras, certifikatinnehavarens uppgifter som antecknats på certifikatet har ändrats, certifikatkortet och öppningskoden har försvunnit eller stulits eller certifikatinnehavaren har dött.

Spärrtjänst: Utfärdarens tjänst som spärrar serviceleverantörers certifikat för personaktörer enligt begäran om spärrning.

Yrkesutbildad person inom hälso- och sjukvården Enligt 2 § 1 mom. lagen om yrkesutbildade personer inom hälso- och sjukvården (559/1994) avses med yrkesutbildad person inom hälso- och sjukvården den som med stöd av lagen har erhållit rätt att utöva yrke (legitimerad yrkesutbildad person) eller tillstånd att utöva yrke (yrkesutbildad person som beviljats tillstånd) den som med stöd av denna lag har rätt att använda i förordning av statsrådet avsedd yrkesbeteckning för en yrkesutbildad person inom hälso- och sjukvården (yrkesutbildad person med skyddad yrkesbeteckning). I detta certifieringsförfarande avses med yrkesutbildad person inom hälso- och sjukvården även studerande som avses i 2 § 3 mom. i lagen.

Annan anställd inom hälso- och sjukvården En annan person som arbetar i en verksamhetsenhet inom hälso- och sjukvård eller en person som utför uppgifter vid en sådan, men som inte är yrkesutbildad person inom hälso- och sjukvården.

Serviceleverantör inom hälso- och sjukvården En verksamhetsenhet inom hälso- och sjukvården eller en yrkesutbildad person inom hälso- och sjukvården som arbetar som självständig yrkesutövare.

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 certifikatkort inom hälso- och sjukvården.

Identifiering *(Identification)***:** Ett förfarande med vilket till exempel användaren av datasystemet identifieras. Typiskt sker identifieringen genom att kontrollera om den angivna koden eller an-

nan 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 verifikations- och krypteringsnycklar är obligatorisk och nyckeln i säker deponering är i vissa situationer användbar utan certifikatinnehavarens samtycke. Privata nycklar för certifikatkort inom hälso- och sjukvården deponeras inte.

Certifikat *(Certificate)***:** En datahelhet som utgörs av en publik nyckel hos en aktör i servicenätverket såsom en yrkesutbildad person inom hälso- och sjukvård 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, verifikations- och krypteringscertifikaten inom hälso- och sjukvården 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.

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 Ett befolkningsregister som innehåller grundläggande uppgifter om finländska medborgare och i Finland fast bosatta utlänningar. Systemet innehåller också information om byggnader, byggprojekt och lägenheter samt fastigheter och lokaler. Befolkningsdatasystemet upprätthålls av Befolkningsregistercentralen och magistraterna. Även församlingar och sjukhus lämnar uppdateringsuppgifter i systemet. Registreringen av uppgifter grundar sig på medborgarnas och myndigheternas lagstadgade anmälningar.

Publicering av uppgifter

3.1 Offentligt register

Utfärdaren ansvarar för upprätthållandet av certifikatregistret samt publiceringen av information som fastställs i kapitel 2.2. Informationsinnehållet och strukturen i registret följer bestämningen THPKI T3.

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

3.2 Uppgifter som publiceras av utfärdaren

Utfärdaren svarar för att certifieringspolicyn, certifieringspraxisen, certifieringsbeskrivningar och utfärdarens certifikat är offentligt tillgängliga på adressen www.fineid.fi Registertjänsten är en offentlig webbtjänst som innehåller verifikations- och krypteringscertifikat beviljade av utfärdaren och avsedda för det offentliga registret samt utfärdarens certifikat och spärrlistan. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi. Verifikations- och krypteringscertifikat, utfärdarens certifikat samt spärrlistorna finns tillgängliga i det offentliga registret på adressen ldap.fineid.fi alla dagar, vid alla tider på dygnet. Signaturcertifikaten publiceras inte i registret.

3.3 Publiceringsfrekvens

Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen. Hanteringen av ändringar har beskrivits i kapitel 9.12.

Verifikations- och krypteringscertifikaten samt spärrlistorna publiceras i certifikatregistret genast när de har skapats.

3.4 Tillträdesrättigheter

Tillgängligheten av uppgifter som utfärdaren publicerat begränsas inte med tillträdesrättigheter.

Identifiering och verifikation

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

4.1 Utnämnande av certifikatinnehavare

4.1.1 Utnämnande

Utnämnandet av innehavaren av certifikatet för hälsovården i verifikations- och krypteringscertifikatet samt signaturcertifikatet har beskrivits i bestämningen THPKI - T2: Befolkningsregistercentralens CA-mall och certifikatens datainnehåll inom hälsovården

Befolkningsregistercentalens 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

Utfärdare för Befolkningsregistercentralens organisationscertifikat är:

CN (Common name) = VRK CA for Organisational Certificates - G3

OU (Organizational unit) = Organisaatiovarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Certifikatinnehavarens namngivningspraxis för organisationscertifikat:

2.5.4.5 (Serial Number) = Specificerande kod

SN (Surname) = Efternamn

G (Given name) = Förnamn

CN (Common name) = Efternamn Förnamn Specificerande kod

C (Country) = FI

Valfria fält:

O (Organization) = Organisationens namn

OU (OrganizationalUnit) = Organisationsenhet

T (Title) = Titel

E (EmailAddress) = e-postadress

UPN (Universal Principal Name) = UPN namn

4.1.2 Betydelse av utnämnande

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

Gruppen av attribut som bildar objektets namnpost i certifikatet är unik och individualiserar innehavaren av certifikatet i fråga. Den identifierande koden ges av utfärdaren. Alla andra personer inom hälsovården ska agera under eget namn.

