

CERTIFIERINGSPRAXIS FÖR TILLFÄLLIGT CERTIFIKAT

OID: 1.2.246.517.1.10.204.1



ISO 9001



ISO/IEC 27001



Väestörekisterikeskus



3.5.2018

VRK/TS/Keh

HANTERING AV DOKUMENT

| | |
|--------------|---------------------|
| Ägare | |
| Upprättat av | Saaripuu Tuire |
| Granskat av | |
| Godkänt av | Kankaanrinne Joonas |

VERSIONSHANTERING

| version nr | åtgärder | datum/person |
|------------|----------------------|--------------|
| v 1.0 | Godkänd version 1.0. | 3.5.2018 |

Innehållsförteckning

| | |
|----------------------------------------------------------------------|----|
| 1 Inledning..... | 12 |
| 1.1 Allmänt | 12 |
| 1.2 Identifikationsuppgifter | 13 |
| 1.3 Certifikatutfärdare och tillämpningsområden för certifikat | 14 |
| 1.3.1 Certifikatutfärdare | 14 |
| 1.3.2 Registrerare..... | 14 |
| 1.3.3 Tillverkare och specificerare av reservkort eller chips | 15 |
| 1.3.4 Spärrtjänst..... | 15 |
| 1.3.5 Publicering av uppgifter om tillfälliga certifikat | 15 |
| 1.3.6 Innehavare av certifikat | 15 |
| 1.3.7 Förlitande part | 15 |
| 1.3.8 Användning av certifikatet | 16 |
| 1.4 Kontaktuppgifter | 16 |
| 1.4.1 Organisation som administrerar certifieringspraxisen | 16 |
| 1.4.2 Kontaktperson | 16 |



3.5.2018

VRK/TS/Keh

| | |
|--------------------------------------------------------------------------------------------|----|
| 2 Allmänna villkor..... | 17 |
| 2.1 Skyldigheter..... | 17 |
| 2.1.1 Certifikatutfärdarens skyldigheter..... | 17 |
| 2.1.2 Registrerarens skyldigheter..... | 18 |
| 2.1.3 Certifikatinnehavarens skyldigheter..... | 18 |
| 2.1.4 Den förlitande partens skyldigheter..... | 19 |
| 2.1.5 Skyldigheter vid publicering av certifikatet..... | 19 |
| 2.2 Ansvar..... | 19 |
| 2.2.1 Certifikatutfärdarens ansvar..... | 19 |
| 2.2.2 Registrerarens ansvar..... | 20 |
| 2.2.3 Certifikatinnehavarens ansvar..... | 20 |
| 2.2.4 Den förlitande partens ansvar..... | 20 |
| 2.2.5 Begränsning av ansvar..... | 21 |
| 2.3 Ekonomiskt ansvar..... | 21 |
| 2.3.1 Certifikatutfärdare..... | 21 |
| 2.3.2 Andra parter..... | 21 |
| 2.3.3 Utfärdarens ekonomiförvaltning..... | 22 |
| 2.4 Tolkning och verkställighet..... | 22 |
| 2.4.1 Lagstiftning som tillämpas..... | 22 |
| 2.4.2 Avgörande av meningsskiljaktigheter..... | 23 |
| 2.5 Avgifter..... | 23 |
| 2.5.1 Beviljande och förnyelse av ett tillfälligt certifikat..... | 23 |
| 2.5.2 Avgifter som hänför sig till användningen av tillfälligt certifikat..... | 23 |
| 2.5.3 Avgifter som hänför sig till markering av tillfälligt certifikat på spärrlistan..... | 23 |
| 2.5.4 Övriga avgifter..... | 23 |
| 2.6 Publicering och tillgänglighet av uppgifter..... | 24 |
| 2.6.1 Publicering av utfärdarens uppgifter..... | 24 |
| 2.6.2 Publiceringsfrekvens..... | 24 |
| 2.6.3 Uppgifternas tillgänglighet..... | 24 |
| 2.6.4 Dataförvaring..... | 24 |
| 2.7 Dataskyddsinspektion..... | 24 |
| 2.7.1 Frekvens av inspektioner..... | 24 |
| 2.7.2 Inspektör..... | 25 |
| 2.7.3 Målen för och omfattningen av inspektionen..... | 25 |
| 2.7.4 Åtgärder vid avvikelser..... | 26 |



3.5.2018

VRK/TS/Keh

| | |
|------------------------------------------------------------------------------------------------------------|----|
| 2.7.5 Information om resultatet av inspektionen..... | 26 |
| 2.8 Publicering av uppgifter..... | 26 |
| 2.8.1 Uppgifter som publiceras av utfärdaren | 26 |
| 2.8.2 Offentliga uppgifter | 27 |
| 2.8.3 Uppgifter som anknyter till upphörande eller avbrott av det tillfälliga certifikatets giltighet..... | 27 |
| 2.8.4 Uppgifter som lämnas ut till myndigheter..... | 27 |
| 2.8.5 Övriga uppgifter..... | 27 |
| 2.8.6 Överlåtelse av uppgifter på certifikatinnehavarens begäran | 27 |
| 2.8.7 Övriga principer för överlåtelse av uppgifter | 27 |
| 2.9 Immaterialrättigheter | 27 |
| 3 Identifiering av certifikatsökande | 28 |
| 3.1 Registrering..... | 28 |
| 3.1.1 Namngivningspraxis | 28 |
| 3.1.2 Leverans av privata nycklar till certifikatinnehavaren | 29 |
| 3.2 Förnyelse av nyckelpar..... | 30 |
| 3.3 Förnyelse av nyckelpar efter införande av certifikat på spärrlista | 30 |
| 3.4 Identifiering av den person som gjort begäran om spärrning | 30 |
| 4 Funktionella krav | 31 |
| 4.1 Ansökan om certifikat..... | 31 |
| 4.2 Beviljande av certifikat..... | 31 |
| 4.3 Mottagning av certifikat..... | 31 |
| 4.4 Upphörande och avbrott av certifikatets giltighet | 31 |
| 4.4.1 Förutsättningar för spärrning av ett certifikat | 31 |
| 4.4.2 Person som gör begäran om spärrning..... | 32 |
| 4.4.3 Spärrning | 32 |
| 4.4.4 Tidpunkten för spärrning | 33 |
| 4.4.5 Krav på avbrott av certifikatets giltighet | 33 |
| 4.4.6 Person som gör begäran om avbrott..... | 33 |
| 4.4.7 Begäran om avbrott | 33 |
| 4.4.8 Begränsningar av avbrottsstid | 33 |
| 4.4.9 Publiceringsfrekvens för spärrlista | 33 |
| 4.4.10 Krav på kontroll av spärrlista | 33 |
| 4.4.11 Kontroll av certifikatets status online | 33 |
| 4.4.12 Krav på kontroll av certifikatets status online | 33 |
| 4.4.13 Särskilda krav gällande avslöjande av certifikatinnehavarens privata nyckel | 34 |



