CERTIFIKATPOLICY

för Befolkningsregistercentralens servicecertifikat
OID: 1.2.246.517.1.10.205

Väestörekisterikeskus

VRK/TS/Keh

03-05-2018

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

VRK/TS/Keh

03-05-2018

Innehållsförteckning

VRK/TS/Keh 03-05-2018

CERTIFIKATPOLICY

1 Allmänt

I detta dokument definieras Befolkningsregistercentralens – här efter certifikatutfärdaren (Certification Authority) – förutsättningar för certifieringsfunktioner enligt öppet nyckelsystem (Public Key Infrastructure; PKI) samt tillämpningsområde och begränsningar för detta dokument. Principerna i detta dokument fastställs på praktisk nivå i certifieringsfunktionerna och i de övriga anvisningarna för förfaringssätt som kompletterar denna certifikatpolicy. I detta dokument iakttas ETSI TS 102 042 v 2.4.1:s (OVCP) riktlinjer för servicecertifikat.

2 Referensförteckning

2.1 Riktgivande referenser

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

[1] Lag om stark autentisering och betrodda elektroniska tjänster (617/2009)

[2] Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)

[3] Lag om offentlighet i myndigheternas verksamhet (621/1999)

[4] IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)

[5] ETSI TS 102 042 V2.1.2: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (2010-04)

[6] Kommunikationsverket M 72/2016

[7] VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen

[8] ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

Vid tolkningen av dokumentet iakttas följande principer:

1. Rubriker och underrubriker i certifieringspraxisen är i huvudsak översättningar av rekommendationer i internationella standarder [RFC 3647]. Vid tolkning av dokumentet ska själva texten prioriteras framför rubrikerna.

2. Ett allmänt villkor är att certifikatutfärdaren ska uppfylla alla de krav i certifieringspraxisen som gäller utfärdare.

2.2 Informativa referenser

De dokument som nämns här näst är inte oumbärliga för användningen av detta dokument, men de kan underlätta för användaren inom vissa ämnesområden. Om referensen inte är specifik tillämpas den senaste versionen av dokumentet (inklusive revisioner).

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.

3 Definitioner och förkortningar

3.1 Definitioner

Attributdata: permanenta uppgifter som fordras för autentisering av yrkesutbildade personer och konstaterande av yrkesrättigheter.

Nyckelpar: Nycklar som används tillsammans inom ett öppet nyckelsystem, varav den ena är publik och den andra privat. Nycklarnas användningssyfte är fastställt i certifikatet. OBS! Se kapitel 4.3

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.

Registertjänst: En offentlig webbtjänst som innehåller samtliga certifikat beviljade av utfärdaren samt utfärdarens certifikat och spärrlistor.

Servercertifikat för hälsoapplikationer: Servercertifikat för social- och hälsovården, som beviljas för att skydda meddelandetrafik i hälsoapplikationer. Det handlar till exempel om mobilapplikationer med vilka användarna samlar in uppgifter om en persons hälsa och förmedlar dem vidare till FPA:s Mina Kanta.

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

Öppet nyckelsystem: Dataskyddsinfrastruktur där dataskyddstjänster produceras med ett öppet nyckelsystem.

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

Förlitande part: Den part som litar på uppgifterna i certifikatet och använder certifikatet för olika dataskyddstjänster, såsom elektronisk autentisering av certifikatets innehavare och konstaterande av digital signatur. OBS! Se RFC 3647.

OCSP-tjänst: Online Certificate Status Protocol. Tjänst där man kan kontrollera certifikatets status i realtid.

Servercertifikat: Servercertifikat, som används för att identifiera servern och skapa en SSL-/TLS-krypterad datatrafikförbindelse mellan servrar. Exempelvis ett certifikat skapat för www-server, som användaren kan använda för att försäkra sig om att servern är pålitlig. En datahelhet som utgörs av serviceproducentens publika nyckel inom ett öppet nyckelsystem och identifieringsuppgifter, som certifikatutfärdaren har skapat och signerat med sin privata nyckel.

Servercertifikat för kommunikation: Filbaserat certifikat för användning exempelvis för mottagning och sändning av krypterade meddelanden med en gemensam e-postadress. Filen innehåller såväl certifikat som deras privata och publika nycklar.

Servicecertifikat: Ett gemensamt namn för server- och e-postservercertifikat samt servercertifikat för hälsoapplikationer.

Registrerare: Registreraren identifierar i enlighet med den certifikatsökandes certifikatpolicy och certifieringspraxis för utfärdarens del och på dennes ansvar.

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

Skyddad användarutrustning: utrustning som förvarar användarnas privata nyckel, skyddar denna nyckel och utför signering eller dekrypteringsfunktioner för användarens del.

Spärrlista (CRL): 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. OBS! Se ITU-T Rekommendation X.509.

Spärrtjänst: Utfärdarens tjänst, där utfärdaren tar emot begäranden om att spärra certifikat, spärrar certifikat och förmedlar information om att ett certifikat spärrats till certifikatsystemet.

Digital signatur: en PKI-signatur i samband med ett elektroniskt meddelande, som kan användas för stark autentisering av meddelandets innehåll och signerarens identitet.

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

Certifikatsystem: Ett datatekniskt system för att skapa certifikat, underteckna spärrlistor och publicera dem i registret.

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 certifikatpolicyer är offentligt tillgängliga. Varje policy identifieras av en egen kod.

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

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

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

Certifikatutfärdare: Organisationen som beviljar certifikat, som svarar för produktionen av certifikat samt utarbetar certifikatpolicy och certifieringspraxis som beskriver organisationens verksamhet. OBS! Se kapitel 4.1

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

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

Certifikatsökande: Organisation eller privatperson som ansöker om certifikat och pålitligt identifieras i samband med detta.

Innehavare av certifikat: En organisation eller privatperson vars data och publika nyckel har bekräftats med utfärdarens elektroniska signatur och som innehar den privata nyckeln för certifikatet.

Användning och användningssyfte för certifikat: I detta dokument avses med användning av certifikat såväl användning av själva certifikatet som användning av medföljande nycklar. Exempelvis avses med användning av certifikat vid digital signering såväl användning av den privata nyckeln vid signeringen som användning av den publika nyckeln och certifikatet vid autentisering av signatur.

Privat nyckel: Den privata delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatinnehavarens privata nyckel sparas i en trygg miljö för att skydda denna från otillbörlig användning.