4.1.3 Anonym eller pseudonym

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

4.1.4 Innehåll av namnfälten

Innehållet av namnfälten har fastställts i kapitel 3.1.1.

4.1.5 Namnpostens unicitet

Namnposten som definieras i kapitel 3.1.1 identifierar innehavaren av serviceleverantörers certifikat för personaktörer. Personens koduppgift identifierar certifikatinnehavaren på ett unikt sätt.

4.1.6 Användningsrättighet till produktnamn

—

4.2 Verifikation av personlighet

4.2.1 Metod för att bevisa innehavet av en privat nyckel

Serviceleverantörers privata nycklar för personaktörer skapas alltid med certifikatkortets chips. Certifikatkortet som innehåller de privata nycklarna överlåts till serviceleverantörers personaktör efter att hans eller hennes identitet har tillförlitligt verifierats och certifikatet har registrerats och skapats.

4.2.2 Autentisering av organisation som företräder certifikatsökanden

Av sökande av serviceleverantörers certifikat för personaktörer krävs verifikation av de organisationer de representerar. Organisationen som certifikatsökanden representerar verifieras utifrån ett pappersintyg som organisationen överlåtit till sökanden.

4.2.3 Identifiering av personen

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. Uppgifter i anslutning till identifieringen sparas i utfärdarens beställnings- och administrationssystem för certifikat (Vartti).

4.2.4 Certifikatsökandens uppgifter som utfärdaren inte kontrollerar

Alla personuppgifter som krävs för ansökan om serviceleverantörers certifikat för personaktörer kan hämtas från befolkningsdatasystemet och de arbetsgivaruppgifter som organisationen som sökanden representerar lämnat.

4.2.5 Förutsättningar för beviljande av certifikat

Endast en person som arbetar i en verksamhetsenhet inom hälso- och sjukvård eller en person som utför uppgifter vid en sådan, men som inte är yrkesutbildad person inom hälso- och sjukvården, har rätt att ansöka om serviceleverantörers certifikat för personaktörer. När anställningsförhållandet upphör ska serviceleverantörers certifikat för personaktörer spärras.

4.2.6 Förutsättningar och krav för samarbete mellan utfärdare

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

4.3 Identifiering och verifikation vid förnyelse av certifikat

4.3.1 Identifiering och verifikation vid förnyelse av certifikat

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

4.3.2 Identifiering och verifikation efter spärrning av certifikat

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

4.4 Identifiering av den person som gjort begäran om spärrning

Begäran om spärrning av certifikat kan göras per telefon eller skriftligen till certifikatutfärdaren.

När spärrningsbegäran görs per telefon eller skriftligen, registreras anmälarens och certifikatinnehavarens uppgifter i beställning- och administrationssystemet för certifikat (Vartti).

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.

Funktionella krav för hantering av certifikatets livscykel

Detta kapitel beskriver de krav som ställts för utfärdarens, registrerarens och serviceleverantörers personaktörs verksamhet. I kapitlet behandlas också spärrning av certifikat.

5.1 Ansökan om certifikat

Serviceleverantörers certifikat för personaktörer ansöks personligen vid ett registreringsställe.

Uppgifterna i ansökan sparas i utfärdarens beställnings- och administrationssystem för certifikat (Vartti).

Ansökan om serviceleverantörers certifikat för personaktörer förutsätter att sökanden:

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

Sökanden ges information om leveranssätt för certifikatet och kuverten med PIN-koden.

Sökanden ges användningsvillkoren för certifikatet som ingår i certifikatpolicydokumenten.

5.1.1 Vem som helst kan göra en certifikatansökan

Certifikatansökan kan göras av en person som arbetar i en verksamhetsenhet inom hälso- och sjukvård eller en person som utför uppgifter vid en sådan, men som inte är yrkesutbildad person inom hälso- och sjukvården.

5.1.2 Processen för beviljande av certifikat och ansvar

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

Datakommunikationsförbindelserna mellan utfärdarens datasystem är skyddade. Personer som använder beställnings- och administrationssystemet för certifikat identifieras med administrationskort som utfärdaren beviljat. Datainnehållet i certifikatet består av de uppgifter som angetts på ansökningsblanketten.

Registreraren lämnar certifikatansökan till utfärdaren för beviljande av certifikat, när registreraren och sökanden har granskat och godkänt uppgifterna i ansökan med sin underskrift.