3.5.2018

VRK/TS/Keh

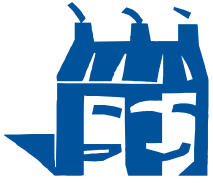
| | |
|--------------------------------------------------------------------------------------------|----|
| 4.5 Övervakning av systemet..... | 34 |
| 4.6 Arkivering av uppgifter om certifikat | 34 |
| 4.6.1 Material som sparas | 34 |
| 4.6.2 Skydd av arkiv | 35 |
| 4.6.3 Säkerhetsförfaranden för arkiverat material | 35 |
| 4.6.4 Metoder för införskaffning och tryggnad av arkiverat material | 35 |
| 4.7 Hantering av kontinuerlig verksamhet och undantagsfall | 35 |
| 4.7.1 Utfärdarens privata nyckel har röjts eller Utfärdarens certifikat har spärrats | 35 |
| 4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof..... | 36 |
| 4.8 Då utfärdarens verksamhet upphör | 36 |
| 5 Krav på fysisk, funktionell och personalsäkerhet | 37 |
| 5.1 Arrangemang kring fysisk säkerhet..... | 37 |
| 5.1.1 Läge och lokalernas egenskaper | 37 |
| 5.1.2 Fysisk tillgång till verksamhetslokalen..... | 37 |
| 5.1.3 Elmatning och luftkonditionering | 37 |
| 5.1.4 Brandsäkerhet..... | 37 |
| 5.1.5 Förvaring av uppgifterna | 37 |
| 5.1.6 Hantering av onödigt informationsmaterial | 38 |
| 5.1.7 Vattenskador..... | 38 |
| 5.1.8 Reservarrangemang | 38 |
| 5.2 Funktionella krav | 38 |
| 5.2.1 Ansvarsfördelning | 38 |
| 5.2.2 Antal personer som behövs för uppgifterna | 38 |
| 5.2.3 Uppgiftsspecifik autentisering..... | 39 |
| 5.3 Personlig säkerhet | 39 |
| 5.3.1 Utförande av bakgrundskontroll av personalen | 39 |
| 5.3.2 Förfarande vid utförande av bakgrundskontroll | 39 |
| 5.3.3 Krav på utbildning | 40 |
| 5.3.4 Underhåll av expertis och kompetens..... | 40 |
| 5.3.5 Krav på uppgiftsrotation..... | 40 |
| 5.3.6 Åtgärder vid avvikelser | 40 |
| 5.3.7 Personal som representerar organisationen | 40 |
| 5.3.8 Handlingar som tillhandahålls personalen | 40 |
| 6 Tekniska säkerhetsarrangemang..... | 41 |
| 6.1 Skapande och sparande av nyckelpar..... | 41 |



3.5.2018

VRK/TS/Keh

| | |
|-----------------------------------------------------------------------------------|----|
| 6.1.1 Skapande av nyckelpar | 41 |
| 6.1.2 Överlåtelse av en privat nyckel till certifikatinnehavaren..... | 41 |
| 6.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren | 41 |
| 6.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren | 42 |
| 6.1.5 Nycklarnas längder..... | 42 |
| 6.1.6 Nycklarnas användningsändamål:..... | 42 |
| 6.2 Skydd av privat nyckel | 42 |
| 6.2.1 Standarder som gäller den kryptografiska modulen..... | 42 |
| 6.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel | 42 |
| 6.2.3 Överlåtelse av en privat nyckel till förlitande part..... | 43 |
| 6.2.4 Säkerhetskopior av en privat nyckel | 43 |
| 6.2.5 Arkivering av en privat nyckel | 43 |
| 6.2.6 Administration av en privat nyckel i kryptografiska moduler..... | 43 |
| 6.3 Andra faktorer som anknyter till nyckeladministration | 43 |
| 6.3.1 Arkivering av en publik nyckel | 43 |
| 6.3.2 Användningstid för publika och privata nycklar..... | 43 |
| 6.4 Aktiveringsuppgift | 44 |
| 6.4.1 Skapande och ibruktage av aktiveringsuppgift..... | 44 |
| 6.4.2 Skydd av aktiveringsuppgift..... | 44 |
| 6.4.3 Andra faktorer som anknyter till aktiveringsuppgiften | 44 |
| 6.5 Säkerhetskrav som gäller användning av datorer och tillgång till dessa | 44 |
| 6.5.1 Utrustningssäkerhet..... | 44 |
| 6.6 Livscykeladministration av certifikatsystemet..... | 44 |
| 6.6.1 Övervakning som gäller systemutvecklingen | 45 |
| 6.6.2 Hantering av säkerhet..... | 45 |
| 6.7 Datanätets säkerhet..... | 45 |
| 6.8 Övervakning av användning av kryptografisk modul | 45 |
| 7 Profiler för certifikat och spärllistor | 45 |
| 7.1 Tekniska uppgifter om certifikat..... | 45 |
| 7.2 Profil för spärllistor | 45 |
| 8 Hantering av dokument innehållande bestämmelser | 46 |
| 8.1 Ändring av bestämmelser | 46 |
| 8.2 Publicering och information..... | 46 |
| 8.3 Förfarande för ändring och godkännande av certifikatpolicy | 46 |



VRK/TS/Keh

CERTIFIERINGSPRAXIS Dnro 798/617/16 7 (46)
FÖR TILLFÄLLIGT CERTIFI-
KAT v.1.0

3.5.2018



VRK/TS/Keh

3.5.2018

DEFINITIONER OCH FÖRKORTNINGAR

Definitioner

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

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

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

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

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

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

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

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

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

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

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

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

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



VRK/TS/Keh

3.5.2018

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

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

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

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

Yrkesutbildad person inom hälso- och sjukvården En yrkesutbildad person inom hälso- och sjukvården som med stöd av lagen har erhållit rätt att utöva yrke (legitimerad yrkesutbildad person) eller tillstånd att utöva yrke (yrkesutbildad person som beviljats tillstånd) samt som med stöd av denna lag har rätt att använda i förordning av statsrådet avsedd yrkesbeteckning för en yrkesutbildad person inom hälso- och sjukvården (yrkesutbildad person med skyddad yrkesbeteckning) och som har registrerats i centralregistret övre yrkesutbildade personer inom hälso- och sjukvården.

