Certifieringspraxis för medborgarcertifikat som ingår i ID-kort

OID: 1.2.246.517.1.10.2.1

13.3.2010

Befolkningsregistercentralen

Innehållsförteckning

Definitioner och förkortningar

Definitioner

Aktiveringsdata: Konfidentiell information (PIN-kod) som behövs för aktiveringen av de privata nycklar som finns lagrade på mikrochips och för användningen av dem inom den öppna nyckeltekniken (t.ex. elektroniska signaturer).

Asymmetrisk krypteringsteknik: Vid asymmetrisk kryptering används ett nyckelpar med en publik och en privat nyckel. Ett meddelande som har krypterats med en publik nyckel kan bara dekrypteras med en privat nyckel som hör till samma nyckelpar.

Betalkort: Allmän benämning på bank-, kredit-, kombinations-, kontant- och betaltidskort.

Certifieringspraxis: En beskrivning av hur certifikatutfärdaren ska genomföra certifikatpolicyn. Varje certifieringspraxis har en individualiserande kod.

Certifikat: Ett elektroniskt intyg som knyter den signerade informationen till undertecknaren och bekräftar undertecknaren. Certifikatet innehåller en kod som individualiserar anknytande certifieringspraxis.

Certifikatanvändning och användningsområde för certifikat: I detta dokument avses med certifikatanvändning användningen av såväl själva certifikatet som tillhörande nycklar. Till exempel med användningen av certifikat för elektroniska signaturer avses användningen av dels privata nycklar för signaturer, dels publika nycklar och certifikat för autentisering av signaturer.

Certifikatbeskrivning: Ett dokument som innehåller de viktigaste elementen i certifikatpolicyn och certifieringspraxisen.

Certifikatinnehavare: Person vars identitet och publika nyckel har verifierats med certifikatutfärdarens elektroniska signatur och som innehar de privata nycklar som certifikatet hänför sig till.

Certifikatinnehavarens autentiserings- och krypteringscertifikat: Ett certifikat som används för elektronisk identifiering av personer och för kryptering av data. Certifikatinnehavaren använder sin

privata autentiserings- och krypteringsnyckel för elektronisk identifiering och för dekryptering av krypterade data eller meddelanden. För användningen av nyckeln behövs en baskod (PIN 1).

Certifikatinnehavarens signeringscertifikat: Med den publika nyckel som finns lagrad på certifikatet verifieras med hjälp av motsvarande privata nyckel, dvs. med signeringsnyckeln, certifikatinnehavarens elektroniska signatur. För signeringen behövs en signaturkod (PIN 2).

Certifikatpolicy: Ett dokument som beskriver de principer som tillämpas när certifikat beviljas samt förlitande parters ansvar. De certifikatpolicier som Befolkningsregistercentralen har publicerat är allmänt tillgängliga. Varje certifikatpolicy har en särskild kod som individualiserar den.

Certifikatregister: Ett register som avses i lagen om stark autentisering och elektroniska signaturer och som ska föras av organ som utfärdar kvalificerade certifikat som bjuds ut till allmänheten. Uppgifterna ska bevaras i minst 10 år efter att ett certifikats giltighet har gått ut.

Certifikatsystem: Ett datatekniskt system med vars hjälp certifikat kan skapas och spärrlistor signeras.

Certifikatsökande: Person som ansöker om medborgarcertifikat och som identifieras på ett tillförlitligt sätt i samband med ansökan.

Certifikatutfärdare: En organisation som beviljar certifikat, svarar för produktionen av certifikat och upprättar en certifikatpolicy och en certifieringspraxis som beskriver verksamheten.

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

Certifikatutfärdarens privata nyckel: En privat nyckel som används för att signera certifikat som beviljas av utfärdaren och spärrlistor som denne publicerar.

Datasystem för certifiering: Ett datatekniskt system som består av certifikatsystem, datakommunikation, certifikatregister och spärrlisttjänster, informations- och spärrtjänst samt administrering av certifikat och kort.

Elektronisk kommmunikationskod: En identifikator som består av siffror och en kontrollbeteckning och som kan användas för att individualisera finska medborgare och utlänningar som enligt lagen om hemkommun är fast bosatta i Finland och införda i befolkningsdatasystemet.

Förlitande part: En part som litar på certifikatuppgifterna och använder certifikatet för olika tjänster inom IT-säkerhet, såsom elektronisk identifiering av certifikatinnehavare och autentisering av elektroniska signaturer.

Identitetskort, ID-kort: Legitimation som har beviljats av polisen och i vars tekniska del kortinnehavarens medborgarcertifikat är lagrat.

Koden som individualiserar certifieringspraxisen är en del av certifikatets datainnehåll.

Kortläsarprogram: Kortläsarprogram används i datorn som s.k. slutanvändarprogram. Med hjälp av programmet kan användaren utnyttja sitt kort och de certifikat som finns lagrade på det i olika användarmiljöer och applikationer, till exempel vid elektronisk kommunikation, för säker e-post och vid inloggning på datorn.

Kvalificerat certifikat: Ett certifikat vars innehåll överensstämmer med det lagstadgade innehållet för kvalificerade certifikat och som har beviljats av en utfärdare som tillhandahåller kvalificerade certifikat och uppfyller kraven i lagen. Datainnehållet i kvalificerade certifikat bestäms i lagen om stark autentisering och elektroniska signaturer.

Medborgarcertifikat: Ett kvalificerat certifikat som Befolkningsregistercentralen beviljar fysiska personer och vars datainnehåll bestäms i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Mikrochip: En teknisk plattform på vilken certifikat och privata nycklar är lagrade och som är inbyggd i ID-kort, betalkort eller mobiltelefonens SIM-kort

Mobilterminal: Mobiltelefon eller annan mobilenhet med vars hjälp man kan använda certifikat och privata nycklar som är lagrade på mikrochips..

Nyckelpar: Nycklar, en publik och en privat, som är knutna till varandra och används inom den öppna nyckeltekniken. Nycklarnas användningsområde anges i certifikatet (se certifikatinnehavarens signeringscertifikat samt autentiserings- och krypteringscertifikat).

PIN-kod: Aktiveringsdata som används för att aktivera den privata nyckeln på ett mikrochip. PIN 1: baskod för autentisering och kryptering. PIN 2: signaturkod för elektroniska signaturer.

Privat nyckel: Den privata delen av det nyckelpar som används vid asymmetrisk kryptering inom den öppna nyckeltekniken. Certifikatinnehavarens privata nycklar finns lagrade på ett mikrochip för att skydda dem mot obehörig användning

Publik nyckel: Vid asymmetrisk kryptering inom den öppna nyckeltekniken används den publika delen av nyckelparet. Med sin elektroniska underskrift bekräftar certifikatutfärdaren att den publika nyckeln hör sig till certifikatinnehavaren. Den publika nyckeln är en del av certifikatets datainnehåll.

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

Registrerare: En registrerare ska för certifikatutfärdarens räkning och på dennes ansvar verifiera identiteten hos den som ansöker om certifikat i enlighet med certifikatpolicyn och certifikatpraxisen.

RSA-algoritm och RSA-nyckel: RSA-algoritmen är en allmänt använd öppen nyckel-algoritm. De privata och publika nycklar som hänför sig till medborgarcertifikat är RSA-nycklar.

Spärrlista: En förteckning som är elektroniskt signerad och publicerad av certifikatutfärdaren och som innehåller certifikat som spärrats mitt under giltighetstiden samt tidpunkten för spärrningen. Av spärrlistan ska framgå publiceringstidpunkten för den och nästa spärrlista. På spärrlistan upptas spärrade certifikat.

Spärrtjänst: Teknisk leverantör som för certifikatutfärdarens räkning tar emot och förmedlar begäran om spärrningar av certifikat till certifikatsystemet.

Öppen nyckelteknik: En IT-säkerhetstjänst, till exempel elektronisk identifiering av en person, som genereras med hjälp av publika och privata nycklar, certifikat och asymmetrisk kryptering.

Öppet nyckelsystem: En säkerhetsinfrastruktur inom vilken IT-säkerhetstjänster genereras med stöd av en öppen nyckelteknik.

Förteckning över förkortningar

CA	Certification Authority, certifikatutfärdare
CP	Certificate Policy, certifikatpolicy
CPS	Certification Practise Statement, certifieringspraxis
CRL	Certificate Revocation List, spärrlista
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, säkerhetsmodul
eID	Elektronisk identifiering av person
HTTP	Hypertext Transfer Protocol
ISO 27001	ISO/IEC 27001
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, standard för verifiering av certifikatstatus i realtid över Internet
OID	Object Identifier, individualiserande beteckning
PDS	PKI Disclosure Statement, certifikatbeskrivning
PIN	Personal Identification Number, PIN-kod
PKI	Public Key Infrastructure, öppet nyckelsystem
PUK	PIN Unblocking Key, PUK-kod
RSA	Rivest, Shamir, Adleman, en algoritm för den öppna nyckeln, en asymmetrisk algoritm
SATU	Elektronisk kommunikationskod
SIM	Subscriber Identity Module
BRC	Befolkningsregistercentralen

1 Inledning

Certifikatpolicyn är en beskrivning som har utarbetats av certifikatutfärdaren och som handlar om de förfaranden och verksamhetsprinciper som ska iakttas vid beviljandet av certifikat. Certifieringspraxisen är en mer detaljerad beskrivning av utfärdarens verksamhet än certifikatpolicyn.

Denna certifieringspraxis tillämpas på Befolkningsregistercentralens medborgarcertifikat som ingår i ID-kort och som beviljas finska medborgare och utlänningar som är fast bosatta i Finland och som är införda i befolkningsdatasystemet.

Ett medborgarcertifikat är ett kvalificerat certifikat enligt lagen om stark autentisering och elektroniska signaturer.

1.1 Allmänt

Ett certifikat är ett elektroniskt intyg som knyter autentiseringsuppgifterna i signaturen till undertecknaren och bekräftar certifikatinnehavarens identitet. Uppgifterna i certifikatet är elektroniskt signerade med certifikatutfärdarens privata nyckel. Ett certifikat enligt denna certifikatpolicy grundar sig på system och tekniker med publika nycklar. Datainnehållet i certifikat som följer denna certifikatpolicy preciseras i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och i lagen om stark autentisering och elektroniska signaturer (617/2009).

Medborgarcertifikat består av ett certifikatpar som används för två olika syften: det ena certifikatet i paret används för autentisering och kryptering och det andra för elektroniska signaturer. Signeringscertifikatet är ett kvalificerat certifikat enligt lagen om stark autentisering och elektroniska signaturer. Befolkningsregistercentralen garanterar att certifikatet innehåller korrekt identitet.

I egenskap av certifikatutfärdare individualiserar Befolkningsregistercentralen certifikatinnehavaren med hjälp av en elektronisk kommunikationskod, som också är en del av certifikatets datainnehåll. Koden utgörs av teknisk identifieringsinformation som definieras i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009)och har särskilt skapats för elektronisk kommunikation. Informationen innehåller inte några identifikationsuppgifter som hänför sig till personen i fråga.

Medborgarcertifikat kan beviljas för och lagras på olika tekniska plattformar, dvs. mikrochips, såsom ID-kort, bankernas chipförsedda betalkort och mobilterminalernas SIM-kort. Denna certifieringspraxis är en beskrivning av medborgarcertifikat som ingår i ID-kort.

Befolkningsregistercentralens certifikatpolicy och certifieringspraxis har båda en individualiserande kod (OID).

Till certifikatutfärdarens uppgifter hör att producera certifikat-, register- och spärrtjänster, sköta registrering samt framställa och individualisera aktivkort. Dessa uppgifter beskrivs närmare i kapitel 1.3.

Befolkningsregistercentralen ska utarbeta en särskild certifikatpolicy för alla typer av certifikat som centralen beviljar och en certifieringspraxis för varje enskild teknisk plattform. I certifikatpolicyn beskrivs för varje typ av certifikat tillämpliga förfaranden, användarvillkor, ansvarsfördelning och andra aspekter på användningen av certifikatet på en allmän nivå. Certifieringspraxisen beskriver mera i detalj de förfaranden som ska följas.