Utfärdaren lämnar till sökanden:

- ett certifikatkort som innehåller kortinnehavarens personliga nyckelpar och certifikat
- ett kodkuvert som innehåller de personliga PIN- och PUK-koderna som behövs för att använda certifikatkortet. Dessa är specificerade utifrån sökandens uppgifter.

Dessutom levererar registreraren bruksanvisningen för certifikatkortet till certifikatsökanden.

5.2 Behandling av certifikatansökan

Certifikatansökan behandlas vid registreringsstället utan obefogat dröjsmål.

Registreraren sparar beställningsuppgifterna för certifikatet i utfärdarens beställnings- och administrationssystem för certifikat (Vartti).

5.2.1 Identifiering och verifikation

Registreraren identifierar certifikatsökanden enligt kapitel 3 och kontrollerar att personen arbetar vid en verksamhetsenhet inom hälso- och sjukvården.

Sökanden personuppgifter kan hämtas från Befolkningsdatasystemet. Det tilltalsnamn som sparas på certifikatet och som sökanden angett har nämnts i ansökan. På blanketten anger registreraren också uppgifter om sökandens tjänsteförhållande, uppgifter om produktion och leverans av certifikatet samt de identifieringsdokument som använts för att identifiera sökanden.

5.2.2 Godkännande eller underkännande av certifikatansökan

Certifikatansökan 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.

5.2.3 Behandlingstiden för certifikatansökan

Certifikatansökan behandlas utan obefogat dröjsmål under registreringsställets öppettider.

5.3 Beviljande av certifikat

5.3.1 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 kapitlen 4.1 och 4.2.

5.3.2 Anmälan om beviljande av certifikat till sökanden

En separat anmälan om beviljande av serviceleverantörers certifikat för personaktörer görs inte.

5.4 Godkännande av beviljat certifikat

5.4.1 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.

5.4.2 Publikation av certifikatet på uppdrag av utfärdaren

Utfärdaren publicerar de beviljade verifikations- och krypteringscertifikaten i certifikatregistret på det offentliga datanätet på det sätt som beskrivs i kaiptel 2.1. Signaturcertifikaten publiceras inte i registret.

5.4.3 Anmälan om beviljande av certifikat till andra parter

En separat anmälan om beviljande av serviceleverantörers certifikat för personaktörer görs inte.

5.5 Användning av certifikat och nyckelpar

5.5.1 Användning av certifikat och nyckelpar på uppdrag av certifikatinnehavaren

Serviceleverantörers certifikat för personaktörer och nyckelpar för dessa certfikat är avsedda att användas i datasystem och tjänster inom social- och hälsovården i Finland.

Serviceleverantörers personaktör ska förbinda sig att agera enligt denna certifieringspraxis vid ansökan och användning av certifikatet.

Serviceleverantörers personaktör ansvarar i första hand för den skada som denne 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 certifieringspraxisen;
- genom ett förfarande som strider mot användningsvillkoren för de certifikat som denne godkänt;
- genom annan avsiktlig eller vårdlös felaktig användning av certifikatet.

Certifikatinnehavaren ska förvara och hantera sina egna certifikat och nyckelpar samt sina koder och sitt certifikatkort noggrant. Certifikatinnehavaren ska förhindra att certifikatkortet försvinner eller att koderna avslöjas eller används olovligt.

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

Serviceleverantörers personaktör ska anmäla spärrtjänsten:

- om certifikatkortet försvinner eller vid misstanke om missbruk.

Om certifikatkortet skadas, ska kortinnehavaren spärra certifikaten på det skadade kortet och hämta ett nytt certifikatkort 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 certifikatkortet. 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 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. Tjänstemannen vid registreringsstället skriver ut ett nytt kodkuvert som innehåller öppningskoden. Öppningskoden lämnas inte per telefon eller brev av dataskyddsskäl.

5.5.2 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 och OCSP-tjänsten eller giltigheten av spärrlistan. 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.

5.6 Ny certifiering av en publik nyckel

Serviceleverantörers certifikat för personaktörer beviljas inte för tidigare certifierade publika nycklar.

5.7 Förnyelse av certifikat

5.7.1 Orsaker till förnyelse av certifikat

Serviceleverantörers certifikat för personaktörer kan förnyas när det föregående certifikatets giltighet upphör, om de förutsättningar för beviljande av certifikat som beskrivs i kapitel 3.2.5 fortfarande är giltiga.

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

5.7.2 Ansökan om förnyelse av certifikat

Endast certifikatinnehavaren kan ansöka om förnyelse av certifikatet.

5.7.3 Hantering av begäran om förnyelse av certifikat

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

5.7.4 Anmälan om förnyelse av certifikatkort till certifikatsökanden

En separat anmälan om förnyelse av serviceleverantörers certifikat för personaktörer görs inte.

5.7.5 Förfarande för godkännande av förnyat certifikat ur certifikatinnehavarens synpunkt

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

5.7.6 Publikation av ett förnyat certifikat

Certifikaten publiceras enligt det förfarande som beskrivs i kapitel 4.4.2.