3.2 Förkortningar

CA Certification Authority, certifikatutfärdare

CP Certificate Policy, certifieringspolicy

CPS Certification Practise Statement, certifieringspraxis

CRL Certificate Revocation List, spärrlista

CSP Certification Service Provider, certifikatutfärdare

EVC Extended Validity Certificate

EVCP Extended Validity Certificate Policy

FINEID Finnish Electronic Identification, finländskt elektroniskt identifieringssystem

HSM Hardware Security Module, kryptografisk modul

HTTP Hypertext Transfer Protocol

ISO 27001, ISO/IEC 27001

LDAP Lightweight Directory Access Protocol

OID Object Identifier, identifierande kod

OVCP Organizational Validation Certificates Policy

PDS PKI Disclosure Statement, certifikatbeskrivning

PKI Public Key Infrastructure, öppet nyckelsystem

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

SSL Secure Socket Layer

TLS Transport Layer Security

BRC Befolkningsregistercentralen

4 Allmänna begrepp

4.1 Certifikatutfärdare

Utfärdaren är den instans som beviljar och skapar certifikat som användarna av certifikattjänster (dvs. beställarna och de förlitande parterna) litar på. Utfärdaren bär helhetsansvaret för att erbjuda de certifikattjänster som fastställs i punkt 4.2. Utfärdaren är specificerad i certifikatet som beviljare av certifikatet, och kvalificerade certifikat signeras med utfärdarens privata nyckel.

Utfärdaren kan anlita övriga partner inom sina certifikattjänster, som erbjuder delar av tjänsten. Utfärdaren innehar alltid helhetsansvaret och säkerställer att de förfaringssätt som fastställs i detta dokument förverkligas. Utfärdaren kan exempelvis införskaffa samtliga deltjänster av underleverantörer, även tjänster för skapande av certifikat. Nyckeln som används för att signera certifikaten innehas dock av utfärdaren och utfärdaren har helhetsansvaret för att de krav som fastställs i detta dokument uppfylls och för de certifikat som utfärdas för allmänheten.

Utfärdaren beviljar certifikat och uppfyller följande villkor:

- Utfärdaren förbinder sig att iaktta villkoren i certifikatpolicyn.
- Utfärdaren utarbetar certifieringspraxis och övriga förfaringssätt som kompletterar certifikatpolicyn.
- Certifikatutfärdaren ska ha tillräcklig ekonomisk beredskap för att trygga den verksamhet som anges i certifikatpolicyn och certifieringspraxisen. Utfärdaren svarar för certifikatverksamheten och anknytande risker och utgår

från att leverantörerna inom certifikatsystemet garderar sig mot risker i verksamheten med hjälp av lämpliga metoder för riskhantering.

- Certifikatutfärdaren för register över registrerare som är godkända av utfärdaren.
- Utfärdaren beslutar om korscertifiering i samråd med övriga utfärdare.
- Certifikatutfärdaren svarar för livscykeln hos nyckelpar som är genererade av utfärdaren (generering, lagring, säkerhetskopiering, publicering och återkallande).

Certifikatutfärdaren förbinder sig att:

1. tillhandahålla de certifikat-, register- och spärrtjänster som fastställs i certifikatpolicyn;
2. tillhandahålla de hanterings- och uppföljningsfunktioner som beskrivs i kapitel 4 till 6 i denna certifikatpolicy;
3. pålitligt identifiera certifikatsökande;
4. bevilja certifikat i enlighet med denna certifikatpolicy;
5. efterleva gällande lagar och förordningar och bestämmelser och riktlinjer enligt dessa samt främja rättigheterna för användare av certifikat och förlitande parter;
6. se till att tillräckliga och oberoende kontroller i enlighet med certifikatpolicyn utförs;
7. svara för att certifikatutfärdarens verksamhet fungerar; och
8. iaktta alla villkor i certifikatpolicyn och certifieringspraxisen.

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

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

4.2 Certifikattjänster

4.2.1 Registrerare

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

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

att man kan lita på den personal man befullmäktigat. Utfärdaren godkänner personalen vid registreringsinstansen utgående från registrerarens utredningar.

Registrerare ska enligt certifikatpolicyn förbinda sig till att:

1. efterleva gällande lagstiftning samt bestämmelser och riktlinjer enligt denna;
2. erbjuda hanterings- och uppföljningsfunktioner enligt vad som fordras i kapitel 4 till 6 i denna certifikatpolicy;
3. utföra identifieringsförfarande för certifikatsökandet enligt kapitel 4 till 6 i denna certifikatpolicy samt enligt certifieringspraxis och lämna uppgifterna om certifikatsökanden till utfärdaren för skapande av certifikat;
4. fullfölja avtalade uppdrag och stödja certifikatanvändares och förlitande parters rättigheter; och
5. iaktta alla de villkor i denna certifikatpolicy och certifieringspraxisen som gäller registreringstjänsten.

Registreraren kan erbjuda extra funktioner eller tjänster som har godkänts av certifikatutfärdaren. Registreraren svarar för alla registreringstjänster som tillhandahålls av registreraren. Registrerare för servicecertifikatet är Befolkningsregistercentralen.

4.2.2 Spärrtjänst

Utfärdarens spärrtjänst spärrar servicecertifikat på innehavarens eller utfärdarens önskemål innan certifikatets giltighetstid har löpt ut. Spärrade servicecertifikat förs in på spärrlistan. Orsaken till spärrning av servicecertifikat kan exempelvis vara att innehavarens privata nyckel har röjts eller att det finns misstanke om detta.

4.2.3 Registertjänst

Registertjänsten är en offentlig webbtjänst som innehåller samtliga certifikat beviljade av utfärdaren samt utfärdarens certifikat och spärrlistor. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

4.3 Certifikatpolicy och certifieringspraxis

4.3.1 Syfte

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

4.3.2 Detaljer

I verksamhetspraxis beskrivs mer ingående än i certifikatpolicyn åtgärder som utfärdaren utför vid beviljande av certifikat och inom den övriga förvaltningen. Här fastställs hur en viss utfärdare uppfyller de tekniska kraven i certifikatpolicyn samt kraven på organisationen och förfaranden.

4.3.3 Approach

Certifikatpolicy och certifieringspraxis skiljer sig i hög grad i sin approach. Certifikatpolicyn utarbetas oberoende av detaljerna i en viss utfärdares verksamhetsmiljö. Certifieringspraxisen utarbetas för sin del i enlighet med en viss utfärdares organisationsstruktur, förfaringssätt, verksamhetslokaler och datatekniska miljö. Certifikatpolicyn kan fastslås av användaren av certifikattjänster, men certifieringspraxisen fastställs alltid av leverantören av certifikat.