Signeringscertifikat som beviljats i enlighet med denna certifieringspraxis ska uppfylla de krav som ställs på sådana kvalificerade certifikat som avses i Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer, nedan direktivet om elektroniska signaturer, och i dess bilagor. I lagen om stark autentisering och elektroniska signaturer (617/2009) finns bestämmelser om elektroniska signaturer som är baserade på kvalificerade certifikat. I Finland utövas tillsynen över certifikatutfärdare av Kommunikationsverket. Bestämmelser om ID-kort finns i lagen om identitetskort (829/1999) och i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Enligt lagen om stark autentisering och elektroniska signaturer är Befolkningsregistercentralen som utgivare av certifikatbaserade identifieringsverktyg också leverantör av identifieringstjänster. I Finland övervakas leverantörerna av identifieringstjänster av Kommunikationsverket.

1.2 Identifikationsuppgifter

Namnet på denna certifieringspraxis är Certifieringspraxis för Befolkningsregistercentralens medborgarcertifikat som ingår i ID-kort, och dess OID är 1.2.246.517.1.10.2.1.

Denna certifieringspraxis hänför sig till certifikatpolicyn för Befolkningsregistercentralens medborgarcertifikat vars OID är 1.2.246.517.1.10.2.

Såväl certifikatpolicyn som certifieringspraxisen finns på adressen http://www.fineid.fi.

1.3 Certifikatutfärdare och tillämpningsområden för certifikaten

Certifikatutfärdaren tillhandahåller certifikattjänster på de villkor som anges i denna certifieringspraxis och svarar gentemot certifikatinnehavaren för deras funktion enligt kapitel 2.2.1 om certifikatutfärdarens ansvar. Certifikatutfärdaren är ansvarig för hela certifikatsystemet liksom för de registrerare och tekniska leverantörer som utfärdaren anlitar. Certifieringspraxisen har registrerats av Befolkningsregistercentralen som är en myndighet som för personregister och vars uppgift enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) är att producera certifierade tjänster för elektronisk kommunikation. Befolkningsregistercentralens certifikattjänst indelas funktionellt i följande delområden.

1.3.1 Certifikatutfärdare

Certifikatutfärdarens uppgift är att:

● tillhandahålla certifikat- och registertjänster samt spärrlisttjänster enligt certifikatpolicyn och certifieringspraxisen
● personligen identifiera den som ansöker om certifikat
● se till att datainnehållet i certifikaten är korrekt
● ansvara för spärrning av certifikat och publicering av spärrlistor med återkallade certifikat
● iaktta kraven på god datasäkerhetsnivå och god informationshantering vid behandlingen av certifikatinnehavarnas personuppgifter.

1.3.2 Registrerare

Polisen sköter registreringen av medborgarcertifikat som ingår i ID-kort.
.
● Registreraren agerar på uppdrag av certifikatutfärdaren och under dennes ansvar.
● Registreraren ska följa certifikatutfärdarens certifikatpolicy och certifieringspraxis.
● Registreraren ska identifiera den som ansöker om certifikat på det sätt som anges i certifieringspraxisen.
● Underlaget till medborgarcertifikat som ingår i ID-kort har framställts av polisen.

● Polisen ska i egenskap av registrerare lämna de identifikationsuppgifter som behövs för identifieringen av personer som ansöker om medborgarcertifikat som ingår i ID-kort och som ligger till grund för genereringen av certifikatet.

1.3.3 Tillverkare och individualiserare av aktivkort

● När det gäller certifikat, tillhörande nyckelpar och aktiveringsinformation handlar tillverkaren på uppdrag av certifikatutfärdaren och under dennes ansvar på det sätt som anges i samarbetsavtalet.
● Tillverkaren ska följa certifikatutfärdarens certifikatpolicy och certifieringspraxis.
● Aktivkort ska individualiseras enligt de uppgifter som lämnas av registreraren.

1.3.4 Spärrtjänst

Spärrtjänsten för certifikat spärrar certifikat som certifikatinnehavaren eller certifikatutfärdaren vill återkalla innan giltighetstiden har gått ut. Spärrade certifikat upptas på en spärrlista. Orsaken till spärrning av medborgarcertifikat som ingår i ID-kort kan vara t.ex. att ID-kortet har försvunnit.

1.3.5 Registertjänst

Registertjänsten är en offentlig webbtjänst som ger allmänheten tillgång till alla medborgarcertifikat som har beviljats av certifikatutfärdaren samt utfärdarcertifikat och spärrlista. Registertjänsten finns på adressen ldap://ldap.fineid.fi.

1.3.6 Certifikatinnehavare

Medborgarcertifikat enligt denna certifieringspraxis kan beviljas finska medborgare eller utlänningar som enligt lagen om hemkommun (201/1994) är fast bosatta i Finland och vilkas personuppgifter har registrerats i befolkningsdatasystemet.

Certifikatinnehavaren ska följa utfärdarens certifikatpolicy och certifieringspraxis.

1.3.7 Förlitande parter

Förlitande parter är personer eller organisationer som litar på innehållet i ett certifikat och använder certifikatet för autentisering, för kryptering av information och för elektroniska signaturer. Förlitande parter ska kontrollera att certifikat som används är giltiga och inte är upptagna på någon spärrlista.

1.3.8 Användning av certifikat

Medborgarcertifikat som utfärdas med stöd av denna certifieringspraxis kan användas för identifiering av personer, kryptering av information och elektroniska signaturer. Certifikatet får användas utan begränsningar i enlighet med sitt syfte i tillämpningar och tjänster som tillhandahålls av förvaltningen och privata organisationer.

I certifikatpolicyn och certifieringspraxisen anges de krav som ställs på utfärdare, registrerare, certifikatinnehavare och förlitande parter samt frågor om lagstiftning och lösning av eventuella tvister.

1.4 Kontaktuppgifter

1.4.1 Organisation som administrerar certifieringspraxisen

Denna certifieringspraxis har registrerats av Befolkningsregistercentralen, som är en myndighet som för personregister. Befolkningsregistercentralens uppgift enligt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) är att utöver sina övriga uppgifter producera certifierade tjänster för elektronisk kommunikation. Befolkningsregistercentralen svarar för administration och uppdatering av certifieringspraxisen.

1.4.2 Kontaktperson

Frågor som gäller certifieringspraxisen kan skickas till adressen:

Befolkningsregistercentralen	vaestorekisterkeskus@vrk.fi
PB 70 (Tunnbindaregatan 1 C)	Tfn +358 9 229 161
00581 Helsingfors	Fax +358 9 2291 6795
FO-nummer: 0245437-2	

Frågor som gäller certifikatpolicyn och dessa dokument besvaras av Befolkningsregistercentralens enhet för certifikattjänster.

Befolkningsregistercentralen (BRC) Certifikattjänster
PB 70
00581 Helsingfors
www.fineid.fi

2 Allmänna villkor

Certifieringspraxisen träder i kraft den 1 december 2010. Förfarandet vid ändring och publicering av certifieringspraxisen beskrivs i kapitel 8 i detta dokument.

2.1 Skyldigheter

2.1.1 Certifikatutfärdarens skyldigheter

● Befolkningsregistercentralens uppgift som certifikatutfärdare föreskrivs i lag.
● Certifikatutfärdaren ska följa gällande lagstiftning i sin verksamhet.
● Certifikatutfärdaren ska handla omsorgsfullt, tillförlitligt och ändamålsenligt.
● Certifikatutfärdaren ska ha tillräcklig teknisk sakkunskap och förfoga över tillräckliga ekonomiska resurser för att ordna verksamheten på lämpligt sätt och täcka ett eventuellt skadeståndsansvar.
● Certifikatutfärdaren ansvarar för alla delområden inom certifikatverksamheten, också för tillförlitligheten och funktionen hos de tjänster och produkter som produceras av tekniska leverantörer eller personer som utfärdaren anlitar, såsom registrerare och korttillverkare.
● Certifikatutfärdaren ska utarbeta och upprätthålla en certifikatpolicy som på ett allmänt plan beskriver de förfaranden och användarvillkor, den ansvarsfördelning och andra aspekter på användningen av medborgarcertifikat som tillämpas på beviljande, underhåll och administration av medborgarcertifikat.
● Certifikatutfärdaren utarbetar och upprätthåller en certifieringspraxis som beskriver hur utfärdaren ska tillämpa certifikatpolicyn.
● Certifikatutfärdaren ska iaktta kraven i certifikatpolicyn och certifieringspraxisen.
● Certifikatutfärdaren ska publicera certifikatpolicyn och certifieringspraxisen så att de är allmänt tillgängliga.

● Certifikatutfärdaren ska ha tillräckligt med personal med den sakkunskap, erfarenhet och kompetens som krävs för att producera certifikattjänster.
● Certifikatutfärdaren ska använda tillförlitliga system och produkter som är skyddade mot obehörig användning.
● Certifikatutfärdaren ska hålla uppgifter om certifikaten och certifikatverksamheten allmänt tillgängliga och utifrån uppgifterna kan utfärdarens verksamhet och tillförlitlighet bedömas.
● Certifikatutfärdaren ska garantera att uppgifterna för genereringen av signaturer hålls konfidentiella.
● Certifikatutfärdaren får inte lagra eller kopiera de uppgifter som lämnas till signeraren för generering av signaturer.

2.1.2 Registrerarens skyldigheter

● Vid registreringen ska registreraren följa certifikatpolicyn och certifieringspraxisen.
● Registreraren ska personligen och tillförlitligt identifiera den som ansöker om certifikat på det sätt som anges i certifieringspraxisen och noggrant kontrollera sökandens identitet liksom andra uppgifter som anknyter till sökandens person och som är nödvändiga vid beviljandet av certifikat.
● Registreraren ska se till att personuppgifterna behandlas omsorgsfullt och konfidentiellt.
● Registreraren ska informera certifikatsökanden om villkoren för användningen av certifikatet.
● I samband med registreringen ska de förfaranden följas som registreraren och utfärdaren kommit överens om.

2.1.3 Certifikatinnehavarens skyldigheter

● Syftet med ett certifikat fastställs i certifikatpolicyn och i certifieringspraxisen för varje enskild typ av certifikat samt i användaranvisningarna för certifikatinnehavare. Certifikatet får användas enbart i avsett syfte för elektroniska signaturer, autentisering eller kryptering av information.
● Innehavare av medborgarcertifikat svarar för att de uppgifter som de har uppgett vid ansökan om certifikatet är korrekta.
● Certifikatinnehavaren svarar för användningen av ID-kortet och det medborgarcertifikat som ingår i det, för rättshandlingar som företas med stöd av certifikatet och för de ekonomiska följderna av det. I fråga om signeringscertifikat iakttas vad som bestäms i direktivet om elektroniska signaturer och i lagen om stark autentisering och elektroniska signaturer.
● Certifikatinnehavaren ska förvara sina privata nycklar och den kod som behövs för användningen skilt från varandra samt förhindra att de privata nycklarna förkommer, hamnar i utomståendes händer, ändras eller används obehörigt. Om innehavaren lämnar ut ID-kortet eller avslöjar PIN-koden för en

annan person t.ex. genom att låna ut den, befrias utfärdare och förlitande parter från det ansvar som eventuellt följer av att kortet används.

● Medborgarcertifikat som ingår i ID-kort ska behandlas och skyddas lika omsorgsfullt som andra liknande kort eller dokument, såsom kreditkort, körkort och pass. Personliga PIN-koder ska förvaras fysiskt åtskilda från ID-kort.

● Om medborgarcertifikatet och ID-kortet förkommer eller vid misstanke om att kortet missbrukas, ska utfärdaren omedelbart underrättas genom ett samtal till den avgiftsfria spärrtjänsten +358 800 162 622. För döva och hörselskadade finns ett motsvarande texttelefonnummer +358 100 2288.

2.1.4 Förlitande parters skyldigheter

Till förlitande parters skyldigheter hör att kontrollera att certifikaten används för avsett syfte. Medborgarcertifikat som är kvalificerade certifikat som ingår i ID-kort används för elektroniska signaturer. Syftet med autentiserings- och krypteringscertifikat är att identifiera personer och kryptera information.

Förlitande parter ska följa certifikatpolicyn och certifieringspraxisen.