5.7.7 Anmälan om beviljande av förnyat certifikat till andra parter

En separat anmälan om förnyelse av serviceleverantörers certifikat för personaktörer görs inte.

5.8 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 certifikat och certifikatkort enligt kapitel 4.7..

5.9 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.

Certifikatutfärdaren informerar inte certifikatinnehavare om spärrade certifikat.

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

5.9.1 Förutsättningar för spärrning av ett certifikat

Ett certifikat spärras om:

- innehavaren av certifikatet begär att certifikatet spärras
- innehavaren av certifikat byter arbetsplats
- certifikatkortet har skadats, försvunnit eller stulits
- öppningskoden samt certifikatkortet har försvunnit eller stulits
- certifikatinnehavaren har dött.

Utfärdaren kan spärra serviceleverantörers certifikat för personaktörer, om certifikatet har använts i strid mot denna certifieringspraxis, lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) 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.

5.9.2 Behörig att begära spärrning

Behörig att begära spärrning av certifikat är:

- Serviceleverantörers personaktör eller hans eller hennes lagstadgade representant i fråga om personens eget certifikat;
- utfärdaren om förutsättningarna i punkt 4.9.1 uppfylls.

5.9.3 Spärrning av certifikat

Certifikatinnehavaren begär att spärrtjänsten eller registreringsstället 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 kapitel 3.4.

Utfärdaren kan spärra certifikat på tjänsten vägnar:

- 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
- identifieringskod/registreringsnummer eller 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 certifikatkortet har svunnit, certifikatinnehavarens dödstid eller motsvarande
- personuppgifter för den som spärrat certifikatet
- tidpunkten för spärrning av certifikatet.

Certifikatet spärras med en korthanteringsapplikation och uppgifterna om spärrningen förvaras i 5 år efter spärrningstidpunkten.

5.9.4 Certifikatinnehavarens skyldighet att begära spärrning

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

5.9.5 Hanteringstid för begäran om spärrning av ett certifikat

Spärrtjänst och registreringsställen behandlar begäran om spärrning av certifikat utan dröjsmål.

5.9.6 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 (OCSP-tjänsten eller den giltiga spärrlistan). Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat giltigheten.

5.9.7 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.

5.9.8 Maximal giltighetstid för spärrlista

En uppdaterad spärrlista gäller i högst 8 timmar. I varje spärrlista anges när giltighetstiden går ut.

5.9.9 Kontroll av certifikatets status i realtid

Kontroll av certifikatets status i realtid är inte i bruk.

5.9.10 Krav för kontroll av certifikatets status i realtid

—

5.9.11 Andra kontrollåtgärder för certifikatets status

—

5.9.12 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.

5.9.13 Spärrning av certifikat för en bestämd tid

Certifikat kan inte spärras för en bestämd tid.

5.9.14 Vem kan begära om spärrning för en bestämd tid

—

5.9.15 Förfaringssätt för spärrning av certifikat för en bestämd tid

—

5.9.16 Begränsningar för spärrning av certifikat för en bestämd tid

—

5.10 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.

5.11 Upphörande av certifikatets giltighet

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

5.12 System för reservnyckel och återlämning av nycklar

Säker deponering gäller inte serviceleverantörers verifikations- och krypteringsnycklar för personaktörer. Certifikaten kan således inte användas utan certifikatinnehavarens samtycke och privata nycklar kan inte återlämnas om kortet skadats eller försvunnit.

Hantering av fysisk, användnings- och personalsäkerhet

I detta kapitel beskrivs de åtgärder som förutsätts av utfärdaren, registreraren och certifikatinnehavaren gällande fysisk säkerhet samt användnings- och personalsäkerhet. I fråga om utfärdarens och registrerarens säkerhetskrav följs anvisningen VAHTI 5/2004.

6.1 Hantering av fysisk säkerhet

Utfärdarens privat nycklar med vilka certifikaten och spärrlistorna undertecknas, har skyddats mot fysisk intrång.

Utfärdaren, registreringsställen samt korttillverkaren förvarar produktionsutrustningen och säkerhetskopiorna så att olovliga personer inte har tillgång till lagrad information och så att det är omöjligt att ändra, förfalska eller förstora informationen. Säkerhetskopiorna förvaras både för återställning av information och arkivering. I fall av olyckor förvaras säkerhetskopior i andra lokaler än produktionssystemen för certifikat.

Noggrannare villkor för hantering av fysisk säkerhet fastställs i certifieringspraxisen. Utfärdaren kommer vid behov separat överens om detaljerna för hantering av fysisk säkerhet med de leverantörer denne anlitar.

6.1.1 Placering och konstruktion av lokaler

Registreringsställets lokaler har placerats i lokaler i lokalklass 1 (basskydd) enligt anvisningen VAHTI 1/2002.

System som används för produktion av certifikat har placerats i maskinsalar i lokalklass 3 (specialskydd) enligt anvisningen VAHTI 1/2002. Maskinsalarna har indelats i avdelningar och de fördubblade datasystemen har placerats i olika maskinsalar som kan verka oberoende av varandra.