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

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

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

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

Aktörer inom social- och hälsovården: anställda hos serviceleverantörer inom social- och hälsovården som inte är yrkesutbildade personer inom social- och hälsovården eller personal inom social- och hälsovården. I gruppen i fråga ingår övriga personer och specialgrupper som använ-



VRK/TS/Keh

3.5.2018

der riksomfattande datasystem, såsom dataskyddsansvariga samt datasystemleverantörer, konsulter osv.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



VRK/TS/Keh

3.5.2018

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

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

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

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

Lista över förkortningar

| | |
|------------------------------|--------------------------------------------------------------------------------------------|
| CA | Certification Authority, certifikatutfärdare |
| CP | Certificate Policy, certifieringspolicy |
| CPS | Certification Practise Statement, certifieringspraxis |
| CRL | Certificate Revocation List, spärrlista |
| FINEID | Finnish Electronic Identification |
| HSM | Hardware Security Module, kryptografisk modul |
| HST | Elektronisk identifiering av person |
| HTTP | Hypertext Transport Protocol |
| ISO 27001 | ISO/IEC 27001 |
| LDAP | Lightweight Directory Access Protocol |
| OCSP certifikatets status | Online Certificate Status Protocol, onlinetjänst för återställande av certifikatets status |
| OID | Object Identifier, identifierande kod |
| PDS | PKI Disclosure Statement, certifikatbeskrivning |
| PIN | Personal Identification Number, PIN-kod |
| PKI | Public Key Infrastructure, öppet nyckelsystem |
| PUK | PIN Unblocking Key, PUK-kod |



3.5.2018

VRK/TS/Keh

RSA Rivest, Shamir, Adleman, en algoritm för publik nyckel, icke-symmetrisk algoritm

BRC Befolkningsregistercentralen

1 Inledning

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

Certifieringspraxis tillämpas på Befolkningsregistercentralens tillfälliga certifikat.

Ett tillfälligt certifikat är ett certifikat som stödjer användningen av organisationscertifikat beviljat av Befolkningsregistercentralen, OID:1.2.246.517.1.10.203.

1.1 Allmänt

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

Ett tillfälligt certifikat är ett verifikations- och krypteringscertifikat eller ett verifikations- och krypteringscertifikat samt signaturcertifikat. Befolkningsregistercentralen garanterar identitetens riktighet.

Ett tillfälligt certifikat enligt denna policy kan beviljas en organisationskund. Om en organisationskund registrerar tillfälliga certifikat för personalen inom hälso- och socialvården eller aktörer inom social- och hälsovården ska alla de parter som avses i denna certifikatpolicy följa lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de författningar som utfärdats med stöd av dessa och de krav som ställts med stöd av dessa.

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

Det tillfälliga certifikatet kan lagras på olika aktivkort.

Befolkningsregistercentralens certifikatpolicy och certifieringspraxis har en egen unik kod (OID).

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

Befolkningsregistercentralen skapar en separat certifikatpolicy för varje typ av certifikat som den utfärdar som för varje tekniskt underlag för certifieringspraxis. Certifikatpolicy beskriver de för-



VRK/TS/Keh

3.5.2018

faringsätt, som används per certifikattyp användarvillkor och ansvarsfördelning och övriga aspekter av användningen av certifikat på ett allmänt plan. Certifieringspraxis beskriver de förfaringsätt som tillämpas på ett detaljerat plan.

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

Utfärdaren är leverantör av certifikattjänster och beviljar certifikat enligt Förordningen.

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

Befolkningsregistercentralen har fungerat som lagstadgad certifikatutfärdare för hälsovården sedan 1.12.2010 och fungerar dessutom som lagstadgad certifikatutfärdare för socialvården sedan 1.4.2015 med stöd av ändringar i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) samt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009). Befolkningsregistercentralens enhet för certifikattjänster ansvarar för verkets certifikatverksamhet.

1.2 Identifikationsuppgifter

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

Denna certifieringspraxis heter Certifieringspraxis för Befolkningsregistercentralens tillfälliga certifikat vars OID är 1.2.246.517.1.10.204.1.

Denna certifieringspraxis refererar till Certifikatpolicyn för tillfälliga certifikat vars OID är 1.2.246.517.1.10.204.

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.

Både certifikatpolicyn och certifieringspraxisen finns på adressen www.fineid.fi.



3.5.2018

VRK/TS/Keh

1.3 Certifikatutfärdare och tillämpningsområden för certifikat

Utfärdaren producerar certifikattjänster enligt villkoren i denna certifieringspraxis och ansvarar för att de fungerar i innehavarens användning enligt 2.2.1 som beskriver utfärdarens ansvar. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifieringspraxis är registrerad av Befolkningsregistercentralen. Befolkningsregistercentralen är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) är att utöver övriga tjänster producera tjänster inom certifierad elektronisk kommunikation. Befolkningsregistercentralens certifikattjänst indelas operativt i följande delområden:

1.3.1 Certifikatutfärdare

Utfärdarens uppgift är att:

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

1.3.2 Registrerare

Registreringen av ett tillfälligt certifikat sker enligt förfarandet i lagen om stark autentisering och betrodda elektroniska tjänster och denna certifieringspraxis. Registreraren för tillfälliga certifikat på reservkort är samarbetspartnern som ingått ett registreringsavtal med Befolkningsregistercentralen.

- Registreraren agerar på certifikatutfärdarens uppdrag och ansvar.
- Registreraren följer certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Registreraren identifierar certifikatsökanden enligt certifieringspraxisen.
- Registreringsstället levererar de uppgifter som anknyter till identifiering av personen och till ansökan av certifikatet, enligt vilka certifikatet skapas.
- Registreraren följer principer för god hantering av personuppgifter i sitt uppdrag.