Förlitande parter kan uppriktigt lita på ett medborgarcertifikat efter att ha kontrollerat att ***certifikatet är giltigt och inte har upptagits på någon spärrlista***. Förlitande parter är skyldiga att kontrollera certifikat mot en spärrlista. För att försäkra sig om att giltighetstiden för ett certifikat stämmer, ska en förlitande part följa nedan angivna åtgärder för spärrkontroll.

En förlitande part som kopierar spärrlistan från registret ska försäkra sig om spärrlistans äkthet genom att kontrollera den elektroniska signaturen för den utfärdare som har signerat spärrlistan. Dessutom ska spärrlistans giltighetstid kontrolleras.

Om det till följd av funktionsstörningar i utrustningen eller registertjänsten inte är möjligt att få tillgång till den senaste spärrlistan från registret, ska ett medborgarcertifikat inte godkännas, i fall giltighetstiden för den senast erhållna spärrlistan har gått ut. Alla godkännanden av medborgarcertifikat efter att giltighetstiden har gått ut sker på den förlitande partens egen risk.

2.1.5 Skyldigheter i samband med publiceringen av medborgarcertifikat

Medborgarcertifikat publiceras i ett allmänt tillgängligt offentligt register och spärrade medborgarcertifikat i en spärrlista mot vilken förlitande parter ska kontrollera uppgifter om certifikatens giltighet.

2.2 Ansvar

2.2.1 Certifikatutfärdarens ansvar

I egenskap av certifikatutfärdare svarar Befolkningsregistercentralen för säkerheten inom hela certifikatsystemet. För de tjänster som uppdragits åt utfärdaren svarar utfärdaren på samma sätt som om denne själv skulle ha producerat tjänsten.

Befolkningsregistercentralen svarar för att medborgarcertifikat genereras med iakttagande av de förfaranden som anges i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009), i lagen om stark autentisering och elektroniska signaturer, i lagen om elektronisk kommunikation i myndigheternas verksamhet, i certifikatpolicyn och i certifieringspraxisen samt enligt de uppgifter som certifikatsökanden har lämnat. Befolkningsregistercentralen svarar bara för de uppgifter som den har lagrat i certifikatet.

Befolkningsregistercentralen svarar för att medborgarcertifikat kan användas från det att de överlämnas till innehavaren tills giltighetstiden går ut, förutsatt att de används på behörigt sätt och inte har upptagits på någon spärrlista. Mottagaren av ett medborgarcertifikat ska ha identifierats på det sätt som anges för medborgarcertifikat. Innan ett avtal undertecknas ska certifikatinnehavaren få anvisningar om användningen av certifikatet.

Genom signeringen av ett medborgarcertifikat med sin privata nyckel intygar certifikatutfärdaren att personuppgifterna i certifikatet har kontrollerats enligt de förfaranden som har fastslagits i certifikatpolicyn och certifieringspraxisen.

Utfärdaren svarar för att de medborgarcertifikat som spärras tillhör rätt person och upptas på en spärrlista inom den tid som anges i denna certifieringspraxis.

2.2.2 Registrerarens ansvar

Registrerare av ID-kort är polisen som registrerar certifikatsökande för utfärdarens, dvs. Befolkningsregistercentralens räkning. Närmare bestämmelser om polisen åtgärder i samband med registreringen finns i lagen om identitetskort.

2.2.3 Certifikatinnehavarens ansvar

Medborgarcertifikatet är innehavarens elektroniska identitet och får därför inte överlåtas till någon annan.

Innehavaren av ett medborgarcertifikat svarar för användningen av certifikatet, för de rättshandlingar som företas med stöd av certifikatet och för de ekonomiska följderna av det.

Om ett ID-kort kvarlämnas i avläsaren, kan det leda till att kortet missbrukas. När en terminalsession avslutas eller terminalen lämnas utan tillsyn ska certifikatinnehavaren avlägsna ID-kortet från avläsaren och på föreskrivet sätt stänga de program som har använts.

Certifikatinnehavarens ansvar för användningen av ett medborgarcertifikat som ingår i ett ID-kort upphör när innehavaren har anmält till spärrtjänsten de uppgifter som är nödvändiga för att spärra certifikatet och efter att ha fått ett meddelande om spärrningen från den funktionär som mottagit samtalet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

2.2.4 Förlitande parters ansvar

Förlitande parter kan inte uppriktigt lita på giltigheten hos medborgarcertifikat eller elektroniska signaturer, om de inte har kontrollerat certifikatets giltighetstid mot en spärrlista. Om ett medborgarcertifikat godkänns i sådana fall, befrias Befolkningsregistercentralen från sitt ansvar. Förlitande parter är skyldiga att kontrollera att ett beviljat certifikat har använts i överensstämmelse med sitt syfte i den rättshandling det gäller.

2.2.5 Ansvarsbegränsningar

Befolkningsregistercentralens skadeståndsansvar i samband med produktionen av certifikattjänster regleras i skadeståndslagen (412/1974). På Befolkningsregistercentralen tillämpas också

bestämmelserna om certifikatutfärdarens ansvar i lagen om stark autentisering och elektroniska signaturer och lagen om elektronisk kommunikation i myndigheternas verksamhet.

Befolkningsregistercentralen svarar inte för eventuella skador som orsakas av att PIN-koden, PUK-koden eller certifikatinnehavarens privata nycklar röjs, om inte avslöjandet 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.

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 till 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 spärrlistan meddelas på förhand.

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

Vid fel i en nättjänst eller applikation som hänför sig till ett certifikat avsett för medborgare och organisationer svarar utfärdaren inte för användningen av certifikatet eller för de kostnader som det orsakar användaren.

Kortinnehavarens ansvar för användningen av ett medborgarcertifikat upphör när innehavaren har anmält till spärrtjänsten de uppgifter som är nödvändiga för att spärra certifikatet och efter att ha fått ett meddelande om spärrningen från den funktionär som mottagit samtalet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

2.3 Ekonomiskt ansvar

2.3.1 Certifikatutfärdare

Befolkningsregistercentralens skadeståndsansvar i samband med produktionen av certifikattjänster regleras i skadeståndslagen (412/1974). På Befolkningsregistercentralen tillämpas också bestämmelserna om certifikatutfärdarens ansvar i lagen om stark autentisering och elektroniska signaturer och lagen om elektronisk kommunikation i myndigheternas verksamhet.

Befolkningsregistercentralens ansvar gentemot förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Befolkningsregistercentralens åtgärder.

2.3.2 Övriga parter

Förlitande parter kan lita på att medborgarcertifikat och elektroniska signaturer är korrekta efter att ha kontrollerat att certifikatet inte har upptagits på någon spärrlista och att certifikatets giltighetstid inte har gått ut, om de inte har några andra skäl att på goda grunder misstänka att certifikatet inte används korrekt.

Certifikatutfärdaren svarar för medborgarcertifikat enligt åtagandena i denna certifieringspraxis och i den certifikatpolicy som gäller medborgarcertifikat.

2.3.3 Certifikatutfärdarens ekonomiförvaltning

Ekonomiförvaltningen av de certifikattjänster som tillhandahålls av Befolkningsregistercentralen och övervakningen av tjänsterna regleras särskilt. Befolkningsregistercentralen är ett ämbetsverk som lyder under finansministeriet. Den ekonomiska förvaltningen av ämbetsverket grundar sig på lagar och förordningar som reglerar den statliga ekonomin samt på finansministeriets och Statskontorets föreskrifter. Statens revisionsverk ansvarar för tillsynen av ekonomin. Dessutom beskrivs utfallet av verksamheten utifrån aspekterna effektivitet, lönsamhet och produktivitet.

2.4 Tolkning och verkställighet

2.4.1 Tillämplig lagstiftning

Signeringscertifikat som beviljats med stöd av denna certifieringspraxis ska uppfylla de krav på kvalificerade certifikat som ställs i Europaparlamentets och rådets direktiv om elektroniska signaturer (1999/93/EG).

I lagen om stark autentisering och elektroniska signaturer (617/2009) finns bestämmelser om elektroniska signaturer som är baserade på kvalificerade certifikat. Bestämmelser om ID-kort finns i lagen om identitetskort (829/1999) och bestämmelser om certifikat som beviljas av Befolkningsregistercentralen i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Befolkningsregistercentralens skadeståndsansvar i samband med produktionen av certifikattjänster regleras i skadeståndslagen (412/1974). På Befolkningsregistercentralen tillämpas också kraven i lagen om stark autentisering och elektroniska signaturer (617/2009) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Enligt lagen om kommunikation i myndigheternas verksamhet är det i alltid möjligt att använda kvalificerade certifikat för kommunikationen inom myndighetsförvaltningen..

Befolkningsregistercentralen följer principerna om god sed för behandling av personuppgifter i personuppgiftslagen (523/1999) och god informationshantering i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid Befolkningsregistercentralen tryggas informationssäkerheten bl.a. med hjälp av kontinuerlig utbildning. Befolkningsregistercentralen har också berett uppförandekoder för såväl informations- som certifikattjänster.

Befolkningsregistercentralen får de uppdrag som hänför sig till registrering och identifiering av personer från polisen. I denna verksamhet iakttar Befolkningsregistercentralen bestämmelserna i lagen om samservice inom den offentliga förvaltningen (223/2007).

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

I Finland övervakas utfärdare av kvalificerade certifikat av Kommunikationsverket.

Befolkningsregistercentralen svarar för att medborgarcertifikat som ingår i ID-kort genereras enligt de förfaranden som anges i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, i lagen om stark autentisering och elektroniska signaturer, i lagen om elektronisk kommunikation i myndigheternas verksamhet och i certifikatpolicyn och i enlighet med de uppgifter som certifikatsökanden lämnat.

Befolkningsregistercentralens certifikattjänster övervakas av Kommunikationsverket, som är ett sådant tillsynsorgan som avses i lagen om stark autentisering och elektroniska signaturer och som meddelar föreskrifter och rekommendationer om verksamheten kring kvalificerade certifikat. Därför deltar Befolkningsregistercentralen inte i frivilliga ackrediteringssystem. Befolkningsregistercentralens certifikatverksamhet övervakas av Kommunikationsverket och i fråga om behandlingen av personuppgifter följer Befolkningsregistercentralen personuppgiftslagen och samarbetar fortlöpande med dataombudsmannen.

När det gäller avgörande av besvär och lösning av tvister samt administrativ tillsyn och rättsskipning iakttas gällande lagstiftning. Vid produktionen av kvalificerade certifikat ska i synnerhet lagen om stark autentisering och elektroniska signaturer beaktas.

2.4.2 Lösning av tvister

Vid beviljandet av medborgarcertifikat svarar Befolkningsregistercentralen för att certifikaten uppfyller de krav som ställs i denna certifieringspraxis och i den certifikatpolicy som gäller medborgarcertifikat.

Eventuella meningsskiljaktigheter avgörs i enlighet med Finlands rättsordning. När det gäller avgörande av besvär och lösning av tvister samt administrativ tillsyn och rättsskipning iakttas gällande lagstiftning. Vid produktionen av kvalificerade certifikat ska i synnerhet lagen om stark autentisering och elektroniska signaturer beaktas.

2.5 Avgifter

I detta kapitel specificeras avgifter som hänför sig till användningen av medborgarcertifikat som ingår i ID-kort.

2.5.1 Beviljande och förnyande av medborgarcertifikat

Medborgarcertifikat som ingår i ID-kort ska sökas från polisens serviceställe. Certifikatet beviljas alltid på basis av en ny ansökan med iakttagande av de identifieringsförfaranden som anges i lagen om identitetskort. Priset på ID-kort bestäms enligt gällande förordning av finansministeriet om avgifterna för Befolkningsregistercentralens prestationer.

2.5.2 Avgifter för användning av medborgarcertifikat

Certifikatutfärdaren debiterar inte certifikatinnehavaren särskilt för användningen av certifikaten, spärrtjänsten eller det offentliga registret. Enskilda tillhandahållare av webbaserade tjänster kan ta ut en avgift av dem som använder deras tjänster. Användningen av medborgarcertifikat kräver ingen särskild anmälan eller särskilt tillstånd av utfärdaren.