6.1.2 Fysisk tillgångskontroll

Registreringsställen omfattas av passagekontroll så att obehöriga personers tillträde till lokalerna har förhindrats genom att låsa lokalerna tillräckligt effektivt.

Systemen för certifikatproduktion finns i lokaler med bemannad övervakning dygnet runt, elektronisk låsning som registrerar händelserna och en inspelande kameraövervakning. I lokalerna kommer man endast med en personlig passagenyckel och alla händelser registreras i passageövervakningssystemet.

6.1.3 El och luftkonditionering

Eltillförsel och luftkonditioneringens funktionalitet vid registreringsställen ska säkerställas separat.

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.

6.1.4 Vattenskada

Registreringsställen skyddas mot vattenskador.

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

6.1.5 Eldsvåda

Registreringsställen skyddas mot brandskador.

Systemen för certifikatproduktion ligger i maskinsalar försedda med automatisk släckning.

6.1.6 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 (621/1999).

6.1.7 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.

6.1.8 Säkerhetskopiering över nätet

Säkerhetskopieringen av certifikatproduktionssystemet sker i certifikatsystemets interna datakommunikationsnät.

6.2 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.

6.2.1 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.

Dessutom uppföljer och övervakar utfärdaren enligt lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007)att dataskydd och datasekretess som anknyter till den service som denne ger förverkligas.

6.2.2 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.

6.2.3 Identifiering och verifikation av personer för olika roller

Personer som arbetar med utfärdarens arbetsuppgifter som nämns i kapitel 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.

6.2.4 Roller som kräver separering av uppgifter

En registrerare kan inte ha rollen som huvudanvändare av systemet.

6.3 Hantering av personalsäkerhet

6.3.1 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.

6.3.2 Förfarande för kontroll av bakgrund

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

6.3.3 Utbildningsfrekvens och -krav

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

6.3.4 Fortutbildningsfrekvens och -krav

—

6.3.5 Frekvens och ordning av rotation av arbetsuppgifter

—

6.3.6 Följder av olovliga åtgärder

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

6.3.7 Krav på underleverantörers personal

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

6.3.8 Dokument som levereras till personalen

Personalen som deltar i certifikatverksamheten har förutom denna certifieringspraxis också verksamhetsanvisningar som definierar deras verksamhet till sitt förfogande.

6.4 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.

6.4.1 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.

6.4.2 Analyseringsfrekvensen av logguppgifter

Logguppgifter analyseras vid behov.

6.4.3 Förvaringstiden för logguppgifter

Logguppgifterna förvaras i enlighet med gällande arkivbestämmelser.

6.4.4 Skydd av logguppgifter

Endast separat berättigade personer har tillgång till logguppgifterna.

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

6.4.5 Säkerhetskopiering av logguppgifter

Logguppgifterna säkerhetskopieras varje dag.

6.4.6 Genomförande av insamlingssystemet för logguppgifter (intern/extern)

Utfärdaren ansvarar för insamlingssystemet för logguppgifter.

6.4.7 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.

6.4.8 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.

6.5 Material som arkiveras

6.5.1 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
- granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet.

6.5.2 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 (13/2003).

6.5.3 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.

6.5.4 Säkerhetskopiering av arkiven

Inga säkerhetskopior tas av arkivuppgifterna.

6.5.5 Tidsstämpel för arkivuppgifter

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

6.5.6 Insamlingssystemet för arkivuppgifter (intern/extern)

Utfärdaren har inget insamlingssystem för arkivuppgifter.

6.5.7 Tillgängligheten och integriteten av arkivuppgifterna

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

6.6 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 certifikatkortet.

6.7 Förberedelse inför störningssituationer

6.7.1 Plan för funktionsstörningar och äventyrande av verksamheten

Utfärdaren har en kontinuitets- och beredskapsplan 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.

6.7.2 Skada på certifikatsystemet, programmen eller uppgifterna

I undantagssituationer följer utfärdaren kontinuitets- och återhämtningsplanen.

6.7.3 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 certifikatkort med nya privata nycklar skapas för certifikatinnehavaren.

6.7.4 Kontinuiteten av verksamheten efter störningssituation

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

6.8 Nedläggning

6.8.1 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 läggs ned 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 kapitel 5.5.7 bevaras även efter att utfärdarens verksamhet har lagts ned.
- Spärrlistorna finns tillgängliga på angivet sätt under deras giltighetstid.

6.8.2 Nedläggning av registrerarens verksamhet

Nedläggning av registrerarens verksamhet är en situation där den rättighet att registrera serviceleverantörers certifikat för personaktörer som utfärdaren beviljat en organisation inom hälso- och sjukvård upphör permanent.

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

Hantering av teknisk säkerhet

I detta kapitel behandlas villkoren för hantering av utfärdarens, registrerarens och serviceleverantörers personaktörers publika och privata nycklar och motsvarande tekniska bestämningar.