4.3.4 Övriga dokument som publiceras av utfärdaren

Utöver certifikatpolicyn och certifieringspraxisen kan utfärdaren även publicera övriga dokument som gäller utfärdarens verksamhet. Dessa användarvillkor kan innehålla kommersiella villkor av olika slag eller gälla exempelvis ett visst öppet nyckelsystem. Även om man inte nödvändigtvis informerar kunden om dessa villkor, kan de ändå tillämpas.

Certifikatbeskrivningen är en del av utfärdarens användarvillkor, som gäller verksamheten i ett öppet nyckelsystem. Utfärdaren bör göra certifikatbeskrivningen tillgänglig för såväl beställarna som de förlitande parterna.

4.4 Beställare och signerare

Med "Beställare" avses den instans som ansöker om certifikat av utfärdaren och har ett avtalsförhållande med utfärdaren (organisation eller privatperson). Med "Signerare" avses den instans som beviljats certifikatet (organisation eller privatperson). Beställaren bär ansvar för användningen av den privata nyckeln i anslutning till certifikat med publik nyckel. Signeraren är den person som kan identifieras med den privata nyckeln och som använder den privata nyckeln.

Då certifikat beviljas privatpersoner för deras egen användning kan samma instans vara såväl beställare som signerare. I övriga fall, exempelvis då certifikat beviljas till anställda, är beställaren och signeraren olika instanser. Exempelvis kan en arbetsgivare vara beställare och en anställd signerare.

I detta dokument används dessa två termer för att åskådliggöra skillnaden vid behov. I samtliga fall är skillnaden i fråga dock inte tydlig.

5 Inledning om certifikatpolicydokument

5.1 Allmänt

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

Certifieringspraxis tillämpas på Befolkningsregistercentralens servicecertifikat. Servicecertifikat är ett certifikat som beviljas av Befolkningsregistercentralen och som används för att autentisera serviceleverantörens – organisationens eller privatpersonens – service eller tjänst.

Ett certifikat är en uppsättning data som kopplar samman identifikationsuppgifter i samband med autentisering eller kryptering med innehavaren av certifikatet och autentiserar innehavaren

av servicecertifikatet. Certifikatets uppgifter har signeras digitalt med certifikatutfärdarens privata nyckel. Certifikat enligt denna certifieringspraxis utgår från öppet nyckelsystem (PKI).

Servicecertifikaten kan användas för identifiering av såväl den offentliga förvaltningens som den privata sektorns tjänster. Med hjälp av servicecertifikatet kan den som utnyttjar tjänsten försäkra sig om att tjänsteleverantören är pålitlig.

Befolkningsregistercentralens certifieringspraxis har en egen unik kod (OID). I utfärdarens funktioner ingår produktion av certifikat-, register- och spärrtjänster samt registrering, Dessa funktioner beskrivs närmare i kapitel 4.2.

5.2 Individuella koder

I certifikatet ingår två individuella koder (OID). Den ena koden beskriver vilken ETSI TS 102 042 certifikatpolicy som iakttas för certifikatet och den andra är den individuella koden för certifieringspraxisen.

Dessutom har certifikatpolicyn en egen individuell BRC-kod, som fastställer certifikatpolicyn.

Individuella koder är:

OID för den ETSI TS 102 042-policy som ska iakttas (OVCP): 0.4.0.2042.1.3 [itu-t(0), identified-organization(4), etsi(0), other-certificate-policies(2042), policy-identifiers(1), ovcp (7)]

BRC:s OID för certifieringspraxis fastslås i certifieringspraxis.

OID för certifikatpolicyn för BRC:s servicecertifikat: 1.2.246.517.1.10.205.

Certifikatpolicyn, dess certifikatbeskrivning och certifieringspraxis finns på adressen http://www.fineid.fi/.

5.3 Användarsamfund och tillämpningsbarhet

Användningssyftet för servicecertifikat enligt denna certifikatpolicy beskrivs i certifieringspraxis. Certifikatet kan användas i enlighet med användningssyftet utan begränsningar inom förvaltningen samt i applikationer och tjänster som erbjuds av privatpersoner.

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.

5.4 Överensstämmelse med krav

5.4.1 Allmänt

Utfärdaren producerar certifikattjänster enligt villkoren i certifikatpolicyn och ansvarar för att de fungerar i innehavarens användning. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifikatpolicy är registrerad av Befolkningsregistercentralen. Certifikatpolicydokumenten publiceras på adres-

sen www.fineid.fi där de är tillgängliga för allmänheten. Utfärdarens verksamhet auditeras årligen samt vid större förändringar i systemet. En certifikatauditeringsrapport är tillgänglig på begäran.

Dataskyddsgranskning

Befolkningsregistercentralen utför en dataskyddsgranskning för de tekniska leverantörernas lokaler, utrustning och verksamhet på ett ändamålsenligt sätt.

Befolkningsregistercentralens dataskyddsgranskning utförs av en utomstående inspektör som är oberoende av utfärdaren.

Målen för granskningen fastställs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller, om Befolkningsregistercentralen utför granskningen, i enlighet med informationssäkerhetsstandarden ISO 27001, Befolkningsregistercentralens informationssäkerhetspolicy eller tekniska leveransavtal. Dataskyddsegenskaper som kontrolleras är bl.a. konfidentialitet, integritet och användbarhet.

Vid granskningen kontrolleras överensstämmelsen hos certifikatpolicyn, certifieringspraxis och anvisningar för tillämpning med ETSI TS 102 042-standarden inom hela certifikatorganisationen och certifikatsystemet.

Åtgärder vid avvikelser

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

Information om resultatet av granskningen

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

Arkivering av granskningsmaterial

Utfärdaren arkiverar granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet. Det arkiverade materialet förvaras enligt bestämmelserna för myndigheter som fungerar som utfärdare.

Planer och policy för utfärdarens verksamhet samt utfärdarens skyldigheter vid undantagsfall eller störningar beskrivs i punkt 7.4.8. Hantering av kontinuerlig verksamhet och undantagsfall

5.4.2 Krav på överensstämmelse med krav

Utfärdarens skyldigheter beskrivs i punkt 6.1. Utfärdarens verksamhet uppfyller kraven i punkt 6.1 Dessutom uppfyller utfärdarens verksamhet och tillsynen av verksamheten de krav som specificeras i punkt 7.

6 Skyldigheter, ansvar och ansvarsbegränsningar

6.1 Certifikatutfärdarens skyldigheter

Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar.