2.5.3 Avgifter för upptagning av medborgarcertifikat på spärrlista

Anmälan av medborgarcertifikat till en spärrlista är avgiftsfri. Det är också avgiftsfritt att hämta spärrlistor från registret och kontrollera giltighetstiden för medborgarcertifikat mot en spärrlista.

2.5.4 Övriga avgifter

Den som använder en informationstjänst ska betala en särskild avgift enligt gällande prislista.

Om en tjänsteleverantör vill ordna en informationsförsörjningstjänst som omfattar dels koder som individualiserar innehavare av medborgarcertifikat, dels identifikationsuppgifter eller andra uppdateringsdata i det egna bakgrundssystemet, kan leverantören hos Befolkningsregistercentralen ansöka om tillstånd att få lämna ut uppgifter till informationstjänsten. Denna tjänst prissätts enligt lagen om grunderna för avgifter till staten och finansministeriets förordning om avgifterna för Befolkningsregistercentralens prestationer.

2.6 Publicering och åtkomst av uppgifter

2.6.1 Publicering av certifikatutfärdarens uppgifter

Certifikatutfärdaren ska publicera alla medborgarcertifikat och spärrlistor i ett avgiftsfritt, allmänt tillgängligt offentligt register.. Utfärdaren ska publicera certifikatpolicyn, certifieringspraxisen, certifikatbeskrivningen (PDS) och andra offentliga dokument som anknyter till produktionen av certifikattjänster på sina webbsidor.

2.6.2 Publiceringsfrekvens

Medborgarcertifikat publiceras i ett offentligt register genast när de har genererats och de ska finnas kvar i registret under hela giltighetstiden. Certifikatutfärdaren ska publicera en spärrlista som gäller i två timmar från det att den har publicerats. Spärrlistan uppdateras en gång i timmen med en ny spärrlista.

2.6.3 Åtkomst av uppgifter

Register- och spärrlistsuppgifterna är allmänt tillgängliga. De allmänna FINEID-specifikationerna, som publiceras av certifikatutfärdaren, finns på utfärdarens webbsidor. Certifikatpolicyn och certifieringspraxisen finns likaså på utfärdarens webbsidor.

2.6.4 Informationslager

Uppgifter som publicerats av certifikatutfärdaren kan fås från utfärdarens webbsidor. Certifikatsystemets konfidentiella uppgifter finns lagrade i utfärdarens konfidentiella informationslager. Utfärdarens uppgifter arkiveras enligt gällande arkivbestämmelser. Särskild vikt fästs vid behandlingen av personuppgifter. För produktionen av certifikattjänster har Befolkningsregistercentralen gett ut särskilda uppförandekoder som stöder sig på personuppgiftslagen. Med tanke på behandlingen av personuppgifter har utfärdaren också berett en registerbeskrivning för varje delområde i certifikatsystemet enligt bestämmelserna i personuppgiftslagen.

2.7 Granskning av datasäkerheten

Kommunikationsverket, som övervakar dem som utfärdar kvalificerade certifikat, får granska certifikatutfärdarens verksamhet på det sätt som anges i lagen om stark autentisering och elektroniska signaturer.

2.7.1 Granskningsfrekvens

Befolkningsregistercentralen ska granska sina tekniska leverantörers lokaler, utrustning och verksamhet på lämpligt sätt. Granskningar ska göras minst en gång per år och alltid när en ny avtalsperiod inleds. Vid granskningarna tillämpar Befolkningsregistercentralen rutinerna i informationssäkerhetsstandarden ISO/IEC 27001.

Med hjälp av granskningarna utreds om de tekniska leverantörerna följer avtalen med beaktande av kraven i informationssäkerhetsstandarderna. Som regel bedöms de tekniska leverantörerna enligt standarden ISO/IEC 27001 och Kommunikationsverkets föreskrifter.

2.7.2 Granskare

Befolkningsregistercentralens säkerhetsgranskningar utförs av centralens datasäkerhetschef eller av en utomstående granskare som är specialiserad på auditering av tekniska leverantörer av certifikattjänster.

2.7.3 Områden som täcks av granskningen

Granskningsobjekten bestäms i lagen om stark autentisering och elektroniska signaturer eller, om Befolkningsregistercentralen utför granskningen, i informationssäkerhetsstandarden ISO/IEC 27001 i enlighet med Befolkningsregistercentralens datasäkerhetspolicy eller tekniska leveransavtal.

Granskningarna ska genomföras med beaktande av de åtta delområdena inom informationssäkerheten. Till de egenskaper som granskas hör tillförlitlighet, integritet och användbarhet.

Granskningarna omfattar de föreskrifter som Kommunikationsverket meddelat om datasäkerheten i certifikatutfärdarens verksamhet.

Vid granskningarna ställs policyn, certifieringspraxisen och tillämpningsanvisningarna i relation till hela verksamheten i certifikatorganisationen och certifikatsystemet. Befolkningsregistercentralen övervakar att tillämpningsanvisningarna är förenliga med certifikatpolicyn.

Vid granskningarna ska förutom den administrativa informationssäkerheten också beaktas leverantörerna av tjänster, bl.a. enligt följande indelning:

Spärrtjänst:
- kommunikationssäkerhet
- personell säkerhet
- fysisk säkerhet

Certifikatproduktion:
- arbetsfördelning och enskilda uppgifter – personell säkerhet
- fysisk säkerhet
- säkerhet som hänför sig till utfärdarens nycklar
- produktionssystem och reservsystem för certifikaten
- kommunikationssäkerhet

Kortproduktion:
- produktionslinjen som helhet från början till slut
- kvalitetskontroll vid kortproduktionen
- kommunikationssäkerhet
- personell säkerhet
- fysisk säkerhet

Registertjänst:
- använda komponenter
- kontrollförbindelser
- underhåll av registret och åtgärder vid störningar
- personell säkerhet
- kommunikationssäkerhet
- fysisk säkerhet

HelpDesk:
- kommunikationssäkerhet
- personalens kompetens och utbildning
- rutiner för olika hjälpfunktioner

2.7.4 Åtgärder vid avvikelser

Observerade avvikelser ska registreras i granskningsrapporten och uppmärksammas i enlighet med lag, informationssäkerhetsstandarden ISO 27001 och gällande leveransavtal.

2.7.5 Information om resultaten av granskningen

Resultatet av granskningarna meddelas på det sätt som anges i lag, informationssäkerhetsstandarden ISO/IEC 27001, Befolkningsregistercentralens datasäkerhetspolicy och gällande leveransavtal. En detaljerad formbunden redogörelse för resultatet av granskningarna avsedd för internt bruk är konfidentiell information och uppgifterna lämnas inte till allmänheten. Särskilda formbundna rapporter kan upprättas för användning utanför organisationen.

Befolkningsregistercentralen ska informera Kommunikationsverket om resultaten av granskningarna på det sätt som anges i lagen om stark autentisering och elektroniska signaturer och i Kommunikationsverkets föreskrifter och rekommendationer.

2.8 Publicering av uppgifter

2.8.1 Uppgifter som publiceras av certifikatutfärdaren

Uppgifterna i certifikatsystemet är konfidentiella, om de inte grundar sig på bestämmelserna om utlämning av uppgifter i personuppgiftslagen, lagen om offentlighet i myndigheternas verksamhet, lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) eller lagen om stark autentisering och elektroniska signaturer eller är avsedda för syften som anges i utfärdarens certifikatpolicy eller certifieringspraxis.

2.8.2 Offentliga uppgifter

Uppgifterna i det allmänna registret och i spärrlistan är offentliga, likaså certifieringspraxisen och de uppgifter som anges i certifikatpolicyn samt de publicerade FINEID-specifikationerna

2.8.3 Giltighetsperioden för medborgarcertifikat upphör eller avbryts

Giltighetsperioden för medborgarcertifikat anges i certifikatet. Certifikat som spärras mitt under giltighetsperioden publiceras i en offentlig spärrlista.

2.8.4 Uppgifter som ska lämnas till myndigheter

Vilka uppgifter som ska lämnas till myndigheterna bestäms med stöd av gällande lagstiftning.

2.8.5 Övriga uppgifter

Uppgifterna i certifikatsystemet lämnas inte ut för andra syften än för sådana som anges ovan i detta kapitel.

2.8.6 Utlämning av uppgifter på begäran av certifikatinnehavaren

Certifikatinnehavaren har lagstadgad rätt att ta del av uppgifter om sig själv, såsom personuppgifter.

2.8.7 Övriga principer som gäller utlämningen av uppgifter

Med tanke på certifikatutfärdarens trovärdighet är det viktigt att Befolkningsregistercentralen på alla tänkbara sätt ser till att den konfidentiella information som centralen får ta del av i certifikatverksamheten hålls hemlig och att principerna om god informationshantering iakttas, om inte annat följer av myndigheternas rätt att få information om verksamheten inom certifikatsystemet.

Vid behandlingen av personuppgifter ska Befolkningsregistercentralen följa personuppgiftslagen och speciallagstiftningen på området. Befolkningsregistercentralen har berett uppförandekoder för behandlingen av personuppgifter dels i samband med utlämningen av uppgifter, dels inom certifikatverksamheten. Vid behandlingen av personuppgifter ska särskild noggrannhet iakttas.

2.9 Immateriella rättigheter

Enligt de tekniska leveransavtalen har Befolkningsregistercentralen upphovsrätten till alla uppgifter som gäller certifikat och dokumentation. Befolkningsregistercentralen har full ägande- och dispositionsrätt till denna certifieringspraxis.

3 Identifiering av certifikatsökanden

3.1 Registrering

I kapitel 4.1–4.3 beskrivs de förfaranden och processer som ska följas vid identifiering och autentisering av certifikatsökande.

Certifikatsökandes rättigheter och skyldigheter anges i ansökningshandlingen och i de allmänna användarvillkoren vilka tillsammans utgör det avtal som ingås med sökanden. I ansökningshandlingen finns uppgifter om bägge parters rättigheter och skyldigheter.

I ansökningshandlingen och i användarvillkoren ska tydligt anges att den som ansöker om ett medborgarcertifikat med sin signatur bekräftar att de givna uppgifterna är korrekta och att den godkänner att ett medborgarcertifikat skapas och publiceras i ett offentligt register. Samtidigt godkänner sökanden de bestämmelser och villkor som gäller användningen av medborgarcertifikat samt förbinder sig att sörja för förvaringen av certifikatet och tillhörande PIN-koder och anmäla eventuellt missbruk eller förlust av kortet.

Mellan certifikatutfärdaren och registreraren, korttillverkaren och andra leverantörer som är producenter på certifikattjänsternas olika delområden har det ingåtts ett avtal som obestridligen uttrycker alla parters rättigheter, ansvar och skyldigheter.

Den som ansöker om medborgarcertifikat svarar för att alla uppgifter som är av betydelse för certifikatet och som sökanden har lämnat till certifikatutfärdaren eller registreraren är riktiga. Innehavaren av ett medborgarcertifikat får använda certifikatet enbart för avsett syfte.

Vid beviljandet av ett medborgarcertifikat godkänner utfärdaren samtidigt certifikatansökan.

Den som ansöker om ett medborgarcertifikat kan, om den så önskar, lagra sin e-postadress såväl på certifikatet som i befolkningsdatasystemet. E-postadressen införs i både medborgarcertifikatet och

befolkningsdatasystemet i den form som sökanden uppger. E-postadressen i medborgarcertifikatet, liksom övriga data i certifikatet, införs i ett offentligt register. E-postadressen kan inte ändras under certifikatets giltighetstid.

Innehavare av medborgarcertifikat har möjlighet att byta ut de ursprungliga PIN-koderna mot nya koder. Användningen av medborgarcertifikat för elektroniska nättjänster kräver ett kortläsarprogram som kan laddas ner från Befolkningsregistercentralens webbsidor http://www.fineid.fi. Med hjälp av programmet kan certifikatinnehavaren också byta ut PIN-koderna för sitt ID-kort.

Innehavare av medborgarcertifikat ska förhindra att deras privata nycklar och tillhörande PIN-koder används i strid med användarvillkoren genom att ta hand om sitt kort och koderna på det sätt som anges i villkoren.