Nyckelparet för serviceleverantörers personaktörer 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.

7.1 Skapande och leverans av nyckelpar till certifikatinnehavaren

7.1.1 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 certifikatkortets chips.

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

7.1.2 Leverans av en privat nyckel till certifikatinnehavaren

Certifikatkortet som innehåller de privata nycklarna och koderna som behövs för att använda det levereras till certifikatinnehavaren på så vis att det inte är möjligt för utomstående att komma åt dem.

7.1.3 Leverans av certifikatsökandens publika nyckel till utfärdaren

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

7.1.4 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 varje certifikatkort inom hälso- och sjukvård.

7.1.5 Nycklarnas längd

Utfärdarens nycklar är RSA-nycklar med 4096 bitar.

Serviceleverantörens signaturnycklar för personaktörer samt verifikations- och krypteringsnycklar är RSA-nycklar med minst 2048 bitar.

7.1.6 Skapande och kvalitet av parametrar för publik nyckel

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

7.1.7 Nycklarnas användningsändamål:

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

Användningsändamålen för serviceleverantörers nyckelpar för personaktörer är verifikation av certifikatinnehavaren och kryptering av information samt utvecklad elektronisk signatur.

7.2 Skydd av privat nyckel och hantering av kryptografiska moduler

7.2.1 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 serviceleverantörers privata nyckel för personaktörer som har sparats på certifikatkortet, levereras till personen enligt förfaranden i denna certifieringspraxis.

Serviceleverantörers certifikatkort för personaktörer är i enlighet med giltiga tillämpliga standarder, såsom ISO/IEC 7816, Javacard Platform 2.2.2 och GlobalPlat-form 2.1.1. Certifikatkortets innehåll är i enlighet med bestämningen THPKI T5.

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

7.2.2 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 annan person inom hälso- och sjukvård kan hanteras och användas endast av innehavaren av nyckeln.

7.2.3 System för reservnyckel för privata nycklar

Systemet för reservnyckeln för certifikatkort inom hälso- och sjukvård är inte tillgängligt.

7.2.4 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 serviceleverantörers privata nycklar för personaktörer tas eller förvaras inte.

En privat nyckel för serviceleverantörers personaktör röjs inte för utomstående i någon fas av certifikatkortets livscykel, och privata nycklar för serviceleverantörers personaktörer förvaras inte någon annanstans än på certifikatkortet för hälso- och sjukvård.

7.2.5 Arkivering av privata nycklar

Utfärdarens privata nycklar förstörs efter att deras giltighetstid har upphört.

Privata nycklar för serviceleverantörers personaktör arkiveras inte. Utfärdaren har inte tillgång till certifikatinnehavarnas privata nycklar.

7.2.6 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.

7.2.7 Förvaring av privata nycklar

Utfärdarens privata nycklar förvaras krypterade i kryptografiska moduler.

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

7.2.8 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 certifikatkortets 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 kod.

Koden på certifikatkortet låses efter att koden matats fel fem gånger.

Låsningen av koden kan öppnas med rätt öppningskod.

7.2.9 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 certifikatkortets privata nycklar förhindras genom att avlägsna certifikatkortet från kortläsaren.

7.2.10 Förstörande av en privat nyckel

Bara certifikatutfärdaren kan förstöra utfärdarens privata nycklar.

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

Om serviceleverantörers personaktör vill förstöra sin egen privata nyckel, ska denne anmäla spärrtjänsten om spärrningen av certifikatkortet i fråga och se till att informationen på certifikatkortets chips förstörs till exempel genom att klippa kortet itu.

7.2.11 Klassificering av säkerhetsnivån av certifikatkort och kryptografiska moduler

Certifikatkorten och de kryptografiska modulerna ska uppfylla de standarder och klasser som nämns i kapitel 6.2.1.

7.3 Andra faktorer som påverkar hanteringen av nyckelparet

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

7.3.1 Arkivering av publika nycklar

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

7.3.2 Giltighetstiden för certifikat och nycklar

Serviceleverantörers certifikat och nyckelpar för personaktörer är giltiga i högst 60 månader. Giltighetstiden börjar från tidpunkten för beviljande av certifikatet. Certifikatet kan vid behov beviljas för en kortare bestämd tid.

Giltighetstiden för utfärdarens certifikat och nyckelpar är 16 år från tidpunkten av skapandet av nycklarna. Nycklar används inte före giltighetstiden eller efter giltighetstiden för något ändamål.

7.4 Aktiveringsuppgifter

7.4.1 Skapande av aktiveringsuppgift

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

Öppningskoden som behövs för att öppna en låst kod är 8 tecken lång. Öppningskoden förvaras i utfärdarens datasystem.

7.4.2 Skydd av aktiveringsuppgift

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

7.4.3 Andra faktorer om aktiveringsuppgiften

—

7.5 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.

7.5.1 Särskilda krav

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

7.5.2 Klassificering av utrustningssäkerhet

—

7.6 Hantering av säkerhet under livscykeln

7.6.1 Hantering av systemutveckling

Utvecklingen av utfärdarens system sker i utvecklings- och testmiljöer 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.