VRK/TS/Keh

3.5.2018

- Befolkningsregistercentralen övervakar att kundorganisationen följer de villkor för registrering som nämns i avtalet och de bestämmelser som gäller registrering i lagen om stark autentisering och betrodda elektroniska tjänster.
- Registreraren använder det beställnings- och administrationssystem som certifikatutfärdaren erbjudit för registrering, beställning och spärrning av reservkort.

1.3.3 Tillverkare och specificerare av reservkort eller chips

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

1.3.4 Spärrtjänst

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

1.3.5 Publicering av uppgifter om tillfälliga certifikat

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

1.3.6 Innehavare av certifikat

Ett organisationscertifikat enligt denna certifieringspraxis kan beviljas de personer som identifierats enligt lagen om stark autentisering och betrodda elektroniska tjänster eller i fråga om personal inom social- och hälsovården eller aktörer inom social- och hälsovården kan tillfälliga certifikat dessutom överlåtas enligt kraven i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de förordningar som utfärdats med stöd av dessa. Innehavare av ett tillfälligt certifikat för personal inom social- och hälsovården och aktörer inom hälso- och sjukvården kan vara personal inom social- och hälsovården eller en aktör inom social- och hälsovården.

Certifikatinnehavaren ska följa certifikatutfärdarens certifikatpolicy och certifieringspraxis.

1.3.7 Förlitande part

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



3.5.2018

VRK/TS/Keh

1.3.8 Användning av certifikatet

Befolkningsregistercentralen följer denna certifieringspraxis när den beviljar tillfälliga certifikat. Certifikatinnehavare och förlitande parter ska följa denna certifieringspraxis.

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

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

1.4 Kontaktuppgifter

1.4.1 Organisation som administrerar certifieringspraxisen

Denna certifikatpolicy är registrerad av Befolkningsregistercentralen. Befolkningsregistercentralen är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) är att utöver övriga tjänster producera tjänster inom certifierad elektronisk kommunikation. Befolkningsregistercentralen svarar för administrationen och uppdateringen av denna certifikatpolicy.

Upphovsrätten enligt denna certifieringspraxis tillfaller Befolkningsregistercentralen.

1.4.2 Kontaktperson

Frågor som gäller denna certifieringspraxis skickas till följande adress:

Befolkningsregistercentralen (BRC) vaestorekisterikeskus@vrk.fi

PB 123 (Fågelviksgränden 4) Tfn 0295 535 001

00531 Helsingfors Fax (09) 876 4369

FO-nummer: 0245437-2

Frågor som gäller certifikatpolicyn besvaras av Befolkningsregistercentralens Certifikattjänstenhet.



3.5.2018

VRK/TS/Keh

2 Allmänna villkor

Denna certifieringspraxis träder i kraft 3.5.2018. Ändringsförfarandet för och publiceringen av certifieringspraxisen har beskrivits i punkt 8 i detta dokument.

2.1 Skyldigheter

2.1.1 Certifikatutfärdarens skyldigheter

- Befolkningsregistercentralen har ett lagstadgat uppdrag att fungera som certifikatutfärdare.
- Kundorganisationen ansvarar för sin del för spärrning av certifikat enligt avtalet mellan BRC och kundorganisationen.
- Kundorganisationen ska kontrollera riktigheten av uppgifter som gäller slutanvändarna enligt avtalet mellan BRC och kundorganisationen.
- Utfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser samt möjlighet att hantera krav på skadeersättning.
- Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer eller personer som man anlitar, t.ex. registrerare och korttillverkare.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning för beviljande av tillfälliga certifikat samt övriga aspekter av användningen av det tillfälliga certifikatet på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyen.
- Utfärdaren följer certifikatpolicyen och certifieringspraxisen.
- Utfärdaren publicerar certifikatpolicyen och certifieringspraxisen och gör dem allmänt tillgängliga.
- Utfärdaren anställer tillräckligt med personal med den expertis, erfarenhet och kompetens som fordras för produktionen av certifikattjänster.
- Utfärdaren använder pålitliga system och produkter som är skyddade från otillbörlig användning.
- Utfärdaren tillhandahåller offentligt information om certifikat och certifikatverksamheten, utgående från vilken utfärdarens verksamhet och pålitlighet kan bedömas.



VRK/TS/Keh

3.5.2018

- Utfärdaren säkerställer att uppgifterna för skapande av signatur är tillförlitliga.
- Utfärdaren sparar eller kopierar inte uppgifter för skapande av signatur som lämnats till undertecknaren.

2.1.2 Registrerarens skyldigheter

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

2.1.3 Certifikatinnehavarens skyldigheter

- Användningsändamålet för certifikatet har fastställs i varje certifikattyps certifikatpolicy, certifieringspraxis och certifikatinnehavarens användningsvillkor. Certifikat får endast användas enligt dess användningsändamål för verifikation, kryptering eller elektronisk signatur.
- Innehavaren av det tillfälliga certifikatet ansvarar för att de uppgifter som uppges då man ansöker om det tillfälliga certifikatet är riktiga.
- Certifikatinnehavaren ansvarar för användningen av det tillfälliga certifikatet, de rättshandlingar som denne gör med certifikatet och deras ekonomiska följder.
- Innehavaren av det tillfälliga certifikatet förvarar de privata nycklar som finns på chipset och den kod som behövs för att använda dessa separat samt strävar efter att förhindra att de privata nycklarna försvinner, hamnar i utomståendes händer, ändras eller används olovligt. Att lämna chipset eller avslöja PIN-koden för en annan person, t.ex. genom att låna, frigör utfärdaren och parten som litar på det tillfälliga certifikatet från eventuellt ansvar som orsakas av användningen av chipset.
- Det tillfälliga certifikatet hanteras och skyddas med samma noggrannhet som andra motsvarande chips, kort eller dokument, såsom kreditkort, körkort och pass. Personliga PIN-koder ska förvaras fysiskt på annat ställe än chipset som innehåller det tillfälliga certifikatet och de privata nycklarna.
- Om chipset eller kortet försvinner eller om det finns möjlighet till missbruk, ska man omedelbart meddela registreraren i organisationen för certifikatinnehavaren, som spär certifikatet i beställnings- och administrationssystemet för kort.