Om certifikatinnehavaren misstänker att ett medborgarcertifikat används i strid med avtalsvillkoren, ska innehavaren omedelbart anmäla certifikatet till spärrtjänsten.

3.1.1 Namngivningspraxis

.

Befolkningsregistercentralens utfärdare av rotcertifikat är:
CN (Common name) = VRK Gov. Root CA
OU (Organizational unit) = Certifikattjänster
OU (Organizational unit) = Certification Authority Services
O (Organization) = Befolkningsregistercentralen CA
S (State) = Finland
C (Country) = FI

Befolkningsregistercentralens utfärdare av medborgarcertifikat är:
CN (Common name) = VRK Gov. CA for Citizen Qualified Certificates
OU (Organizational unit) = Statens medborgarcertifikat
O (Organization) = Befolkningsregistercentralen CA
S (State) = Finland
C (Country) = FI

Certifikatinnehavarens namngivningspraxis för medborgarcertifikat:
2.5.4.5 (Serial Number) = Elektronisk kommunikationskod

SN (Surnamn) = Efternamn
G (Given name) = Förnamn
CN (Common name) = Efternamn Förnamn Elektronisk kommunikationskod
C (Country) = FI
E (EmailAddress) = e-postadress (valfritt)

Certifikatutfärdarens publika nyckel sparas på utfärdarcertifikatet, i det offentliga registret och på certifikatinnehavarens aktivkort. För visuell identifiering av kortinnehavaren har ID-korten individualiserats med personens fotografi och signaturprov.

Uppgifterna i ett medborgarcertifikat ska entydigt precisera certifikatinnehavaren. Vid behov kan certifikatutfärdaren ta reda på certifikatinnehavarens officiella identitet.

3.1.2 Leverans av privata nycklar till certifikatinnehavaren

Privata nycklar som hör till ett medborgarcertifikat och som genererats i kortets tekniska del överlämnas till certifikatsökanden när certifikatet lämnas ut. Det finns inga kopior av privata nycklar som genererats i den tekniska delen och det är inte heller möjligt att senare göra kopior av dem.

Ett medborgarcertifikat som ingår i ett ID-kort överlämnas till certifikatsökanden enligt överenskommelse med den registrerare som företräder utfärdaren.

Korttillverkaren ska posta de bas- och signaturkoder som är behövs för användningen av certifikatet till den person och adress som anges i ansökan.

3.2 Förnyande av nyckelpar

Publika nycklar i ett medborgarcertifikat och privata nycklar på ett mikrochip kan inte förnyas. För att generera nya nyckelpar krävs ett nytt medborgarcertifikat.

När ett medborgarcertifikat förnyas ska samma rutiner iakttas som vid första ansökan om certifikat.

3.3 Förnyande av nyckelpar efter upptagning på spärrlista

Publika nycklar i ett medborgarcertifikat och privata nycklar på ett mikrochip kan inte förnyas. För att generera nya nyckelpar krävs ett nytt medborgarcertifikat.

När ett medborgarcertifikat förnyas ska samma rutiner iakttas som vid första ansökan om certifikat.

3.4 Identifiering av den som begär spärrning

Innehavaren av ett medborgarcertifikat kan, om den så önskar, begära att få certifikatet spärrat innan giltighetstiden går ut.

Förfarande vid begäran om spärrning
Ett certifikat spärras i första hand av certifikatinnehavaren om denne upptäcker att certifikatet har försvunnit eller misstänker att det kan missbrukas. Begäran om spärrning kan också lämnas exempelvis av korttillverkaren eller registreraren.

Om det finns anledning att misstänka att ett certifikat missbrukas till exempel på grund av att det försvunnit eller blivit stulet, ska certifikatet omedelbart spärras. Medborgarcertifikat kan spärras genom ett samtal till den avgiftsfria allmänna spärrtjänsten +358 800 162 622 eller till texttelefontjänsten för hörselskadade +358 100 2288.

Varje begäran om spärrning, grunderna för spärrningen, hur den som begärt spärrning har identifierats och certifikatutfärdarens åtgärder till följd av begäran ska arkiveras. Samtal som gäller begäran om spärrning spelas in.

Identifiering av den som begär spärrning
Den som begär spärrning identifieras genom kontroll av uppringarens personliga uppgifter. Om den som ringer samtalet inte är innehavare av det certifikat som ska spärras, ska såväl uppringaren som certifikatinnehavaren identifieras.

Utifrån certifikatinnehavarens identifikationsuppgifter är det möjligt att få fram uppgifter som individualiserar certifikatet och möjliggör begäran om spärrning.

Om begäran om spärrning lämnas av registreraren eller korttillverkaren, ska identifieringen genomföras på det sätt som beskrivs i kapitel 4.4.3.

Spärrtjänsten meddelar den som begärt spärrning under samtalets gång om begäran om spärrning har lyckats.

Om den som begär spärrning av ett medborgarcertifikat som överlämnats till en certifikatinnehavare inte är innehavare av certifikatet och begäran om spärrning inte beror på att innehavaren kontaktat certifikatutfärdaren eller registreraren, ska innehavaren meddelas också per brev om spärrningen av certifikatet.

4 Funktionella krav

4.1 Ansökan om certifikat

Certifikatsökandes rättigheter och skyldigheter anges i ansökningshandlingen och i de allmänna anvisningar som lämnas till användaren innan ansökan undertecknas. Tillsammans bildar dessa det avtal som ingås med certifikatsökanden. I ansökningshandlingen finns uppgifter om bägge parters rättigheter och skyldigheter. Vid ansökan om medborgarcertifikat godkänner sökanden samtidigt de allmänna användarvillkoren.

I ansökningshandlingen och i anvisningarna ska tydligt anges att certifikatsökanden genom signeringen bekräftar att de givna uppgifterna är korrekta och godkänner att ett certifikat skapas och publiceras i ett offentligt register. Samtidigt godkänner sökanden de bestämmelser och villkor som gäller användningen av medborgarcertifikat samt förbinder sig att sörja för förvaringen av certifikatet och tillhörande PIN-koder och anmäla eventuellt missbruk eller förlust av certifikaten/ID-kortet.

Mellan certifikatutfärdaren och registreraren, korttillverkaren och andra leverantörer som är producenter på certifikattjänsternas olika delområden ingås ett avtal som obestridligen uttrycker alla parters rättigheter, ansvar och skyldigheter.

Ansökan om medborgarcertifikat görs vid ett personligt besök hos den polismyndighet som är registrerare eller hos någon annan registreringsinstans. I samband med ansökan ska personen styrka sin identitet med ett identitetsbevis som har utfärdats av polisen. Dessa är ID-kort och pass. Godkända identifikationsdokument är också ett giltigt pass eller ID-kort som har beviljats av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet, Schweiz eller San Marino och ett giltigt pass som beviljats av en myndighet i någon annan stat. Om sökanden inte har något av de ovan

nämnda dokumenten, kan polisen styrka identiteten på annat sätt. Identifieringssättet antecknas i ansökningsblanketten och en funktionär vid registreringsinstansen bestyrker med sin underskrift att personen har identifierats.

De uppgifter som personen uppger jämförs med Befolkningsregistercentralens uppgifter.

4.2 Beviljande av certifikat

Genom att godkänna ansökan om medborgarcertifikat beviljar certifikatutfärdaren certifikatet. Genom att bevilja certifikatet svarar utfärdaren för att datainnehållet är korrekt när certifikatet lämnas ut.

4.3 Mottagande av certifikat

Ett medborgarcertifikat kan hämtas personligen från registreringsinstansen.

När certifikatet lämnas ut uppmärksammas certifikatsökanden om att det inte finns och inte heller senare är möjligt att göra kopior av de privata nycklarna.

Certifikatinnehavaren kan gå in på Befolkningsregistercentralens webbsidor och ladda ner ett kortläsarprogram med vilket medborgarcertifikatet kan användas vid elektronisk kommunikation.

4.4 Giltighetsperiod för medborgarcertifikat

4.4.1 Förutsättningar för spärrning av certifikat

Ett medborgarcertifikat ska upptas på en spärrlista, om det finns anledning att misstänka missbruk till exempel på grund av att certifikatet har försvunnit eller blivit stulet. Medborgarcertifikat kan spärras genom ett samtal till den avgiftsfria spärrtjänsten. Begäran om spärrning ska göras omedelbart vid misstanke om missbruk.

Certifikatinnehavaren svarar för att de privata nycklarna och tillhörande PIN-koder används enligt användarvillkoren genom att skydda sitt ID-kort och koderna på det sätt som anges i villkoren.

4.4.2 Behörig att begära spärrning av certifikat

Begäran om spärrning av ett medborgarcertifikat görs i första hand av certifikatinnehavaren. Om den som ringer samtalet inte är innehavare av det certifikat som ska spärras, ska såväl certifikatinnehavaren som uppringaren identifieras.

Begäran om spärrning kan också göras av korttillverkaren eller registreraren. Den metod som används för att identifiera personen som begär spärrning av certifikatet ska registreras.

Grunderna och tidpunkten för spärrningen samt uppgifter om den som utfört spärrningen ska sparas.

4.4.3 4Förfarande vid spärrning

Ett medborgarcertifikat kan spärras på följande sätt:

a) Genom ett samtal till spärrtjänsten

b) Genom ett besök hos registreraren

Uppgiften om att ett medborgarcertifikat har upptagits på en spärrlista ska vara offentligt tillgänglig senast en timme efter att begäran om spärrning har konstaterats vara giltig och godkänts. Spärrlistan gäller i två timmar.

1. Indragning av ID-kort

Polisen drar alltid in ett ID-kort när kortinnehavaren begär det. ID-kort som beviljats minderåriga dras också in om vårdnadshavaren tar tillbaka sitt samtycke. Ett ID-kort får dras in om det har försvunnit, stulits, förstörts, anteckningarna på kortet har ändrats eller det används obehörigt av någon annan än den som beviljats kortet. Ett ID-kort får också dras in om de uppgifter som är avsedda för medborgarcertifikatet har ändrats. För att spärra certifikat under kortens giltighetstid ska polisen anmäla indragna kort till spärrtjänsten och efter att giltighetstiden har gått ut alltid när kort har försvunnit eller stulits. Kortinnehavare som före indragningen vill göra en spärranmälan för att spärra certifikatet ska själva lämna anmälan till spärrtjänsten.

2. Andra sätt att förhindra användning av medborgarcertifikat

Kortinnehavaren ansvarar för spärrningen av ett medborgarcertifikat. Ett medborgarcertifikat som beviljats av Befolkningsregistercentralen kan efter anmälan från kortinnehavaren upptas på en spärrlista och får då inte längre användas. Däremot får eventuella andra tillämpningar på kortets tekniska plattform fortfarande användas på avsett sätt. Även om användningen av medborgarcertifikatet förhindras, får ett ID-kort fortfarande användas som ID-kort och som resedokument för finska medborgare.

Ett medborgarcertifikat kan spärras genom ett samtal till spärrtjänstnumret. Certifikatinnehavarens ansvar upphör efter att en individualiserande anmälan som möjliggör spärrning har tagits emot. Samtidigt upphör certifikatinnehavarens ansvar för användningen av certifikatet. Vid behov kan anmälan göras också av en annan person, varvid personens identitet ska fastställas liksom dennes relation till innehavaren av det ID-kort som ska dras in.

Spärrtjänsten meddelar den som begärt spärrning under samtalets gång om begäran om spärrning har lyckats.

Om den som begär spärrning av ett medborgarcertifikat som överlämnats till en certifikatinnehavare inte är innehavare av certifikatet och begäran om spärrning inte beror på att innehavaren kontaktat certifikatutfärdaren eller registreraren, ska innehavaren meddelas också per brev om spärrningen av certifikatet.

Spärrade certifikat kan inte åter tas i användning.

3. Användningen av ID-kort som ID-kort och resedokument för finska medborgare förhindras

Kortinnehavaren kan göra en anmälan till polisen om personens ID-kort har försvunnit eller stulits. Polisen gör en anteckning om anmälan i sitt ID-kortregister och kortet godkänns inte längre som ID-kort eller som resedokument. Samtidigt ska polisen också anmäla medborgarcertifikatet i kortets tekniska del till en spärrlista. När kortinnehavaren meddelat polisen om att kortet har upphittats, gör polisen en anteckning om detta i ID-kortregistret. Efter att denna anteckning har införts godkänns ID-kortet som ID-kort eller som resedokument för finska medborgare.