7.6.2 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 kapitel 5.2;
- uppföljning av säkerhet;
- regelbundna säkerhetskontroller;
- tekniska skyddslösningar och -metoder; samt
- förfarande för befullmäktigande och godkännande av applikationsändringar.

7.6.3 Säkerhetsklassificering av livscykeln

—

7.7 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.

7.8 Tidsstämpel

Tidsstämpeltjänsten är för tillfället inte i bruk.

VRK/TS/Keh

3.5.2018

Profil för certifikat och spärrlista

8.1 Profil för certifikat

Profilen för serviceleverantörers certifikat för personaktörer har beskrivits i bestämningen Befolkningsregistercentralens CA-mall för hälso- och sjukvården

= THPKI - T2: Befolkningsregistercentralens CA-mall och certifikatens datainnehåll inom hälsovården.

8.2 Profil för spärrlista

Profilen för spärrlistan för serviceleverantörers certifikat för personaktörer har beskrivits i bestämningen Befolkningsregistercentralens CA-mall för hälso- och sjukvården = THPKI - T2: Befolkningsregistercentralens CA-mall och certifikatens datainnehåll inom hälsovården.

8.3 Kontroll av spärrlista i realtid (OCSP)

OCSP-protokollet är tillgängligt.

Godkännandekontroll

Utfärdaren svarar för att dess certifieringsverksamhet följer denna certifieringspraxis samt certifikatpolicy. Kommunikationsverket som övervakar utfärdare kan inspektera utfärdarens verksamhet under de förutsättningar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster.

Utfärdaren kan inspektera sina tekniska leverantörer i enlighet med vad som kommits överens i leveransavtalen med de tekniska leveverantörerna. Inspektionen görs minst en gång om året och alltid när en ny avtalsperiod börjar.

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

Inspektionen utförs av Befolkningsregistercentralens dataskyddschef eller en av Befolkningsregistercentralen skaffade utomstående inspektör som är specialiserad på auditering av tekniska leverantörer av certifikattjänster. Inspektionen görs genom att beakta genomförandet av dataskyddets åtta delområden. Dataskyddsegenskaper som inspekteras är bl.a. konfidentialitet, integritet och användbarhet.

Inspektionen omfattar Kommunikationsverkets bestämmelser om datasäkerhet för utfärdaren.

9.1 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.

9.2 Inspektör

Inspektionen utförs 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.

9.3 Inspektörens förhållande till part som inspekteras

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

9.4 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.

9.5 Åtgärder som ska vidtas vid avvikelser

Utfärdaren vidtar utan fördröjning korrigerande åtgärder vid upptäckta avvikelser.

9.6 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.

Allmänna villkor

Detta kapitel innehåller skyldigheter och ansvar för utfärdaren, registreraren, certifikatinnehavaren och andra parter som anknyter till certifikatsystemets verksamhet samt frågor som gäller utredningen av konflikter.

10.1 Avgifter och andra arvoden

Avgifter och andra fastställs enligt 22 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), 25 § i lagen om elektroniska recept, lagen om grunderna för avgifter till staten (150/1992) och Finansministeriets förordning om avgifterna för Befolkningsregistercentralens prestationer (873/2008).

10.1.1 Avgift för beviljande av certifikat

—

10.1.2 Avgift för användning av certifikat

—

10.1.3 Avgift för spärrning av certifikat eller förfrågan om status

—

10.1.4 Avgifter för andra tjänster, såsom avgift för Stödtjänsten

—

10.1.5 Ersättningar

Ersättningar fastställs enligt avtalen med parterna för certifikatsystemet.

10.2 Ekonomiska skyldigheter

Utfärdaren ska enligt 13 § i lagen om stark autentisering och betrodda elektroniska tjänster ha med tanke på verksamhetens omfattning tillräckliga ekonomiska resurser för att ordna verksamheten och täcka ett eventuellt skadeståndsansvar.

10.3 Konfidentialitet och dataskydd

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

10.3.1 Privata uppgifter

Privata uppgifter kan endast avslöjas med stöd av en bestämmelse i finsk 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.

10.3.2 Offentliga uppgifter

Publika nycklar för verifikations- och krypteringscertifikat 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 finsk lag, förordning eller bestämmelser som utfärdats med stöd av dessa.

10.3.3 Skydd av privata uppgifter

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

10.4 Integritetsskydd

I fråga om integritetsskydd följs den gällande finska lagstiftningen.

10.4.1 Plan för skydd av privata uppgifter

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

10.4.2 Privata uppgifter som hanteras i utfärdarens system

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

10.4.3 Publika uppgifter som hanteras i utfärdarens system

Vid hanteringen av publika uppgifter i utfärdarens system följs lagen om offentlighet i myndigheternas verksamhet (621/1999).

10.4.4 Ansvar för skydd av privata uppgifter

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

10.4.5 Användning eller publicering av privata uppgifter med certifikatinnehavarens samtycke

Konfidentialiteten och dataskyddet av uppgifterna har fastställts i kapitel 9.3.