3.5.2018

VRK/TS/Keh

2.1.4 Den förlitande partens skyldigheter

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

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

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

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

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

2.1.5 Skyldigheter vid publicering av certifikatet

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

2.2 Ansvar

2.2.1 Certifikatutfärdarens ansvar

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

Befolkningsregistercentralen svarar för att det tillfälliga certifikatet har skapats enligt de förfaranden som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster, certifieringspolicyn samt certifieringspraxisen och enligt de uppgifter sökanden har uppgett och att det uppfyller utfärdarens skadeståndsansvar som fastställs i lagarna eller om det är fråga om ett tillfälligt certifikat som skapas för personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas. Befolkningsregistercentralen ansvarar endast för den information som man sparar i certifikatet.

Befolkningsregistercentralen svarar för att det tillfälliga certifikatet används sakligt, och att det är tillgängligt för användning från att det överläts under hela dess giltighetstid, förutsatt att



VRK/TS/Keh

3.5.2018

certifikatet inte spärras. Det tillfälliga certifikatet har överlåtits till en person som har identifierats på det sätt som förutsätts av det tillfälliga certifikatet. Certifikatinnehavaren har före undertecknandet av avtalet fått anvisningar för användning av det tillfälliga certifikatet.

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

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

2.2.2 Registrerarens ansvar

Registreraren för det tillfälliga certifikatet är det registreringsställe som registrerar certifikatet för Befolkningsregistercentralen som är utfärdare enligt ett avtal som separat ingåtts för denna verksamhet. Registreraren ansvarar för den registrering som denne gjort och för spärrningen av certifikatet. I fråga om registreringen följs kraven som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och certifieringspraxisen eller om det är fråga om ett tillfälligt certifikat som skapas för personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas.

2.2.3 Certifikatinnehavarens ansvar

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

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

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

2.2.4 Den förlitande partens ansvar

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



3.5.2018

VRK/TS/Keh

2.2.5 Begränsning av ansvar

På Befolkningsregistercentralen tillämpas lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar bestämmelserna i skadeståndslagen (412/1974).

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

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 den ifrågavarande kundorganisationens certifikatfakturering under de föregående tre månaderna (BRC:s andel).

Befolkningsregistercentralen svarar inte för indirekta skador eller följdskador som har orsakats certifikatinnehavaren. Befolkningsregistercentralen svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter för certifikatinnehavaren.

Befolkningsregistercentralen 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 spärllistan meddelas på förhand.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Certifikatinnehavare eller förlitande parter ska i sådana fall svara för egna kostnader som följer av detta och utfärdaren är inte skyldig att ersätta certifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

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

2.3 Ekonomiskt ansvar

2.3.1 Certifikatutfärdare

På Befolkningsregistercentralen tillämpas lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar bestämmelserna i skadeståndslagen (412/1974). I fråga om den förlitande parten ansvarar befolkningsregistercentralen för högst orsakade direkta skador enligt punkten ansvarsbegränsningar.

2.3.2 Andra parter

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



VRK/TS/Keh

3.5.2018

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

2.3.3 Utfärdarens ekonomiförvaltning

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

2.4 Tolkning och verkställighet

2.4.1 Lagstiftning som tillämpas

På Befolkningsregistercentralen tillämpas lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar bestämmelserna i skadeståndslagen (412/1974). Om det är fråga om ett tillfälligt certifikat som skapas för personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas.

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

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

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

Om Befolkningsregistercentralens ställning föreskrivs i lagen (166/1996) och förordningen om registerförvaltningen (248/1996).

Befolkningsregistercentralen svarar för att de tillfälliga certifikaten har skapats enligt de förfaranden som beskrivs i lagen om stark autentisering och betrodda elektroniska tjänster samt certifikatpolicy och certifieringspraxisen. Ett tillfälligt certifikat skapas enligt de uppgifter som sökanden har uppgett eller om det är fråga om personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas.



VRK/TS/Keh

3.5.2018

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

I fråga om hantering av personuppgifter följer Befolkningsregistercentralen personuppgiftslagen. Befolkningsregistercentralen samarbetar kontinuerligt med Dataombudsmannen i fråga om hanteringen av personuppgifter.

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

2.4.2 Avgörande av meningsskiljaktigheter

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

2.5 Avgifter

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

2.5.1 Beviljande och förnyelse av ett tillfälligt certifikat

Ett tillfälligt certifikat ansöks enligt vad som beskrivs i certifieringspraxisen.

Priset på reservkortet fastställs enligt finansministeriets vid var tid gällande förordning om avgifterna för Befolkningsregistercentralens prestationer.

Tillfälliga certifikat prissatts enligt Befolkningscentralens giltiga prislista för företagsekonomiska prestationer.

2.5.2 Avgifter som hänför sig till användningen av tillfälligt certifikat

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

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

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

2.5.4 Övriga avgifter

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

Om tjänstleverantören vill ordna en informationsförsörjningstjänst mellan en kod som specificerar tillfälliga certifikat och koduppgifter i sitt eget bakgrundssystem eller andra uppdateringsuppgifter, kan tjänstleverantören ansöka om tillstånd till överlåtelse av uppgifter i informat-



VRK/TS/Keh

3.5.2018

ionstjänsten hos Befolkningsregistercentralen. Denna tjänst prissätts enligt den giltiga lagen om grunderna för avgifter till staten och finansministeriets förordning om avgifterna för Befolkningsregistercentralens prestationer.

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

2.6 Publicering och tillgänglighet av uppgifter

2.6.1 Publicering av utfärdarens uppgifter

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

2.6.2 Publiceringsfrekvens

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

2.6.3 Uppgifternas tillgänglighet

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

2.6.4 Dataförvaring

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

2.7 Dataskyddsinspektion

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

2.7.1 Frekvens av inspektioner

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



VRK/TS/Keh

3.5.2018

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

2.7.2 Inspektör

Befolkningsregistercentralens dataskyddsinsektion görs av Befolkningsregistercentralens dataskyddschef eller en utomstående inspektör som är specialiserad på auditering av tekniska leverantörer av certifikattjänster.

2.7.3 Målen för och omfattningen av inspektionen

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

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

I inspektionen jämförs policyn, certifieringspraxisen och tillämpningsanvisningar med hela certifikatorganisationens och -systemets verksamhet. Befolkningsregistercentralen kontrollerar att tillämpningsanvisningarna är enhetliga med certifikatpolicyn.