När personen får ett nytt ID-kort, klipper polistjänstemannen bort en bit av det utgångna kortets nedre högra hörn där fotografiet sitter. Innehavaren får dock använda ett kort som på detta sätt gjorts odugligt för att hantera sina krypterade dokument och filer och fortfarande utnyttja eventuella tillämpningar och uppgifter som personen själv har lagrat på kortet

4. Spärrning av certifikat på initiativ av Befolkningsregistercentralen

Befolkningsregistercentralen spärrar alltid medborgarcertifikat när centralen fått uppgifter om att certifikatinnehavaren har avlidit. Befolkningsregistercentralen lämnar i sådana fall ett meddelande om spärrningen till den avlidnes rättsinnehavare.

Befolkningsregistercentralen får spärra medborgarcertifikat som den har signerat med sin privata nyckel, om det finns anledning att misstänka att centralens privata nycklar har röjts eller hamnat i orätta händer.

Befolkningsregistercentralen spärrar certifikat som centralen beviljat, om den upptäcker fel i certifikatets datainnehåll.

Alla giltiga certifikat som har beviljats med den röjda nyckeln ska upptas i en eller flera spärrlistor för vilka giltighetstiden inte går ut förrän giltighetstiden för det sista spärrade certifikatet har gått ut.

Om de privata nycklar eller andra tekniska förfaranden som Befolkningsregistercentralen har använt för genereringen av sina certifikat har röjts eller på annat sätt blivit obrukbara, ska Befolkningsregistercentralen på lämpligt sätt meddela alla kortinnehavare och Kommunikationsverket om det som har hänt.

Befolkningsregistercentralen kan av särskilda skäl spärra certifikat.

4.4.4 Tidpunkt för spärrning

Ett medborgarcertifikat ska spärras genast vid begäran om spärrning.

4.4.5 Krav som gäller avbrytande av giltighetsperioden

Giltighetsperioden för medborgarcertifikat kan inte avbrytas tillfälligt. Spärrade medborgarcertifikat kan inte åter tas i användning.

4.4.6 Behörig att begära avbrytande

Giltighetsperioden för medborgarcertifikat kan inte avbrytas tillfälligt.

4.4.7 Förfarande vid begäran om avbrytande

Giltighetsperioden för medborgarcertifikat kan inte avbrytas tillfälligt.

4.4.8 Begränsningar som gäller avbrytande

Giltighetsperioden för medborgarcertifikat kan inte avbrytas tillfälligt.

4.4.9 Publiceringsfrekvens för spärrlista

Uppgiften om att ett medborgarcertifikat har upptagits på en spärrlista ska vara allmänt tillgänglig senast en timme efter att begäran om spärrning har konstaterats vara giltig och godkänts. Spärrlistan gäller i två timmar.

I spärrlistan ska anges tidpunkten för publiceringen av nästa spärrlista.

En ny spärrlista ska publiceras senast när giltighetstiden för den aktuella spärrlistan går ut.

Vid systemuppdateringar och andra liknande avvikande situationer kan BRC publicera spärrlistor med varierande periodicitet och förlängda giltighetstider.

4.4.10 Kontrollkrav för spärrlista

Förlitande parters skyldigheter beskrivs i kapitel 2.1.4

4.4.11 Kontroll i realtid av certifikatstatus

Tills vidare kan certifikatutfärdaren inte erbjuda kontroll i realtid av certifikatstatus, dvs. OCSP-service. Utfärdaren publicerar spärrlistor över spärrade certifikat.

4.4.12 Krav som gäller kontroll i realtid av certifikatstatus

Tills vidare kan certifikatutfärdaren inte erbjuda kontroll i realtid av certifikatstatus..

4.4.13 Särskilda krav som gäller certifikatinnehavarens privata nyckel

Till certifikatinnehavarens skyldigheter hör att skydda användningen av sina privata nycklar genom att hantera mikrochipet eller kortet och koderna på det sätt som anges i användarvillkoren. Vid misstanke om att ett medborgarcertifikat används i strid med avtalsvillkoren ska certifikatinnehavaren omedelbart anmäla certifikatet till spärrlistan.

4.5 Övervakning av systemet

För övervakningen av systemet ska certifikatutfärdaren spara logguppgifter om händelser som gäller certifikatproduktion, hantering av certifikatsystemets användarrättigheter, konfiguration av enheter, systemprogram och applikationer inklusive ändringar samt säkringar och återställningar av dem. Utfärdaren ska också bevaka dokument som hänför sig till verksamheten. Observerade avvikelser ska rapporteras på avtalat sätt.

4.6 Arkivering av certifikatuppgifter

4.6.1 Material som ska lagras

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten att ta del av uppgifter regleras i lagen om offentlighet i myndigheternas verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i 10 år från det att giltighetstiden för certifikaten har gått ut. Certifikatutfärdaren ska arkivera följande uppgifter:

a) Ansökningsblankett som undertecknats av sökanden samt verifikat över att ID-kortet och anknytande allmänna användarvillkor har tagits emot.
b) Uppgifterna i ID-kort som beviljats av polisen förs in i polisens register över ID-kort för vilket polisen har ansvaret.
c) Beviljade medborgarcertifikat, deras datainnehåll och tilläggsuppgifter om certifikatens livscykel från det att deras giltighetstid har gått ut eller från det att certifikaten har spärrats.
d) Händelser som gäller generering och förnyelse av certifikatutfärdarens privata nyckel.
e) Uppgifter om begärda spärrningar av medborgarcertifikat.
f) Spärrlistor som har skickats till det offentliga registret och andra uppgifter som gäller spärrningar av medborgarcertifikat.
g) Giltiga och tidigare publicerade certifikatpolicier och anknytande certifieringspraxis.
h) Åtgärder som har vidtagits av de systemadministratörer som har registrerats som användare av systemet och av systemanvändare ska sparas i loggfilerna.
i) Granskningsrapporter och protokoll från säkerhetsgranskningar och auditeringar av systemet.

Arkivuppgifter ska förvaras enligt bestämmelserna om myndigheter som utfärdar certifikat.

4.6.2 Skydd av arkiv

Dokument som ska arkiveras och som gäller ansökningar om ID-kort, identifiering av personer och utlämning av kort förvaras av polisen i ändamålsenliga lokaler.

Arkivuppgifter ska förvaras i lokaler med hög säkerhetsnivå och åtkomstkontroll.

4.6.3 Rutiner för säkring av arkivmaterial

Säkerhetskopior ska förvaras fysiskt åtskilda från originaluppgifterna.

4.6.4 Metoder för åtkomst och säkring av arkivmaterial

Om certifikatutfärdarens verksamhet avbryts eller upphör ska utfärdaren underrätta alla kunder om att arkivet fortfarande är tillgängligt. Alla förfrågningar som gäller arkiverad information ska skickas till utfärdaren eller till en instans som utfärdaren har uppgett innan verksamheten upphörde.

Certifikatutfärdaren ska försäkra sig om arkivens tillgänglighet och läsbarhet också i sådana fall att verksamheten avbryts eller upphör.

Informationen i arkivet får lämnas ut om det är motiverat med tanke på certifikatinnehavare eller förlitande parter.

4.7 Kontinuiteten i verksamheten och hantering av exceptionella situationer

Befolkningsregistercentralen har en kontinuitets- och beredskapsplan som möjliggör kontinuitet i centralens verksamhet.

4.7.1 Certifikatutfärdarens privata nyckel har röjts eller utfärdarcertifikatet spärrats

I varje certifieringspraxis ska certifikatutfärdaren ange de åtgärder som certifikatinnehavare, förlitande parter samt anställda hos registrerare och certifikatutfärdare ska vidta, om utfärdarens privata nyckel röjs eller på annat sätt blir oanvändbar.

I sådana fall ska certifikatutfärdaren antingen upphöra med sin verksamhet på det sätt som anges under 4.8 eller vidta följande åtgärder:

a) Utfärdaren underrättar alla certifikatinnehavare, förlitande parter och kunder som utfärdaren har ingått avtal med eller som annars till följd av avtalsförhållande eller myndighetsverksamhet står i en sådan relation till utfärdaren att denne är skyldig att informera dem om vad som har skett.
b) Utfärdaren genererar en ny nyckel enligt kapitel 6.
c) Alla beviljade och giltiga certifikat som har beviljats med den röjda nyckeln upptas på en eller flera spärrlistor för vilka giltighetstiden inte går ut förrän giltighetstiden för det sista spärrade certifikatet har gått ut.
d) Utfärdaren arkiverar de uppgifter som avses i 38 § i lagen om stark autentisering och elektroniska signaturer för den tid som anges i lagen och följer även i övrigt arkivlagens bestämmelser om arkivering.

4.7.2 Säkerheten vid naturkatastrofer eller andra allvarliga avbrott

I Befolkningsregistercentralens säkerhetspolicy har de åtgärder beaktats som ska vidtas om den yttre säkerheten hotas. Befolkningsregistercentralen har beviljats informationssäkerhetscertifikatet ISO 27001 som ställer krav på centralens verksamhet också efter eventuella katastrofer. Vid beviljande och underhåll av medborgarcertifikat ska Befolkningsregistercentralen följa de rutiner som iakttas inom informationssäkerheten.

4.8 Certifikatutfärdarens verksamhet upphör

Om alla tjänster som hänför sig till certifikatutfärdarens beviljande av certifikat upphör permanent, anses utfärdarens verksamhet ha upphört. Verksamheten anses inte ha upphört om certifikattjänsten överförs från en organisation till en annan.

Utfärdaren ska så snabbt som möjligt meddela de instanser om anges under punkt a) i kapitel 4.8 om att certifikattjänsterna upphör, dock minst en månad före upphörandet.

Innan verksamheten upphör ska åtminstone följande åtgärder vidtas:

a) Alla beviljade och giltiga certifikat ska upptas på en eller flera spärrlistor vilkas giltighetstid inte går ut förrän giltighetstiden för det sista spärrade certifikatet har gått ut.

b) Utfärdaren ska dra in alla sina avtalsparters fullmakter att för utfärdarens räkning utföra uppgifter som ingår i beviljandet av certifikat.

c) Utfärdaren ska försäkra sig om att den åtkomst av utfärdarens arkiv som avses i 4.6 kvarstår också efter att utfärdarens verksamhet har upphört.

d) Utfärdaren ska sköta arkiveringen av de uppgifter som avses i 38 § i lagen om stark autentisering och elektroniska signaturer och även i övrigt iaktta arkivlagens bestämmelser om arkivering av uppgifter.

5 Fysiska, funktionella och personorienterade krav på säkerheten

Befolkningsregistercentralen har beviljats ett datasäkerhetscertifikat som garanterar att informationssäkerheten vid BRC uppfyller kraven i standarden ISO/IEC 27001.

Befolkningsregistercentralen anlitar tekniska leverantörer för datatekniska uppgifter som gäller certifikattjänsterna. Som utfärdare ska Befolkningsregistercentralen på ändamålsenligt sätt svara för säkerheten och verksamheten inom produktionen av certifikat på alla dess delområden.

Vid Befolkningsregistercentralen tillämpas principen om god informationshantering. Befolkningsregistercentralens enhet för certifikattjänster svarar för tjänster som gäller tillhandahållandet av certifikat.

5.1 Fysisk säkerhet

Befolkningsregistercentralen har beviljats ett datasäkerhetscertifikat som garanterar att informationssäkerheten vid BRC uppfyller kraven i standarden ISO/IEC 27001. Befolkningsregistercentralen anlitar tekniska leverantörer för datatekniska uppgifter som gäller certifikattjänsterna. Som utfärdare ska BRC på lämpligt sätt svara för säkerheten och verksamheten inom produktionen av certifikat på alla dess delområden.

5.1.1 Lokaler och deras egenskaper

Certifikatutfärdarens system är placerade i datorhallar med hög säkerhetsnivå. Lokalerna ska uppfylla kraven i de anvisningar och föreskrifter som gäller säkerheten i datorcentraler.