- Befolkningsregistercentralen har ett lagstadgat uppdrag att fungera som certifikatutfärdare.
- Utfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt hantera eventuella krav på skadeersättning.
- Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer och personer som man anlitar.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning för beviljande av servicecertifikat samt övriga aspekter av användningen av servicecertifikatet på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren uppfyller kraven enligt certifikatpolicyn och certifieringspraxisen.
- Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen och gör dem allmänt tillgängliga.
- Utfärdaren anställer tillräckligt med personal med den expertis, erfarenhet och kompetens som fordras för produktionen av certifikattjänster.
- Utfärdaren använder pålitliga system och produkter som är skyddade från otillbörlig användning.
- Utfärdaren tillhandahåller offentligt information om certifikat och certifikatverksamheten, utgående från vilken utfärdarens verksamhet och pålitlighet kan bedömas.

Registrerarens skyldigheter

Registrerare för servicecertifikatet är Befolkningsregistercentralen.

- Registreraren efterlever certifikatpolicyn och certifieringspraxisen i samband med registreringen.

- Registreraren identifierar servicecertifikatsökanden med stark autentisering på det sätt som beskrivs i certifieringspraxisen, på så sätt att sökandens identitet, rätt att ansöka om servicecertifikat samt övriga uppgifter som fordras för beviljande av servicecertifikat noga kontrolleras.
- Registreraren ser till att uppgifterna hanteras omsorgsfullt och konfidentiellt.
- Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med utfärdaren.

6.2 Certifikatbeställarens och certifikatinnehavarens skyldigheter

- Innehavaren av servicecertifikatet ansvarar för att certifikatet används i de användningssyften som anges i ansökan om servicecertifikat samt i enlighet med certifikatpolicyn, certifieringspraxisen och de bindande avtalsvillkoren för certifikatinnehavare.
- Befolkningsregistercentralen kan även bevilja servicecertifikatet för egna syften. Då efterföljer den samma krav som de övriga organisationerna.
- Certifikatinnehavaren (serviceleverantören) ansvarar för att de uppgifter som uppges då man ansöker om certifikatet är riktiga.
- Certifikatinnehavaren ska förvara sin privata nyckel i en trygg miljö och sträva efter att förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.
- Certifikatinnehavaren ska omedelbart informera utfärdaren om man känner till eller misstänker att certifikatinnehavarens privata nyckel har röjts eller att certifikatets informationsinnehåll är felaktigt. I detta fall spärrar utfärdaren certifikatet i fråga och samma privata nyckel kan inte användas för att skapa ett nytt certifikat.
- Certifikatinnehavarens ansvarar för användningen av ett certifikat upphör när innehavaren har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Samtliga gällande servicecertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade servicecertifikatets 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 innehavare av certifikat och Kommunikationsverket på ändamålsenligt sätt.

Den som ansöker om servicecertifikat lämnar in en certifikatbegäran som skapats på den service man vill certifiera till registreraren, utgående från vilken servicecertifikatet skapas.

Utfärdarens privata nyckel som använts för signering av servicecertifikatet och den motsvarande publika nyckeln är 4 096-bitars RSA-nycklar.

Längden för den privata och publika nyckeln i servicecertifikatet fastställs av certifikatsökanden. Nyckellängden för servicecertifikat som beviljas av Befolkningsregistercentralen är minst 2 048 bitar.

6.3 Den förlitande partens skyldigheter

Den part som litar på servicecertifikatet är skyldig att säkerställa att certifikatet används enligt användningssyftet.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan i god tro lita på servicecertifikatet efter att parten kontrollerat att certifikatet är i kraft och inte finns på spärrlistan. Förlitande parter svarar för kontrollen av gällande spärrlistor. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat de spärrade certifikaten på det sätt som beskrivs nedan.

Förlitande parter som hämtar spärrlistan i registret ska kontrollera spärrlistans integritet och autenticitet med stöd av utfärdarens digitala 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 certifikat enligt denna certifieringspraxis inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Om en förlitande part ändå godkänner ett certifikat, sker det på den förlitande partens eget ansvar.

6.4 Ansvar och ansvarsbegränsningar

Certifikatutfärdarens ansvar

Befolkningsregistercentralen efterlever i sin servicecertifikatverksamhet den gällande lagstiftningen i Finland.

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 servicecertifikaten har skapats enligt de förfaranden som beskrivs i certifikatpolicyn och certifieringspraxisen och utgående från de uppgifter som certifikatsökanden lämnat. Befolkningsregistercentralen ansvarar endast för den information som man sparat i servicecertifikatet.

Befolkningsregistercentralens skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande samarbetsavtal och skadeståndslagen (412/1974) . Befolkningsregistercentralen omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Befolkningsregistercentralen svarar för att servicecertifikatet är tillgängligt för användning från att det överlåts under hela dess giltighetstid, förutsatt att certifikatet inte spärras.

Befolkningsregistercentralen svarar för att servicecertifikatet har överlåtits till en certifikatsökande, som autentiserats på det sätt som förutsätts för servicecertifikat.

Vid signering av servicecertifikatet med sin privata nyckel intygar certifikatutfärdaren att utfärdaren har kontrollerat uppgifterna i certifikatet med de metoder som beskrivs i servicecertifikatpolicyn och certifieringspraxisen.

Utfärdaren ansvarar för att rätt servicecertifikat förs in på spärrlistan och att det förs in på spärrlistan inom den tid som fastställs i certifieringspraxisen.

Registrerarens ansvar

Registrerare för servicecertifikatet är Befolkningsregistercentralen eller dess avtalspartner för Befolkningsregistercentralens räkning och på dess ansvar.

Certifikatinnehavarens ansvar

Innehavaren av servicecertifikatet ansvarar för att certifikatet används i de användningssyften som anges i ansökan om servicecertifikat.

Certifikatinnehavarens ansvarar för användningen av ett certifikat upphör när innehavaren har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Den förlitande partens ansvar

Den part som litar på servicecertifikatet kan inte uppriktigt lita på certifikatet om den förlitande parten inte kontrollerat certifikatets giltighet på spärrlistan. Om servicecertifikatet trots allt godkänns frias Befolkningsregistercentralen från ansvar. Den part som litar på servicecertifikatet ska kontrollera att det beviljade certifikatet motsvarar användningssyftet i det funktioner det används för.

Begränsning av ansvar

Befolkningsregistercentralen svarar inte för eventuella skador eller kostnader som orsakas av att certifikatinnehavarens privata nycklar 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 certifikatfaktureringen 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 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.