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

Spärrtjänst:

- Datakommunikationssäkerhet
- Personalsäkerhet
- Fysisk säkerhet

Certifikatproduktion:

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

Kortproduktion:

- produktionslinjen som helhet i hela dess sträckning
- kvalitetskontroll vid kortproduktion



VRK/TS/Keh

3.5.2018

- datakommunikationssäkerhet
- personalsäkerhet
- fysisk säkerhet

Registertjänst:

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

HelpDesk-verksamhet:

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

2.7.4 Åtgärder vid avvikelser

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

2.7.5 Information om resultatet av inspektionen

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

Befolkningsregistercentralen informerar bland annat Kommunikationsverket om resultaten av inspektionen.

2.8 Publicering av uppgifter

2.8.1 Uppgifter som publiceras av utfärdaren

Uppgifterna i certifikatsystemet är konfidentiella, om de inte grundar sig på bestämmelser om överlåtelse av uppgifter enligt personuppgiftslagen, lagen om elektronisk kommunikation i myndigheternas verksamhet och lagen om befolkningsdatasystemet och Befolkningsregister-



3.5.2018

VRK/TS/Keh

centralens certifikattjänster (661/2009) eller lagen om stark autentisering och betrodda elektroniska tjänster eller de ändamål som fastställs i certifikatpolicy eller certifieringspraxisen.

2.8.2 Offentliga uppgifter

Uppgifterna i det offentliga registret och spärllistan är offentliga, likaså de uppgifter som fastställs i certifieringspraxisen och certifikatpolicy, samt de publicerade FINEID-specifieringarna.

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

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

2.8.4 Uppgifter som lämnas ut till myndigheter

Uppgifter som lämnas ut till myndigheter fastställs enligt gällande lagstiftning.

2.8.5 Övriga uppgifter

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

2.8.6 Överlåtelse av uppgifter på certifikatinnehavarens begäran

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

2.8.7 Övriga principer för överlåtelse av uppgifter

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

I hanteringen av personuppgifter följer Befolkningsregistercentralen personuppgiftslagen samt speciallagstiftningen. Befolkningsregistercentralen har berett uppförandekoder för överlåtelse av uppgifter samt hantering av personuppgifter i samband med certifikatverksamheten. Särskild noggrannhet iaktas i hanteringen av personuppgifter.

2.9 Immaterialrättigheter

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



3.5.2018

VRK/TS/Keh

3 Identifiering av certifikatsökande

3.1 Registrering

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

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

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

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

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

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

3.1.1 Namngivningspraxis

Befolkningsregistercentralens rotutfärdare är:

CN (Common name) = VRK Gov. Root CA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Vaestorekisterikeskus CA

S (State) = Finland

C (Country) = FI



VRK/TS/Keh

3.5.2018

Befolkningsregistercentralens utfärdare av tillfälliga certifikat är:

CN (Common name) = VRK CA for Temporary Certificates – G2

OU (Organizational unit) = Tilapaisvarmenteet

O (Organization) = Vaestorekisterikeskus CA

C (Country) = FI

Certifikatinnehavarens namngivningspraxis för tillfälliga certifikat:

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

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

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

3.1.2 Leverans av privata nycklar till certifikatinnehavaren

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



VRK/TS/Keh

3.5.2018

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

3.2 Förnyelse av nyckelpar

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

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

3.3 Förnyelse av nyckelpar efter införande av certifikat på spärrlista

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

3.4 Identifiering av den person som gjort begäran om spärrning

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

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

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

Alla elektroniska åtgärder vid spärrning arkiveras.



3.5.2018

VRK/TS/Keh

4 Funktionella krav

4.1 Ansökan om certifikat

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

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

Man ansöker om ett tillfälligt certifikat genom att personligen besöka ett registreringsställe som är registrerare. Vid ansökan om certifikat kontrolleras identiteten mot ett giltigt dokument som utfärdats av polisen och som styrker personens identitet, till exempel ett ID-kort och pass som utfärdats efter den 11 mars 1999 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. Uppgiften om identifieringssättet antecknas på ansökningsblanketten och tjänstemannen vid registreringsstället bekräftar med sin underskrift att en verifiering av identiteten har ägt rum.

4.2 Beviljande av certifikat

Utfärdaren beviljar det tillfälliga certifikatet då utfärdaren godkänner certifikatansökan.

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

4.3 Mottagning av certifikat

De tillfälliga certifikaten hämtas personligen från registreringsstället.

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

4.4 Upphörande och avbrott av certifikatets giltighet

4.4.1 Förutsättningar för spärrning av ett certifikat

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



3.5.2018

VRK/TS/Keh

4.4.2 Person som gör begäran om spärning

Begäran om spärning görs av registreraren i certifikatinnehavarens organisation.

4.4.3 Spärning

Ett certifikat kan spärras via Befolkningsregistercentralens beställnings- och administrationssystem för kort.

Uppgiften om införandet av certifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärning har konstaterats vara behörig och godkänd. Spärrlistan är giltig i åtta timmar.

Spärning av tillfälliga certifikat

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

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

Spärrade certifikat kan inte tas i bruk igen.

Spärning av certifikat på uppdrag av Befolkningsregistercentralen

Befolkningsregistercentralen spärrar certifikat endast i följande fall:

- Befolkningsregistercentralen spärrar de certifikat som den beviljat om ett fel upptäcks i certifikatens datainnehåll.
- Befolkningsregistercentralen kan spärra certifikat som undertecknats med dess privata nyckel, om det finns anledning att misstänka att Befolkningsregistercentralens privata nycklar har röjts eller hamnat i fel händer.
- Samtliga gällande servercertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.
- Om den privata nyckeln eller annan teknisk metod som använts vid skapandet av Befolkningsregistercentralens certifikat har röjts eller på annat vis blivit oanvändbar ska Befolkningsregistercentralen meddela det inträffade till samtliga kortinnehavare och Kommunikationsverket på ändamålsenligt sätt.
- Befolkningsregistercentralen kan också spärra ett certifikat av ett annat särskilt skäl.



3.5.2018

VRK/TS/Keh

4.4.4 Tidpunkten för spärning

Certifikatet spärras omedelbart i samband med begäran om spärning. Spärrade tillfälliga certifikat kan inte tas i bruk igen.

4.4.5 Krav på avbrott av certifikatets giltighet

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.6 Person som gör begäran om avbrott

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.7 Begäran om avbrott

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.8 Begränsningar av avbrottstid

Giltigheten av tillfälliga certifikat kan inte avbrytas tillfälligt.

4.4.9 Publiceringsfrekvens för spärrlista

Uppgiften om införandet av certifikatet på spärrlistan är offentligt tillgänglig senast inom en timme efter att begäran om spärning har konstaterats vara behörig och godkänd. Spärrlistan är giltig i åtta timmar.