Lokalsäkerheten tillgodoses genom att obehöriga förhindras tillträde till lokalerna. Lokalerna har effektiva låssystem och är stabilt byggda med tillräcklig hållfasthet. I datorhallarna har man undvikit onödiga fönster och för konstruktionen har man valt hållbara byggmaterial.

5.1.2 Fysiskt tillträde till lokalerna

Lokaler där det utförs produktion av certifikattjänster ska ha passagekontroll. Systemet för passagekontroll registrerar såväl lovlig som olovlig passage. För tillträde till datorhallarna krävs autentisering av personen i fråga, varvid personen identifieras, tillträdesrätten kontrolleras och händelserna registreras. Datorhallarna bevakas dygnet runt.

5.1.3 Strömförsörjning och ventilation

Datorhallarna ska ha ändamålsenlig ventilation. I fastigheterna ska finnas beredskap för okontrollerade strömavbrott i form av reservkraftslösningar.

5.1.4 Brandsäkerhet

I datorhallarna ska finnas nödvändiga larmanordningar som varnar för brand, erforderlig utrustning för inledande släckning samt automatiska släckningssystem.

5.1.5 Förvaring av information

Den information som ska arkiveras och säkerhetskopiorna ska förvaras fysiskt åtskilt från certifikatutfärdarens utrustning. Informationen är skyddad mot förlust, ändring och olovlig användning.

5.1.6 Hantering av obehövligt informationsmaterial

Säkerhetsklassificerat utgallrat informationsmaterial ska förstöras på ett säkert sätt.

5.1.7 Vattenskador

I datorhallarna ska finnas ändamålsenliga givare som känner av fukt.

5.1.8 Reservrutiner

Skyddet för utrustningens del har tillgodosetts enligt principen om god informationshantering. Om systemet sviker, kan ett reservsystem tas i bruk utan att konfidentialiteten, integriteten och användbarheten äventyras när det gäller den information som ingår i systemet.

I fråga om reservdelar till viktig utrustning har tillgången och servicen tryggats.

5.2 Funktionella krav

5.2.1 Ansvarsfördelning

Befolkningsregistercentralen anlitar tekniska leverantörer för registreringsuppgifter och datatekniska uppgifter inom certifikatproduktionen. Som certifikatutfärdare svarar Befolkningsregistercentralen för certifikatverksamheten.

Utfärdarens uppgifter har indelats i följande ansvarsområden:
Datasäkerhetsansvarig
Registreringsansvarig
Systemadministratör
Användare av systemet
Övervakare av systemet

Certifikatutfärdaren och de tekniska leverantörerna har ingått ett leveransavtal där leverantörernas uppgifter, metoder, ansvar och säkerhetsrutiner beskrivs i detalj.

5.2.2 Krav på antal personer per uppgift

Generering, aktivering, säkerhetskopiering och återvinning av certifikatutfärdarens privata nyckel ska ske i närvaro av två sådana personer som är betrodda att administrera systemet. Likaså kan utfärdarens privata nyckel återkallas bara under övervakning av två personer i betrodda roller. Vid initieringen av säkerhetsmodulen till utfärdarens privata nyckel ska minst två personer som är betrodda att administrera systemet vara närvarande.

Användningen av systemet kräver en betrodd persons närvaro.

Registreringen av medborgarcertifikat som ingår i ID-kort och identifieringen i samband med det kräver att en person är närvarande. Uppgiften utförs av polisen.

5.2.3 Identifiering enligt uppgift

Registrerare av medborgarcertifikat som ingår i ID-kort:
Registrerare är polisen med stöd av ett s.k. samserviceavtal

Administratörer av certifikatsystemet:
Identifieras med ett personligt kontrollkort som är avsett för administration av systemet. Systemadministratörer är CA-leverantörernas systemexperter samt personer som Befolkningsregistercentralen bemyndigat för uppgiften.

Användare av certifikatsystemet:
Identifieras med ett personligt ID-kort som är avsett för användningen av systemet. Systemanvändare är datoroperatörer, initierare av tekniska certifikatsökningar samt spärrtjänsten.

5.3 Personorienterad säkerhet

Som certifikatutfärdare svarar Befolkningsregistercentralen för certifikatverksamheten. De tekniska leverantörerna har anlitats efter konkurrensutsättning och utför sina uppgifter under Befolkningsregistercentralens ansvar och för dess räkning.

Personalen vid Befolkningsregistercentralens certifikattjänster förväntas ha den utbildning som krävs för arbetsuppgifterna och kännedom om certifikatverksamhet. Experter följer kontinuerligt utvecklingen på området i Finland och i Europa samt utför expertuppgifter på området.

I samband med konkurrensutsättningen gör certifikatutfärdaren en bedömning av kompetensen hos nyckelexperter och anställda hos de tekniska leverantörerna och deras förutsättningar att utföra certifikattjänster. De tekniska leverantörerna upprätthåller och utvecklar personalens kompetens när det gäller utrustning, program och metoder som används inom serviceproduktionen samt i fråga om informationssäkerheten. Dessutom ser de till att personalen är insatt i de databehandlingsuppgifter som ingår i certifikattjänsten på det sätt som tjänsten kräver.

5.3.1 Kontroll av personalens bakgrund

Befolkningsregistercentralen låter utföra grundläggande säkerhetskontroller av sin personal och av de personer bland de tekniska leverantörerna som arbetar med certifikatsystemet. Kontrollerna utförs av skyddspolisen. Befolkningsregistercentralen förbehåller sig rätten att inte godkänna en anställd hos den tekniska leverantören för uppgifter som utförs inom certifikatsystemet.

5.3.2 Kontrollrutiner

Personalens arbetserfarenhet kartläggs vid anställningen. De anställda får genomgå en grundläggande säkerhetskontroll utifrån uppgifter som de har lämnat på en blankett som skickas till skyddspolisen.

Alla personer som utför centrala uppgifter för certifikatutfärdare, producenter av certifikattjänster och registertjänster, spärrtjänst och korttillverkare ska:

- fylla i en blankett som skickas till skyddspolisen och genomgå en grundläggande säkerhetskontroll som baserar sig på uppgifterna i blanketten
- avstå från sådana uppgifter som står i strid med deras åtaganden och ansvar
- veterligen aldrig ha befriats från någon tidigare uppgift på grund av de försummat eller brutit mot sina skyldigheter
- ha lämplig utbildning för sina uppgifter.

5.3.3 Krav som gäller utbildning

Befolkningsregistercentralens anställda ska ha en sådan utbildning som gör att de kan sköta sina uppgifter på bästa möjliga sätt. Befolkningsregistercentralen har en utbildningsplan, och för genomförandet av den svarar centralens förvaltningsenhet.

5.3.4 Sakkunskap och kompetens

Personalens utbildning ska utformas och uppdateras så att den sakkunskap som behövs för att utföra en uppgift alltid är på bästa möjliga nivå med tanke på uppgiften.

5.3.5 Krav som gäller arbetsrotation

För att arbetsrotation ska kunna tillämpas på uppgifterna hos en certifikatutfärdare måste uppgifterna organiseras så att personen kan sköta sina nya uppgifter på bästa möjliga sätt. När arbetsrotationen genomförs är det viktigt att beakta bl.a. de krav som informationssäkerheten ställer, möjligheterna att trygga konfidentialiteten och principen om god sed vid behandlingen av personuppgifter, vilka beskrivs i Befolkningsregistercentralens uppförandekoder för behandling av personuppgifter.

Också inom arbetsrotationen tillämpas Befolkningsregistercentralens policy och plan för informationssäkerhet samt centralens övriga allmänna anvisningar.

5.3.6 Åtgärder vid avvikelser

Befolkningsregistercentralens personal utför sina uppgifter under tjänsteansvar och enligt centralens interna anvisningar. Tjänstemännens ställning regleras i statstjänstemannalagen (750/1994).

5.3.7 Personal som företräder organisationen

Vid rekryteringen av personal är det viktigt att se till att personalens kunskaper och färdigheter uppfyller de krav som ställs på uppgiften och att det av kontrollen av personens bakgrund inte framgår något sådant som gör att personens uppgifter står i strid med produktionen av certifikattjänster.

5.3.8 Dokument som personalen har tillgång till

Personalen har alltid tillgång till Befolkningsregistercentralens kvalitets- och säkerhetsdokument.

6 Teknisk säkerhet

6.1 Generering och lagring av nyckelpar

6.1.1 Generering av nyckelpar

Generingen av nycklar grundar sig på ett inmatat slumptal som är tillräckligt långt och som har skapats så att det är omöjligt att genom uträkning spåra talet, även om man känner till när och med vilken maskinvara talet har skapats. Dessutom ska den algoritm och den metod som används för genereringen av slumptalet uppfylla kvalitetskraven, bl.a. att algoritmen är tillförlitlig, att genereringsmetoden inte är upprepbar och att talet är ett verkligt slumptal. Utfärdaren avslöjar inte vilken noggrannhet och metod som har tillämpats för beräkningen av sannolikheten.

Certifikatutfärdaren:

Utfärdaren genererar sina privata nycklar för signering och publika nycklar som motsvarar signeringsnycklarna. Nycklarna förvaras i säkerhetsmoduler som administreras av utfärdaren. Dessa ska uppfylla säkerhetskraven enligt nivå 3 i FIPS 140-1.

Certifikatinnehavaren:
Generingen av nycklarna kan göras antingen som satsvis bearbetning före certifieringen eller direkt i samband med certifieringen. I bägge fallen ska den privata nyckeln förvaras läs- och skrivskyddat på ett ID-kort.

Utfärdaren genererar certifikatinnehavarens nycklar med ID-kortets mikrochip. Det görs inga kopior av de privata nycklarna.

6.1.2 Överlämnande av privat nyckel till certifikatsökanden

Det ID-kort som innehåller certifikatsökandes privata nycklar och de ursprungliga PIN-koder som behövs för aktiveringen av kortet ska inte samtidigt befinna sig på samma plats innan och när de överlämnas till sökanden. Detta görs så att kortet och PIN-koderna levereras via olika kanaler och vid olika tidpunkter.

Ett medborgarcertifikat som ingår i ett ID-kort ska överlämnas till certifikatsökanden enligt överenskommelse med den registrerare som företräder utfärdaren.

6.1.3 Leverans av certifikatinnehavarens publika nyckel till utfärdaren

De publika nycklarnas integritet ska skyddas ända fram till certifieringen. Efter genereringen av nycklarna lämnar korttillverkaren en certifikatbegäran till certifikatsystemet. I begäran ska ingå uppgifter om den publika nyckeln och övriga certifikatuppgifter. Kommunikationen mellan det system som används för certifikatbegäran och systemet för generering av certifikat ska krypteras och de personer som initierar systemet för certifikatbegäran identifieras med hjälp av kontrollkort som har beviljats av certifikatutfärdaren.

6.1.4 Distribution av utfärdarens publika nyckel till certifikatinnehavaren

Certifikatutfärdarens publika nyckel finns på utfärdarcertifikatet som lagras på ID-kortet. Utfärdarcertifikaten får spridas fritt och finns också i det offentliga registret och på utfärdarens webbsidor.

6.1.5 Nyckelstorlek

Certifikatutfärdarens privata nyckel som används för signering av medborgarcertifikat och den publika nyckel som motsvarar den privata nyckeln är 2048-bitars RSA-nycklar.

Certifikatinnehavarens privata och publika nycklar är 1024-bitars RSA-nycklar och efter den 1 december 2010 kan de också vara 2048-bitars RSA-nycklar.

6.1.6 Nycklarnas användningsområden

Det fält i certifikatets datainnehåll som bestämmer användningsområde avgör användningsområdet för den nyckel som hänför sig till certifikatet (till exempel autentisering, kryptering av information eller elektroniska signaturer). Användningen av nyckeln är begränsad bara till dess användningsområde. En nyckel som är avsedd för elektroniska signaturer får således användas bara för detta syfte, inte exempelvis för autentisering och kryptering av information.

Certifikatutfärdarens certifikat:
Användningsområde: Signering av certifikat och spärrlistor. Den tekniska beskrivningen finns i specifikationerna FINEID S2.