Certifikatutfärdaren har rätt att avbryta tjänsten för den tid ändringar eller underhåll av systemet utförs. Om ändringar eller underhåll av spärrlistan meddelas på förhand.

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

Certifikatinnehavarens ansvar för användningen av ett certifikat upphör när innehavaren eller en representant för certifikatinnehavarens organisation har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

7 . Krav på certifikatutfärdarens verksamhet

Utfärdaren ska utföra följande administrativa åtgärder som uppfyller kraven.

I dessa ingår att erbjuda registreringstjänster, skapa certifikat, distribuera certifikat, spärra certifikat och informera om spärrning (se punkt 4.2). Om kravet anknyter till ett visst serviceområde hos utfärdaren presenteras det under motsvarande underrubriker. Om inget serviceområde specificeras eller om man nämner "utfärdaren i allmänhet", gäller kravet utfärdarens allmänna verksamhet.

Syftet med dessa krav på förfaranden är inte att begränsa certifikatutfärdarens möjligheter att ta betalt för sina tjänster.

Kraven som presenteras gäller säkerhetsmål och administrativa åtgärder som vidtas för att uppnå dessa, för vars del specifika krav ställs, om det anses vara nödvändigt för att uppnå målen.

7.1 Certifieringspraxis

Utfärdaren utarbetar certifieringspraxis och övriga förfaringssätt som kompletterar certifikatpolicyn. Utfärdaren svarar för att certifieringspolicyn, certifieringspraxisen och certifieringsbeskrivningar är offentligt tillgängliga på adressen www.fineid.fi.

Rättigheterna och skyldigheterna för servicecertifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

I ansökningsdokumentet och användarvillkoren nämns tydligt att certifikatsökanden intygar riktigheten hos uppgifterna med sin signatur då certifikatet skapas och att det publiceras i det offentliga registret. Samtidigt godkänner certifikatsökanden reglerna och villkoren för användning av servicecertifikatet samt skyldigheten att anmäla eventuellt missbruk eller röjning av den privata nyckeln.

Utfärdaren fastställer och godkänner certifieringspraxisdokumenten.

Utfärdaren svarar för att dess certifieringsverksamhet och certifieringspraxis iakttar certifikatpolicyn.

Certifikatutfärdarens verksamhet granskas minst en gång om året. Vid granskningen jämförs certifikatpolicyn och certifieringspraxisen med utfärdarens verksamhet som helhet. Utfärdaren vidtar utan fördröjning korrigerande åtgärder vid upptäckta avvikelser.

Algoritmer och övriga tekniska detaljer som används i certifikatverksamheten och certifikaten finns beskrivna i kapitel 7.2.

7.2 Hantering av livscykeln för nycklarna inom ett öppet nyckelsystem

7.2.1 Skapande av certifikatutfärdarens nyckel

Utfärdaren skapar privata nycklar för signering och publika nycklar som motsvarar de privata nycklarna för signering. 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.

Nycklarna förvaras i kryptografiska moduler som administreras av utfärdaren. De överensstämmer till sin säkerhetsnivå med nivå 3 i FIPS 140-1.

Utfärdarens privata nyckel som använts för signering av servicecertifikatet och den motsvarande publika nyckeln är 4 096-bitars RSA-nycklar.

Längden för den privata och publika nyckeln i servicecertifikatet fastställs av certifikatsökanden. Nyckellängden för Befolkningsregistercentralens servicecertifikat är minst 2 048 bitar.

Utfärdaren skapar ett nytt nyckelpar och utfärdarens certifikat senast fem år och tre månader innan det föregående certifikatets giltighetstid löper ut. Utfärdarens certifikat förs in i det offentliga registret enligt kapitel 7.3.5.

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

7.2.2 Lagring, säkerhetskopiering och returnering av utfärdarens privata nyckel

Utfärdarens privata nycklar är skyddade mot röjning och missbruk.

Nycklarna förvaras i kryptografiska moduler som administreras av utfärdaren. De överensstämmer till sin säkerhetsnivå med nivå 3 i FIPS 140-1.

Det görs en säkerhetskopia på certifikatutfärdarens privata nyckel.

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

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

7.2.3 Distribution av utfärdarens publika nyckel

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren. Utfärdaren publicerar sin publika nyckel i ett offentligt register på adressen ldap://ldap.fineid.fi och på webbplatsen http://www.fineid.fi.

7.2.4 System för reservnyckel

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

7.2.5 Användning av certifikatutfärdarens nyckel

Fältet som fastställer användningssyftet i certifikatets datainnehåll anger användningssyftet för nyckeln kopplad till certifikaten.

Med utfärdarens certifikat signeras endast servicecertifikat och relaterade spärrlistor. Den tekniska beskrivningen finns i FINEID S 2-bestämmelsen.

Då giltighetstiden för utfärdarens certifikat upphör förstörs certifikatutfärdarens privata nycklar i den kryptografiska modulen och används inte igen.

Utfärdarens privata nycklar förvaras i kryptografiska moduler.

Aktivering av utfärdarens privata nycklar utförs av för uppdraget befullmäktigade personer med kontrollkort i de kryptografiska modulerna. Användningen av certifikatutfärdarens privata nycklar kan förhindras av personer som är behöriga för uppgiften med hjälp av kontrollkort eller genom bortkoppling av strömmen till den kryptografiska modul som innehåller utfärdarens privata nycklar.

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

Utfärdarens privata nycklar förstörs efter att deras giltighetstid har upphört. Bara certifikatutfärdaren kan förstöra utfärdarens privata nycklar. När certifikatutfärdarens verksamhet upphör, ska utfärdarens privata nycklar och kopiorna av dem förstöras.

Utfärdaren skapar vid behov ett nyckelpar för certifikatinnehavaren. I detta fall levereras certifikatet och dess nyckelpar och lösenord till certifikatinnehavaren på så vis att det inte är möjligt för utomstående att komma åt dem.

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

7.3 Hantering av livscykeln för certifikat inom ett öppet nyckelsystem

7.3.1 Registrering av signerare

Utfärdaren ska säkerställa att signerarna identifieras och autentiseras på ändamålsenligt sätt och att signerarens begäranden om certifikat är kompletta, riktiga och ändamålsenligt befullmäktigade.

Vid namngivningen av innehavaren av servicecertifikatet används offentliga namnuppgifter och övriga uppgifter som uppgetts av certifikatsökanden och kontrollerats av registreraren.