Spärrlistan innehåller tidpunkten för publicering av nästa spärrlista.

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

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

4.4.10 Krav på kontroll av spärrlista

Den förlitande partens skyldigheter har beskrivits i kapitel 2.1.4.

4.4.11 Kontroll av certifikatets status online

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

4.4.12 Krav på kontroll av certifikatets status online

Utfärdaren erbjuder en onlinekontrolltjänst för certifikatets status dvs. OCSP-tjänst.



3.5.2018

VRK/TS/Keh

4.4.13 Särskilda krav gällande avslöjande av certifikatinnehavarens privata nyckel

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

4.5 Övervakning av systemet

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

4.6 Arkivering av uppgifter om certifikat

4.6.1 Material som sparas

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas för en del dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i minst 5 år från tidpunkten då certifikaten upphört att gälla eller om det är fråga om ett tillfälligt certifikat som skapas för personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas.

Utfärdaren arkiverar följande uppgifter:

- a) Certifikatsökandens undertecknade ansökningsblankett, verifikat för mottagande av reservkortet och de allmänna användarvillkoren för certifikatet.
- b) Beviljade certifikat, deras datainnehåll och extra uppgifter med anknytning till hanteringen av deras livscykel från att certifikatets giltighetstid har löpt ut eller certifikatet har spärrats.
- c) Åtgärder med anknytning till skapande och förnyande av utfärdarens privata nyckel.
- d) Begäran om spärrning av certifikat.
- e) Spärrlistor sparade i det offentliga registret och övrig information om spärrningen av certifikat.
- f) Gällande certifikatpolicy och tidigare certifikatpolicy och motsvarande certifieringspraxis.



VRK/TS/Keh

3.5.2018

- g) Åtgärder utförda av användare som registrerats som administratörer för certifikatsystemet och användare av certifikatsystemet sparas loggfiler
- h) Granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditring av systemet.

Det arkiverade materialet förvaras enligt de bestämmelser som gäller myndigheten.

4.6.2 Skydd av arkiv

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

4.6.3 Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

4.6.4 Metoder för införskaffning och tryggnad av arkiverat material

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

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

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

4.7 Hantering av kontinuerlig verksamhet och undantagsfall

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

4.7.1 Utfärdarens privata nyckel har röjts eller Utfärdarens certifikat har spärrats

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

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

- a) Utfärdaren meddelar det inträffade till samtliga innehavare, förlitade parter och avtalskunder eller i övrigt har ett sådant förhållande till utfärdaren på grund av avtalsförhållande eller myndighetsverksamhet att utfärdaren måste informera om det inträffade.
- b) Utfärdaren skapar en ny nyckel i enlighet med kapitel 6.
- c) Samtliga gällande certifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.



VRK/TS/Keh

3.5.2018

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

4.7.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

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

4.8 Då utfärdarens verksamhet upphör

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

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

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

- a) Samtliga gällande certifikat spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.
- b) Utfärdaren upphäver samtliga avtalspartners befogenheter för att utföra åtgärder med anknytning till processen för beviljande av certifikat för utfärdarens del.
- c) Utfärdaren ser till att tillgången till utfärdarens arkiv enligt kapitel 4.6 bevaras även efter att utfärdarens verksamhet har upphört.
- d) Utfärdaren ansvarar för att uppgifterna enligt lagen om stark autentisering och betrodda elektroniska tjänster arkiveras samt följer också annars bestämmelserna i arkivlagen i fråga om arkivering av uppgifter eller om det är fråga om ett tillfälligt certifikat som skapas för personal inom social- och hälsovården eller aktörer inom social- och hälsovården ska även lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt bestämmelser som utfärdats med stöd av dessa och krav som ställts med stöd av dessa följas.



3.5.2018

VRK/TS/Keh

5 Krav på fysisk, funktionell och personalsäkerhet

Befolkningsregistercentralen har beviljats dataskyddscertifikat som säkerställer att BRC:s dataskydd uppfyller kraven i standarden ISO/IEC 27001.

Befolkningsregistercentralen anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. BRC svarar i egenskap av certifikatutfärdare för säkerheten inom certifikatproduktionen och själva produktionen på ett ändamålsenligt sätt inom samtliga delområden.

Befolkningsregistercentralen följer god informationshantering. Tjänster som anknyter till tillhandahållande av certifikat har organiserats till Befolkningsregistercentralens Certifikattjänstenhet.

5.1 Arrangemang kring fysisk säkerhet

5.1.1 Läge och lokalernas egenskaper

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

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

5.1.2 Fysisk tillgång till verksamhetslokalen

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

5.1.3 Elmatning och luftkonditionering

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

5.1.4 Brandsäkerhet

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

5.1.5 Förvaring av uppgifterna

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

Uppgifterna har skyddats mot försvinnande, ändring och olovlig användning.



3.5.2018

VRK/TS/Keh

5.1.6 Hantering av onödigt informationsmaterial

Säkerhetsklassificerat informationsmaterial kasseras på ett pålitligt sätt genom att förstöra.

5.1.7 Vattenskador

Maskinalarna har behöriga detektorer för fuktighet.

5.1.8 Reservarrangemang

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

Tillgången till reservdelar och service för viktig utrustning är säkrad.

5.2 Funktionella krav

5.2.1 Ansvarsfördelning

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

Utfärdarens uppgifter delas in i följande ansvarsområden:

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

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

5.2.2 Antal personer som behövs för uppgifterna

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

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

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



VRK/TS/Keh

3.5.2018

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

Registrering av tillfälliga certifikat fordrar närvaron av en person.

5.2.3 Uppgiftsspecifik autentisering

Registrerare av tillfälliga certifikat:

Registreraren identifieras med användarkod. Registreraren är den organisation med vilken Befolkningsregistercentralen har ingått ett avtal om registrering.

Administratör av certifikatsystemet:

Autentiseras med ett personligt kontrollkort för administration av systemet. Administratörer för systemet är certifikatsystemleverantörens systemexperter samt personer som befullmäktigats för uppdraget av Befolkningsregistercentralen.

Användare av certifikatsystemet:

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

5.3 Personlig säkerhet

Befolkningsregistercentralen fungerar som certifikatutfärdare och svarar för certifikatverksamheten. De tekniska leverantörerna har anlåtats genom upphandling och agerar för Befolkningsregistercentralens räkning och på Befolkningsregistercentralens ansvar.