Certifikatinnehavarens autentiserings- och krypteringscertifikat:
Användningsområde: Autentisering av elektronisk identitet eller kryptering av information.

Certifikatinnehavarens signeringscertifikat:
Användningsområde: Elektroniska signaturer

6.2 Skydd av privata nycklar

6.2.1 Standarder för säkerhetsmoduler

Certifikatutfärdarens privata nycklar förvaras i säkerhetsmoduler som administreras av utfärdaren och som uppfyller kraven på nödvändig säkerhetsstandard.

Utfärdaren svarar för att de privata nycklarna är skyddade mot exponering och obehörig användning. För att tillgodose kraven på säkring av kritisk information tas en säkerhetskopia av utfärdarens privata nycklar.

6.2.2 Personal som deltar i hanteringen av utfärdarens privata nyckel

Vid genereringen av privata nycklar ska minst två personer samtidigt närvara eller aktivera åtgärden.

6.2.3 Utlämning av privat nyckel till betrodd part

Certifikatutfärdarens privata nycklar får inte överföras eller kopieras.

6.2.4 Säkerhetskopiering av privata nycklar

Certifikatutfärdarens privata nycklar och deras säkerhetskopior förvaras omsorgsfullt krypterade i anordningar som tillgodoser kraven på säkring av kritisk information.

6.2.5 Arkivering av privata nycklar

Certifikatutfärdarens privata nycklar förvaras i säkerhetsmoduler som administreras av utfärdaren.

6.2.6 Hantering av privata nycklar i säkerhetsmoduler

Certifikatutfärdarens privata signeringsnycklar skyddas genom fysiska och logiska säkerhetsåtgärder med hög tillförlitlighet. De får bara användas i system som är placerade i en säker miljö. Användningen av nycklarna övervakas med hjälp av särskilda kontrollkort som är skyddade mot obehörig användning.

Personer i betrodda roller inom CA-systemet har kontrollkort som är skyddade med en PIN-kod. Personens rätt att använda certifikatsystemet eller andra system som anknyter till certifiering verifieras med hjälp av dessa kort.

När användningen av utfärdarens nyckel upphör, ska nyckeln förstöras så att den inte längre kan användas eller återskapas. Samtidigt ska säkerhetskopiorna av nyckeln förstöras. De metoder som används för att förstöra defekta anordningar är utformade så att privata nycklar kan förstöras på ett tillförlitligt sätt (genom tillräckligt många överskrivningar) oberoende av om lagringen av nycklarna är baserad på anordningar eller program.

6.3 Andra aspekter på nyckelhantering

6.3.1 Arkivering av publika nycklar

Certifikatutfärdaren arkiverar alla sina certifierade publika nycklar.

6.3.2 Publika och privata nycklars livslängd

Giltighetstiden för medborgarcertifikat som ingår i ID-kort är fem år. Certifikatet kan spärras under sin giltighetstid. Signeringscertifikat får användas för att styrka en signaturs riktighet efter att certifikatet har gått ut eller spärrats, om den verifierade signaturen har skapats innan certifikatet spärrades eller gick ut.

6.4 Aktiveringsdata

6.4.1 Generering och installation av aktiveringsdata

Korttillverkaren genererar de aktiveringsdata, dvs. PIN-koder, som gör det möjligt att använda nycklarna. De individuella PIN- och PUK-koderna fastställs och överförs till kortet och i krypterad form till en datafil innan de överförs till korttillverkarens produktionssystem. Efter att korten har levererats, överförs de krypterade PIN- och PUK-koderna till en avdelning som avskiljts från korttillverkningen, där breven med PIN- och PUK-koder skrivs ut. PIN-koderna skickas efter en överenskommen tid efter leveransen av korten till den adress som sökanden uppgett i kortansökan.

6.4.2 Skydd av aktiveringsdata

PIN-koderna har skyddats så att de inte kan läsas eller kopieras från kortet. Certifikatinnehavaren ansvarar för användningen av nycklarna genom att skydda sitt ID-kort och koderna på det sätt som anges i användarvillkoren.

6.4.3 Andra aspekter på aktiveringsdata

Innehavare av medborgarcertifikat ska informeras om möjligheten att byta ut de ursprungliga PIN-koderna mot nya koder. Kortinnehavare har avgiftsfri tillgång till ett program för byte av PIN-kod på adressen www.fineid.fi.

PIN-koden låses och användningen av det certifikat som ingår i ID-kortet förhindras om fel PIN-kod anges tre gånger i följd. En låst PIN-kod kan låsas upp och åter tas i användning med hjälp av en PUK-kod som kan beställas vid ett personligt besök på polisinrättningens serviceställe för tillståndsärenden. I samband med det kontrolleras sökandens identitet.

PUK-koden skickas till den adress som sökanden uppgett inom en vecka från beställningen. Certifikatinnehavaren kan själv öppna sitt låsta kort med hjälp av ett kortläsarprogram. Programmet med anknytande information finns på adressen http://www.fineid.fi. Versionen av kortläsarprogrammet, mPollux DigiSign Client, bör vara minst 3.0.2.

6.5 Säkerhetskrav som gäller datoranvändning och åtkomst av datorsystem

6.5.1 Utrustningssäkerhet

Inom certifikatsystemet används bara sådan utrustning som lämpar sig för avsett syfte.

Med utrustningssäkerhet enligt principerna om god informationshantering avses att man, om systemet sviker, kan ta i bruk ett reservsystem utan att äventyra integriteten när det gäller den information som ingår i systemet. I fråga om reservdelar till utrustning som är viktig för kontinuiteten i verksamheten har tillgången tryggats.

Praxis vid service och underhåll är att utomstående personal inte har tillträde till system och lokaler som serviceproduktionen ansvarar för. Servicebesök tillåts bara av tekniska leverantörer som har

ingått ett tekniskt leveransavtal och ett sekretessavtal. En uppdaterad lista med godkända tekniska leverantörer hålls tillgänglig.

Servicebesök är möjliga bara under tillsyn av systemadministratören eller av en person som denne bemyndigat.

Certifikatsystemets utrustning bevakas dygnet runt.

6.6 Säkerheten hos certifikatsystemet under dess livscykel

Befolkningsregistercentralen tillämpar en prioritetsklassificering för attribut och system inom certifikattjänsterna och för säkringen av dem, deras angelägenhetsordning och lägsta underhållsnivå.

6.6.1 Övervakning av systemutvecklingen

Systemet utvecklas och testas i en särskild testmiljö. Endast testade, fungerande och godkända lösningar överförs till produktionssystemet.

6.6.2 Säkerhetshantering

Informationssäkerheten vid Befolkningsregistercentralen hanteras i enlighet med Befolkningsregistercentralens datasäkerhetspolicy och standarden ISO 27001.

6.7 Nätverkssäkerhet

Datakommunikationssäkerheten har genomförts så att certifikatsystemets informationsnät bildar en sammanhängande helhet som på lämpligt sätt har separerats från andra informationsnät och vars kritiska delar har dubbelriktats. Meddelanden som förmedlas via nätet och deras avsändare eller mottagare röjs inte för obehöriga utan särskilda åtgärder. Nätet används bara för ärenden som gäller certifikatsystemet. Obehövliga nättjänster har slopats. Nätet är indelat i logiska nätverksdelar med begränsad förbindelse. Metoder för autentisering, passerkontroll och oavvislighet används i betryggande utsträckning.

6.8 Övervakning av säkerhetsmoduler

Certifikatutfärdaren ansvarar för att utfärdarens privata nycklar är skyddade mot exponering och obehörig användning. För att tillgodose kraven på säkring av kritisk information tas en säkerhetskopia tas av utfärdarens privata nycklar.

Användningen av säkerhetsmoduler kräver alltid ett aktivkort för identifiering av personen och verifiering av användarrättigheterna. En modul kan aktiveras bara med systemanvändarens personliga kontrollkort.

För genereringen av nya rättigheter på användarnivå krävs närvaro av två personer på systemadministratörsnivå och motsvarande personliga kontrollkort. Modulen samlar in logguppgifter om händelserna.

7 Profiler för certifikat och spärrlistor

7.1 Teknisk information om certifikaten

Datainnehållet i rotcertifikat, utfärdarcertifikat och certifikatinnehavares certifikat beskrivs i dokumentet FINEID S2. Dokumentet finns på utfärdarens webbsidor, http://www.fineid.fi.

7.2 Spärrlistprofil

Datainnehållet i de spärrlistor som publiceras av certifikatutfärdaren beskrivs i dokumentet FINEID S2. Dokumentet finns på utfärdarens webbsidor, http://www.fineid.fi.

8 Administration av specifikationsdokument

8.1 Ändring av specifikationer

Certifikatutfärdaren kan ändra specifikationerna av lagstiftningsmässiga eller funktionella orsaker. Ändringarna ska registreras i certifikatpolicyn och certifieringspraxisen på det sätt som anges nedan.

8.2 Publicering och information

Certifikatutfärdaren publicerar certifikatpolicyn och certifieringspraxisen, som finns tillgängliga på webbsidorna och på adressen http://www.fineid.fi.

Certifikatutfärdarens offentliga specifikationer som hänför sig till produktionen av certifikat finns på samma webbsidor.

De avtal som ingås med datatekniska leverantörer om leverans av certifikat samt beskrivningarna av produktionssystemen och de specifikationer som gäller produkterna är konfidentiella.

8.3 Förfarande vid ändring och godkännande av certifieringspraxisen

Befolkningsregistercentralen godkänner såväl certifikatpolicyn som certifieringspraxisen för medborgarcertifikat. Dokumenten kan ändras med stöd av Befolkningsregistercentralens interna ändringsprocedurer.

Befolkningsregistercentralen ska i god tid innan ändringarna träder i kraft meddela om dem såväl till Kommunikationsverket som på sina webbsidor.

Befolkningsregistercentralen versionshanterar dokumenten och arkiverar alla dokument som gäller certifikatpolicyn och certifieringspraxisen. Typografiska rättelser och ändringar i kontaktuppgifterna kan införas med en gång.

1. Alla stycken i certifikatpolicyn och certifieringspraxisen kan efter den 1 december 2010 ändras genom ett meddelande om de kommande huvudsakliga ändringarna 30 dagar innan ändringarna börjar gälla.

2. Stycken som enligt Befolkningsregistercentralen inte nämnvärt påverkar certifikatinnehavare och förlitande parter kan efter den 1 december 2010 ändras genom att ändringarna meddelas 14 dagar i förväg.

8.4 Versionshantering

Certifieringspraxis för Befolkningsregistercentralens medborgarcertifikat som ingår i ID-kort, v. 1.6.1.

Version	Datum	Beskrivning/ändringar
v. 1.0	1.4.2003	Godkänd version 1.0
v. 1.1	1.9.2003	Ändringar av lagen om identitetskort (829/1999); ändringarna träder i kraft 1.9.2003
v. 1.2	1.6.2004	Editoriella ändringar
v. 1.3	1.7.2007	Lagändringar; Statsrådets förordning om identitetshandlingar som utfärdas av polisen (707/2006), förordningen trädde i kraft 21.8.2006. Editoriella ändringar. Uppdatering av kontaktuppgifter
v. 1.4	1.5.2008	Ändringar till följd av strukturomvandlingar i statsförvaltningen (ministeriebyte); förtydligande ändringar i sakinnehållet
v. 1.5	1.3.2010	Lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009), lagen träder i kraft 1.3.2010. Befolkningsdatalagen (507/1993) har upphävts. Lagen om stark autentisering och elektroniska signaturer (617/2009), lagen trädde i kraft 1.9.2009. Lagen om elektroniska signaturer (14/2003) har upphävts. Finansministeriets förordning om avgifterna för Befolkningsregistercentralens prestationer (873/2008), förordningen trädde i kraft 1.1.2009.
v. 1.6	1.12.2010	Identifikationshandlingar enligt lagen om stark autentisering och elektroniska signaturer (617/2009), ändringar av storleken på certifikatinnehavares privata och publika nycklar, uppdatering av kontaktuppgifter.
v. 1.6.1	1.12.2010	Ändringar som gäller upplåsning av låsta PIN-koder med hjälp av PUK-koder. Redaktionella ändringar.