Gruppen av attribut som bildar objektets namnpost i certifikatet är unik och individualiserar innehavaren av certifikatet i fråga. Alla innehavarorganisationer av servicecertifikat ska agera under eget namn.

Certifikatinnehavarens privata nycklar skapas i certifikatutfärdarens service eller dennes tekniska leverantörs service, då det gäller service- eller systemsigneringscertifikat. Då det gäller e-postservicecertifikat skapar utfärdaren nyckelparet och certifikatet och levererar dem till certifikatinnehavaren.

Autentisering av organisation som företräder certifikatsökanden

Rättigheterna och skyldigheterna för servicecertifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

I ansökningsdokumentet och användarvillkoren nämns tydligt att certifikatsökanden intygar riktigheten hos uppgifter med sin signatur då certifikatet skapas och eventuellt publiceras i det offentliga registret. Samtidigt godkänner certifikatsökanden reglerna och villkoren för användning av servicecertifikatet samt skyldigheten att anmäla eventuellt missbruk eller röjning av den privata nyckeln.

Utfärdaren och registreraren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheter för samtliga parter.

Sökanden av servicecertifikat svarar för att samtliga uppgifter som är väsentliga för certifikatet och sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren ska använda servicecertifikatet endast i enlighet med dess användningssyfte.

Då utfärdaren beviljar servicecertifikatet godkänner utfärdaren samtidigt certifikatansökan.

Certifikatinnehavaren ska omedelbart anmäla servicecertifikatet till spärrlistan om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

Man ansöker om servicecertifikat med en blankett som kan laddas ner och skrivas ut på webbplatsen http://www.fineid.fi.

Innan certifikatet beviljas ska utfärdaren kontrollera certifikatsökandens uppgifter bl.a. i Patent- och registerstyrelsens onlinetjänst, Virre-registret. Befolkningsregistercentralen utför i samband med detta en kontroll som sker med e-postmeddelande med anknytning till kontrollen av domännamnet. I samband med ansökan lämnas en fullmakt in om certifikatsökanden (ADB-kontaktperson etc.) agerar för ett företags eller en organisations räkning. Statens, kommunernas och församlingarnas myndigheter kontrolleras inte i Virre-registret. Sökandens domännamn som slutar på .fi och information om hur de administreras ska vara tillgänglig för BRC då ansökan behandlas. Övriga domännamn kontrolleras i tillgängliga webbtjänster eller på övrigt pålitligt sätt. Befolkningsregistercentralen beviljar endast servicecertifikat för IP-adresser eller domäner som används i offentligrättsligt syfte.

Vid ansökan om certifikat för privatperson lämnar sökanden personligen ansökan om servicecertifikat till utfärdaren, som kontrollerar identiteten mot ett giltigt dokument som utfärdats av polisen och som styrker personens identitet, till exempel ett ID-kort och pass eller ett körkort som utfärdats efter den 1 oktober 1990.

Godtagbara identifieringshandlingar är också ett giltigt pass eller identitetskort som utfärdats av myndighet i en medlemsstat inom EES, Schweiz eller San Marino, ett giltigt körkort som utfärdats efter 1.10.1990 av myndighet i en medlemsstat inom EES och ett giltigt pass som utfärdats av en myndighet i någon annan stat.

Servicecertifikatet beviljas för högst 27 månader.

Förnyelse av certifikat följer samma ansökningsförfarande som den ursprungliga ansökningen. Certifikatets pris utgår från en årlig avgift enligt Befolkningsregistercentralens serviceprislista.

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

Det beviljade servicecertifikatet levereras till kunden enligt avtalet.

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

Datainnehållet i ett certifikat kan inte ändras efter genereringen av certifikatet. Certifikat ska förnyas när uppgifter om certifikatinnehavaren som påverkar certifikatets datainnehåll ändras. I sådana fall ska certifikatinnehavaren kontakta utfärdaren och ansöka om ett nytt servicecertifikat.

Om användningen av certifikatinnehavarens privata nyckel förhindras ska certifikatet anslutet till nyckeln i fråga alltid förnyas.

Endast den organisation som är innehavare för certifikatet eller en organisationen befullmäktigad instans kan ansöka om att förnya certifikatet.

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

Vid förnyelse av servicecertifikatet iakttas samma rutiner som vid första ansökan om certifikat. Då certifikatinnehavaren förnyar sin privata nyckel fordrar detta alltid ny registrering, ny certifikatansökan och nytt servicecertifikat.

7.3.3 Skapande av certifikat

Certifikatets datainnehåll är beskrivet i FINEID S2-bestämmelsen, som finns på adressen www.fineid.fi.

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

Utfärdaren ser till att den privata nyckeln för innehavaren av e-postservicecertifikat överlämnas till innehavaren i enlighet med förfaringssätten i denna certifikatpolicy.

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

Certifikatinnehavarens privata nycklar är skyddade mot exponering och obehörig användning i certifikatinnehavarens datasystem. Bara interna kommandon i datasystemet ger tillgång till de privata nycklarna.

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

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

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren.

7.3.4 Distribution av användarvillkor

Utfärdaren ska se till att användarvillkoren tillhandahålls beställarna och de parter som litar på certifikatet.

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren.

Certifikatutfärdaren informerar om andra ändringar i certifikatpolicyn än de som anges i kapitel 8 på sin webbplats (www.fineid.fi) minst 30 dagar innan ändringen börjar gälla.

Utfärdaren publicerar samtliga servicecertifikat och spärrlistor i ett offentligt register som kan användas utan avgift. Utfärdaren publicerar certifikatpolicy, certifieringspraxis, certifikatbeskrivning samt övriga offentliga handlingar med anknytning till produktionen av certifikattjänster på sin webbplats http://www.fineid.fi.

Uppgifternas tillgänglighet

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

Dataförvaring

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats http://www.fineid.fi. 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 varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen, som publicerats på utfärdarens webbplats http://www.fineid.fi.

7.3.5 Distribution av certifikat

Certifikatet publiceras i det offentliga registret genast då det skapats och finns i registret under hela dess giltighetstid. Utfärdaren publicerar en spärrlista som är giltig två dygn efter publikationen. Denna spärrlista uppdateras varje timme

Uppgifter om register och spärrlista är offentligt tillgängliga ldap://ldap.fineid.fi.

7.3.6 Spärrning och tillfällig spärrning av certifikat

Spärrning och tillfällig spärrning av certifikat

Certifikatutfärdaren administrerar spärrtjänsten för certifikat. Uppgifterna om spärrade certifikat upptas på en spärrlista som utfärdaren
signerar och som publiceras i ett offentligt register. Utfärdaren tillhandahåller också en OCSP-tjänst för kontroll av certifikatets status. Certifikatet kan inte spärras tillfälligt.