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

5.3.1 Utförande av bakgrundskontroll av personalen

Befolkningsregistercentralen utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar med de tekniska leverantörernas certifikatdatasystem.

5.3.2 Förfarande vid utförande av bakgrundskontroll

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

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

- fylla i en blankett som lämnas in till skyddspolisen, som används för att utföra en säkerhetsutredning för personen
- avstå från uppgifter som strider mot deras skyldigheter och ansvarsområden



VRK/TS/Keh

3.5.2018

- vara personer som inte tidigare har avfärdats på grund av att de försummat eller misskött sina uppgifter
- ha lämplig utbildning för att utföra sina uppgifter.

5.3.3 Krav på utbildning

Personalen på Befolkningsregistercentralen ska ha sådan utbildning att de kan utföra sina uppgifter på bästa möjliga sätt. Vid Befolkningsregistercentralen finns en utbildningsplan. För förverkligandet av planen svarar Befolkningsregistercentralens administrativa enhet.

5.3.4 Underhåll av expertis och kompetens

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

5.3.5 Krav på uppgiftsrotation

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

Även inom arbetsrotationen efterlevs Befolkningsregistercentralens dataskyddspolicy och dataskyddsplan samt Befolkningsregistercentralens övriga allmänna anvisningar.

5.3.6 Åtgärder vid avvikelser

Befolkningsregistercentralens personal agerar i sitt uppdrag med ämbetsmannansvar och i enlighet med Befolkningsregistercentralens interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

5.3.7 Personal som representerar organisationen

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

5.3.8 Handlingar som tillhandahålls personalen

Personalen har alltid tillgång till Befolkningsregistercentralens kvalitets- och säkerhetsdokument.



3.5.2018

VRK/TS/Keh

6 Tekniska säkerhetsarrangemang

6.1 Skapande och sparande av nyckelpar

6.1.1 Skapande av nyckelpar

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

Certifikatutfärdare:

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

Innehavare av certifikat:

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

Utfärdaren skapar certifikatinnehavarens nycklar på ett säkert sätt.

6.1.2 Överlåtelse av en privat nyckel till certifikatinnehavaren

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

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

6.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren

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



3.5.2018

VRK/TS/Keh

6.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren

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

6.1.5 Nycklarnas längder

Utfärdarens privata nyckel som används för att signera organisationscertifikatet samt den motsvarande publika nyckeln är RSA-nycklar med storleken 4096 bitar.

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

6.1.6 Nycklarnas användningsändamål:

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

Certifikatutfärdarens certifikat:

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

Certifikatinnehavarens verifikations- och krypteringscertifikat

Ändamål: Verifikation av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signaturcertifikat

Ändamål: Elektronisk signatur.

6.2 Skydd av privat nyckel

6.2.1 Standarder som gäller den kryptografiska modulen

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

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

6.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel

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



3.5.2018

VRK/TS/Keh

6.2.3 Överlåtelse av en privat nyckel till förlitande part

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

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

6.2.4 Säkerhetskopia av en privat nyckel

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

6.2.5 Arkivering av en privat nyckel

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

6.2.6 Administration av en privat nyckel i kryptografiska moduler

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

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

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

6.3 Andra faktorer som anknyter till nyckeladministration

6.3.1 Arkivering av en publik nyckel

Utfärdaren arkiverar alla publika nycklar som den certifierat.

6.3.2 Användningstid för publika och privata nycklar

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



3.5.2018

VRK/TS/Keh

6.4 Aktiveringsuppgift

6.4.1 Skapande och ibrukttagande av aktiveringsuppgift

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

6.4.2 Skydd av aktiveringsuppgift

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

6.4.3 Andra faktorer som anknyter till aktiveringsuppgiften

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

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

6.5 Säkerhetskrav som gäller användning av datorer och tillgång till dessa

6.5.1 Utrustningssäkerhet

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

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

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

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

Certifikatsystemets utrustning övervakas dygnet runt.

6.6 Livscykeladministration av certifikatsystemet

Befolkningsregistercentralen upprätthåller en klassificering av mål och system för certifikattjänsterna, deras trygghet, prioritering och minimiunderhåll.



3.5.2018

VRK/TS/Keh

6.6.1 Övervakning som gäller systemutvecklingen

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

6.6.2 Hantering av säkerhet

Befolkningsregistercentralens datasäkerhet administreras i enlighet med Befolkningsregistercentralens dataskyddspolicy och standarden ISO/IEC 27001.

6.7 Datanätets säkerhet

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

6.8 Övervakning av användning av kryptografisk modul

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

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

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

7 Profiler för certifikat och spärrlistor

7.1 Tekniska uppgifter om certifikat

Datainnehållen i rotcertifikatet, utfärdarens certifikat och certifikatinnehavarens certifikat har beskrivits i dokument FINEID S2. Dokumentet finns tillgängligt på utfärdarens webbplats, www.fineid.fi.

7.2 Profil för spärrlistor

Datainnehållen i spärrlistor som utfärdaren publicerats har beskrivits i dokument FINEID S2. Dokumentet finns tillgängligt på utfärdarens webbplats, www.fineid.fi.



3.5.2018

VRK/TS/Keh

8 Hantering av dokument innehållande bestämmelser

8.1 Ändring av bestämmelser

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

8.2 Publicering och information

Utfärdaren publicerar certifikatpolicy- och certifieringspraxisen, som är tillgängliga på adresserna www.vaestorekisterikeskus.fi och www.fineid.fi.

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

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

8.3 Förfarande för ändring och godkännande av certifikatpolicy

Befolkningsregistercentralen godkänner såväl certifikatpolicy- som certifieringspraxisen för det tillfälliga certifikatet. Handlingarna kan ändras med Befolkningsregistercentralens interna ändringsförfarande.

Befolkningsregistercentralen informerar om ändringar i god tid innan de träder i kraft på sin egen webbplats.

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

1. Samtliga punkter i certifikatpolicy- och certifieringspraxisen kan ändras genom att anmäla kommande väsentliga ändringar 30 dagar innan de träder i kraft.
2. Punkter som inte enligt Befolkningsregistercentralen märkbart påverkar certifikatinnehavare och förlitande parter kan ändras genom att meddela om ändringarna 14 dagar innan de träder i kraft.