10.4.6 Utlämning av uppgifter till myndigheter

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

10.4.7 Andra omständigheter där uppgifter kan publiceras

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

10.5 Immaterialrättigheter

Alla upphovsrätter som anknyter till utfärdarens system har fastställts i avtalen mellan avtalsparterna.

10.6 Parternas förbindelser

10.6.1 Utfärdarens förbindelser

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

10.6.2 Registrerarens förbindelser

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

10.6.3 Certifikatinnehavarens förbindelser

Certifikatinnehavaren förbinder sig att använda serviceleverantörers certifikat för personaktörer och certifikatkortet enligt denna certifieringspraxis, certifikatpolicy och de givna anvisningarna.

10.6.4 De förlitande parternas förbindelser

De förlitande parterna förbinder sig att ansvara för att de egna hälsovårdssystemen och serviceleverantörers certifikat för personaktörer är kompatibla.

10.6.5 Andra parters förbindelser

—

10.7 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.

10.8 Ansvarsbegränsningar

Befolkningsregistercentralens skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Befolkningsregistercentralen 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).

Befolkningsregistercentralens ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Befolkningsregistercentralens omedelbara åtgärder, dock högst 15 procent av certifikatfaktureringen under de föregående tre månaderna (BRC:s andel) och kraven i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

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.

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.

Utfärdaren ansvarar inte för den skada som orsakats av att certifikatinnehavaren eller den instans som utnyttjar certifikatsystemet har verkat i strid mot lagen, denna certifieringspraxis, certifikatpolicy eller andra anvisningar.

Utfärdaren ansvarar aldrig för indirekta skador eller skador som orsakats av ett oöverstigligt hinder.

Utfärdaren kan också ställa andra ansvarsbegränsningar i avtalen om certifikatsystemet och i de krav som denne ställt för certifikatinnehavaren och den instans som utnyttjar certifikatsystemet.

10.9 Skadestånd

Befolkningsregistercentralens skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande serviceavtal med certifikatsökanden. På Befolkningsregistercentralen 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).

Befolkningsregistercentralens ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Befolkningsregistercentralens omedelbara åtgärder, dock högst 15 procent av certifikatfaktureringen under de föregående tre månaderna (BRC:s andel) och kraven i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

10.10 Giltighetstid och upphörande av giltighet

10.10.1 Giltighetstid för certifieringspraxis

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

10.10.2 Upphörande av giltighetstiden för certifieringspraxisen

Certifieringspraxisen har ingen separat bestämd giltighetstid.

10.10.3 Konsekvenser av upphörande av giltighetstiden för certifieringspraxisen

—

10.11 Kommunikation 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.

10.12 Hantering av ändringar i certifieringspraxisen

Utfärdaren beslutar om ändringar i certifieringspraxisen.

10.12.1 Ändring av certifieringspraxisen

De enda ändringar som kan göras i en godkänd certifieringspraxis utan informering om dessa, är rättelse av layouten eller skrivfel eller ändringar i kontaktuppgifterna. Om andra ändringar ska informeras 14 dagar innan certifieringspraxisen träder i kraft.

10.12.2 Information om ändringar

Certifikatutfärdaren informerar om andra ändringar i certifikatpolicyn än de som anges i kapitel 9.2.1 på sin webbplats (www.fineid.fi) minst 30 dagar innan ändringen träder i kraft.

10.12.3 Ändring av koduppgift i certifieringspraxisen

Koduppgiften i certifieringspraxisen ändras enligt kapitel 1.2 när innehållet i certifieringspraxisen ändras.

10.13 Avgörande av meningsskiljaktigheter

Eventuella tvister som gäller certifikattjänsten inom hälso- och sjukvården och denna certifieringspraxis hanteras i tingsrätten i utfärdarens hemort i Finland.

10.14 Tillämplig lag

På certifikattjänsten inom hälso- och sjukvården och denna certifieringspraxis tillämpas finsk lag.

10.15 Att följa lagen

Vid ordnandet av certifikattjänster inom hälso- och sjukvården följs enbart finsk lag.

10.16 Övriga arrangemang

10.16.1 Avtal

Certifikatansökan och de allmänna användningsvillkoren utgör ett avtal med certifikatsökanden. Användningsvillkoren ingår i certifikatpolicydokumenten. Rättigheterna, ansvar och skyldigheterna mellan utfärdaren och certifikatinnehavaren fastställs i certifikatpolicyn och certifieringspraxisen. Genom att underteckna certifikatansökan förbinder sig serviceleverantörers personaktör följa användningsvillkoren för certifikatet. De gällande användningsvillkoren ges till sökanden i samband med överlåtelsen av certifikatet.

Med sin underskrift förbinder sig serviceleverantörers personaktör 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.

10.16.2 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.

10.16.3 Partiell ogiltighetsklausul

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

10.16.4 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.

10.16.5 Oöverstigligt hinder

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

10.17 Övriga villkor

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