Certifikatutfärdaren informerar inte certifikatinnehavare om spärrade certifikat.

Förutsättningar för spärrning av ett certifikat

Ett certifikat spärras om:

- innehavaren av certifikatet begär att certifikatet spärras

- certifikatinnehavarens uppgifter som påverkar datainnehållet i certifikatet har förändrats
- den privata nyckeln för certifikatet har kommit bort eller röjts
- organisationen som innehar certifikatet har upphört med sin verksamhet.

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

Behörig att begära spärrning

Behörig att begära spärrning av certifikat är:

- representant för organisationen som innehar servicecertifikatet;
- innehavaren av servicecertifikatet
- utfärdaren av certifikatet om förutsättningarna i punkt 6.2 uppfylls.

Process för spärrning av ett certifikat

Innehavaren av certifikatet begär utfärdaren av certifikatet spärra certifikatet. Begäran görs:

1. per telefon
2. personligen vid registreringsinstansen eller
3. skriftligen till certifikatutfärdaren.

Utfärdaren av certifikat spärrar certifikaten om:

- organisationen som innehar certifikatet upphör med sin verksamhet.

Följande uppgifter antecknas om spärrningen av certifikat:

- individuella uppgifter för servicecertifikatet
- personuppgifter för personen bakom spärrningsbegäran
- organisationen för personen bakom spärrningsbegäran
- autentiseringssätt för personen bakom spärrningsbegäran
- tidpunkt för spärrningsbegäran
- orsak till spärrningsbegäran
- personuppgifter för mottagaren av spärrningsbegäran
- eventuella övriga uppgifter som certifikatinnehavaren uppgett

- tidpunkten för röjning av nyckelparet, tidpunkten då organisationen som innehar certifikatet har upphört med sin verksamhet etc.
- personuppgifter för den som spärrat certifikatet
- tidpunkten för spärrning av certifikatet.

Certifikatutfärdaren informerar inte separat certifikatinnehavare om spärrade certifikat. Uppgifterna om spärrningen ska förvaras i 10 år från tidpunkten för spärrningen.

Certifikatinnehavarens skyldighet att begära spärrning

Certifikatinnehavaren ska utan dröjsmål lämna en begäran om spärrning till utfärdaren, om de förutsättningar för spärrning som beskrivs i kapitel 6.2 uppfylls.

Hanteringstid för begäran om spärrning av ett certifikat

Utfärdaren behandlar utan dröjsmål begäranden om spärrning av certifikat.

Förlitande parters skyldighet att kontrollera giltigheten för certifikat

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

Förlitande part ska kontrollera certifikatets gällande status eller spärrlista. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat certifikatets status.

Publiceringsfrekvens för spärrlista

En uppdaterad spärrlista publiceras varje timme.

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

Maximal giltighetstid för spärrlista

En uppdaterad spärrlista gäller i högst 48 timmar. I varje spärrlista anges när giltighetstiden går ut.

Certifikatinnehavaren kan begära att certifikatet spärras innan dess giltighetstid löpt ut.

Förfarande vid begäran om spärrning

Certifikatinnehavaren eller en behörig representant för organisationen som är innehavare av certifikatet ska meddela Befolkningsregistercentralens funktion Certifikattjänster om man känner till eller misstänker att certifikatinnehavarens privata nyckel har röjts. Anmälan görs per telefon tjänstetid till numret (09) 2291 6748, per fax till numret (09) 2291 6795 eller per e-post signerat med kvalificerat certifikat beviljat av Befolkningsregistercentralen till adressen vaestorekisterikeskus@vrk.fi. Anmälan ska innehålla följande uppgifter: anmälarens namn och organisation,

serienumret för servicecertifikatet som spärras. Efter att ha tagit emot anmälan spärrar utfärdaren certifikatet i fråga. Då certifikatinnehavaren har gjort en begäran om spärrning till utfärdaren och fått en bekräftelse på spärrningen (per telefon, fax eller e-post) upphör certifikatinnehavarens ansvar för användningen av certifikatet.

7.4 Utfärdarens lednings- och verksamhetspraxis

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

7.4.1 Hantering av säkerhet

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

7.4.2 Klassificering och hantering av reservice

Befolkningsregistercentralen är ett ämbetsverk underställt finansministeriet, vars certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Befolkningsregistercentralen 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.

Befolkningsregistercentralen svarar i enlighet med de allmänna avtalsvillkoren för IT-anskaffningar inom den offentliga förvaltningen för att man har tillräckliga ekonomiska resurser för att arrangera certifikatverksamheten på ett ändamålsenligt sätt samt hantera eventuella krav på skadeersättning (JIT 2007).

7.4.3 Personal och dataskydd

Befolkningsregistercentralen fungerar som certifikatutfärdare och svarar för certifikatverksamheten. De tekniska underleverantörerna har anlitats 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.

Utförande av bakgrundskontroll

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

Förfarande vid utförande av bakgrundskontroll

Personalens arbetserfarenhet kartläggs vid rekryteringen. En mindre säkerhetsutredning utförs för personen utgående från de uppgifter han eller hon uppger på ett standardiserat formulär.

Förfarandet för säkerhetsutredningen beskrivs detaljerat i certifieringspraxisen.

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.

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.

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 planeringen 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.

Åtgärder vid avvikelser

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

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.

Handlingar som tillhandahålls personalen

Personalen har alltid tillgång till Befolkningsregistercentralens kvalitets- och säkerhetsdokument.

7.4.4 Fysisk säkerhet och omgivningens säkerhet

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.

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.

Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässiga 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.

Reservarrangemang

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

Tillgången till reservdelar och service för viktig utrustning är säkrad.

7.4.5 Hantering av verksamheten

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

Certifikatutfärdarens uppgifter är indelade i ansvarsområden som beskrivs i certifieringspraxisen.

7.4.6 Hantering av tillgång till systemet

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

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

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

Registrering och autentisering av servicecertifikat fordrar närvaron av en person.

7.4.7 Ibruktagning och underhåll av pålitliga system

Autentiseringen av certifikatets registrerare, underhållaren av certifikatsystemet och användaren av certifikatsystemet samt uppdragsbeskrivningen beskrivs detaljerat i certifieringspraxisen.

7.4.8 Hantering av kontinuerlig affärsverksamhet och störningar

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

Beredskap för undantagssituationer är beskriven i certifieringspraxisen.

Utfärdarens privata nyckel har röjts eller certifikatet har spärrats

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

I detta fall ska utfärdaren av rotcertifikatet antingen upphöra med sin verksamhet på det sätt som beskrivs i kapitel 7.4.9 eller utföra följande åtgärder:

a) Utfärdaren av rotcertifikatet 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 av rotcertifikatet skapar en ny nyckel i enlighet med kapitel 7.3.3

c) Utfärdarens samtliga gällande certifikat och certifikat för slutanvändare om beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan giltighetstiden har löpt ut för det av utfärdarens certifikat som spärrats senast.

Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Befolkningsregistercentralens säkerhetspolicy beaktas åtgärder som förorsakas av problem med den externa säkerheten. Befolkningsregistercentralen har fått ISO 27001-dataskyddscertifikatet, som ställer krav på Befolkningsregistercentralens verksamhet även utifall en eventuell katastrof.

7.4.9 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 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 servicecertifikat spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade servicecertifikatets 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 bevaras även efter att utfärdarens verksamhet har upphört.

7.4.10 Tillämplig lagstiftning

Befolkningsregistercentralen efterlever i sin servicecertifikatverksamhet den gällande lagstiftningen i Finland.

Bestämmelser om av Befolkningsregistercentralen beviljade certifikat fastställs i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Befolkningsregistercentralens skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande samarbetsavtal och skadeståndslagen (412/1974) . Befolkningsregistercentralen omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

7.4.11 Förvaring av information om certifikat

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats. 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 varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen.

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 5 år från tidpunkten då certifikaten upphört att gälla. Utfärdaren arkiverar följande uppgifter:

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

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

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

d) Begäranden om spärrning av servicecertifikat

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

f) Gällande certifikatpolicy och tidigare certifikatpolicyn och motsvarande certifieringspraxis

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

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

Det arkiverade materialet förvaras enligt bestämmelserna för myndighet som fungerar som utfärdare av kvalificerade certifikat.

Skydd av arkiv

Utfärdaren förvarar handlingar med anknytning till ansökning om servicecertifikat, autentisering av personer och överlåtelse av servicecertifikat som arkiveras i ändamålsenliga lokaler.

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

Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

Metoder för införskaffning och tryggande av arkiverat material

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

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

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

7.5 Krav på organisationen

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 beviljar certifikat utgående från ansökan. Rättigheterna och skyldigheterna för certifikatsökanden ingår i Befolkningsregistercentralens ansökningsdokument för servicecertifikat och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

Befolkningsregistercentralen och registreraren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheterna för samtliga parter.

Befolkningsregistercentralens certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Befolkningsregistercentralen är ett ämbetsverk underställt finansministeriet. Befolkningsregistercentralen 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.

Befolkningsregistercentralen efterlever i sin servicecertifikatverksamhet den gällande lagstiftningen i Finland. Befolkningsregistercentralen agerar omsorgsfullt, pålitligt och ändamålsenligt. Utfärdaren ser till att uppgifter om certifikat och certifikatverksamhet utgående från vilka utfärdarens verksamhet och pålitlighet kan bedömas är offentligt tillgängliga.

Befolkningsregistercentralen fäster särskild uppmärksamhet vid såväl den egna personalens som leverantörernas och registrerarnas pålitlighet och kompetens för att utföra uppgifterna. Befolkningsregistercentralen har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt täcka eventuellt skadeersättningsansvar. Befolkningsregistercentralens personal agerar i sitt uppdrag med ämbetsmannaansvar och i enlighet med Befolkningsregistercentralens interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

Eventuella tvister löses enligt rättssystemet i Finland. Vid lösningen av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning.

Denna certifikatpolicy har registrerats av Befolkningscentralen och upphovsrätten tillfaller Befolkningsregistercentralen. Befolkningsregistercentralen äger samtliga uppgifter som anknyter till certifikaten och dokumentationen i enlighet med de tekniska leveransavtalen. Befolkningsregistercentralen äger samtliga ägande- och användarrättigheter för denna certifikatpolicy. Befolkningsregistercentralen svarar för administrationen och uppdateringen av denna certifikatpolicy.

8 . Definitionsramar för övriga certifikatpolicydokument

I denna punkt fastställs de övriga allmänna ramarna för certifikatpolicyn för certifikatutfärdare. Utfärdaren kan uppge att man iakttar dessa allmänna definitionsramar enligt kraven i punkt 8.3. Allmänt taget förutsätter överensstämmelse med kraven att man iakttar kraven i punkt 6 och 7 med undantag för de krav som endast tillämpas för utfärdare som beviljar certifikat till allmänheten.

8.1 Hantering av dokument innehållande bestämmelser

Ändring av bestämmelser

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

Publicering och information

Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen, som är tillgängliga på adressen http://www.fineid.fi/.

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

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

Förfarande för ändring och godkännande av certifieringspraxis

Befolkningsregistercentralen godkänner såväl certifikatpolicyn som certifieringspraxisen för servicecertifikatet. Handlingarna kan ändras med Befolkningsregistercentralens interna ändringsförfarande.

Befolkningsregistercentralen informerar om ändringar i god tid innan de träder i kraft till Kommunikationsverket och 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 certifikatpolicyn och certifieringspraxisen kan ändras så att kommande väsentliga ändringar meddelas 30 dagar innan de träder i kraft.

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

8.2 Ytterligare krav

Vid verkställandet av kraven som fastställs i punkt 7.3.4 ska beställare och förlitande parter informeras vad varje policy medför eller begränsar då det gäller kraven i certifikatpolicyn så som de fastställs i detta dokument.

8.3 Överensstämmelse med krav

Utfärdaren får uppge att man iakttar denna certifikatpolicy endast om.

a) om utfärdaren uttrycker att man iakttar den specifika certifikatpolicyn och på begäran lämnar intyg till beställaren och de förlitande parterna om överensstämmelse med kraven. Intyget kan exempelvis vara auditerarens berättelse som bekräftar att utfärdaren uppfyller kraven i den specifika certifikatpolicyn. Det kan röra sig om en intern auditerare inom organisationen, men auditeraren får inte vara över- eller underordnat med avdelningen som utför utfärdarens verksamhet.

b) om en behörig och oberoende part inom den senaste tiden har bedömt uppfyllningen av kraven i den specifika certifikatpolicyn hos utfärdaren. Resultaten av granskningen ska på begäran göras tillgängligt för beställarna och de förlitande parterna.

VRK/TS/Keh

03-05-2018