Väestörekisterikeskus
Befolkningsregistercentralen

PKI Disclosure Statement

Befolkningsregistercentralens medborgarcertifikat

v. 1.7

ISO 9001

ISO/IEC 27001

1. Inledning

Detta dokument beskriver på allmän nivå certifikatutfärdarens verksamhetssätt samt villkoren och begränsningarna för användningen av certifikatet.

Detta dokument hänför sig till dokumenten:

Certifikatpolitik för Befolkningsregistercentralens medborgarcertifikat

OID:1.2.246.517.1.10.2

Certifieringspraxis för medborgarcertifikat som ingår i elektroniskt ID-kort

OID: 1.2.246.517.1.10.2.1.

Certifieringspraxis för medborgarcertifikat som ingår i Bank Kort

OID: 1.2.246.517.1.10.2.3.

Certifieringspraxis för medborgarcertifikat som ingår ID-kort med sjukförsäkrings-uppgifter

OID: 1.2.246.517.1.10.2.4.

2. PKI Disclosure Statement

2.1 Certifikatutfärdarens adressuppgifter

Befolkningsregistercentralen

Besöksadress:	**Postadress:**
Tunnbindaregatan 1 C	PB 70
00580 Helsingfors	00581 Helsingfors

Telefon/växel: (09) 229 161

Telefax: (09) 2291 6795

E-post: förnamn.efternamn@vrk.fi

Registratorskontor: vaestorekisterikeskus@vrk.fi

www.fineid.fi

FO-nummer: 0245437-2

2.2 Certifikatets typ, kontrollförfarande och brukssyfte

Ett medborgarcertifikat är ett certifikat för säker elektronisk kommunikation, vilket kan sparas i olika tekniska underlag, t.ex. på ett elektroniskt ID-kort, ett bankkort med mikrochips eller på mobilterminalens SIM-kort.

Medborgarcertifikat ansöks genom att personligen besöka den polismyndighet som fungerar som registrerare eller annan registreringsinstans. Vid ansökningen kontrolleras personens identitet på det sätt som beskrivits i certifieringspraxis. Om den sökande inte har on. dokument, identifierar polisen den sökande på annat sätt.

Uppgiften om identifieringssättet antecknas på ansökningsblanketten och funktionären vid registreringsinstansen bekräftar med sin egen signatur att personens identitet verkligen har kontrollerats. De av personen lämnade uppgifterna, t.ex. koder, namn och officiell adress jämförs med Befolkningsregistercentralens uppgifter. I fråga om medborgarcertifikat används för individualisering av personen en skilt för sig för elektronisk kommunikation skapad, i lagen om befolkningsdatasystemet och Befolkningsregistercentralens cetrifikattjänster (661/2009) preciserad e-kod (SATU).

Medborgarcertifikat kan användas för verifiering av person, kryptering av ett meddelande och för elektronisk signatur. Signaturcertifikatet som beviljats i enlighet med dokumentet ”Certifikatpolitik för statens medborgarcertifikat” uppfyller de krav som ställts för kvalificerade certifikat, avsedda i Europaparlamentets och rådets direktiv (1999/93 EG) om elektroniska signaturer och dess bilagor. Medborgarcertifikatet kan användas obegränsat i administrativa tillämpningar och tjänster eller sådana tillämpningar och tjänster som tillhandahålls av en enskild organisation.

2.3 Litande på certifikatet

Certifikatets brukssyfte har preciserats i certifikatpolitiken och certifieringspraxisen för ifrågavarande certifikat samt i den bruksansvisning som lämnas till certifikatinnehavaren. Certifikatet får användas endast enligt dess brukssyfte. Den förtroende parten skall kontrollera att giltighetstiden för det certifikat som används inte har gått ut och att certifikatet inte har upptagits på spärrlistan. Den förtroende parten kan inte uppriktigt lita på certifikatet, om certifikatets giltighetstid inte har kontrollerats på spärrlistan. Den förtroende parten är skyldig att kontrollera certifikaten inte är upptagna på spärrlistan innan de godkänns.

2.4 Certifikatinnehavarens skyldigheter

- Certifikatets användningssyfte har preciserats i certifikatpolitiken, certifieringspraxisen och certifikatinnehavarens bruksanvisningar för varje enskilt certifikat. Certifikatet får användas endast enligt dess användningssyfte.
- Certifikatinnehavaren svarar för att de uppgifter är riktiga som lämnats vid ansökan om certifikatet.
- Certifikatinnehavaren svarar själv för användningen av medborgarcertifikatet, för rättshandlingar som företagits med det samt deras ekonomiska följder. I fråga om signaturcertifikatet följs vad som bestämts i direktivet om elektroniska signaturer och lagen om stark autentisering och elektroniska signaturer.
- Certifikatinnehavaren förvarar sina privata nycklar och de koder som behövs för deras användning skilt för sig samt strävar efter att hindra att de privata nycklarna förkommer, kommer i händerna på utomstående, ändras eller används utan lov. Utlämnande av aktivkortet till eller avslöjande av PIN-koden för en annan person t.ex. genom att låna ut den befriar certifikatutfärdaren och den förtroende parten från ansvar som eventuellt vållas av att kortet används.
- Det elektroniska ID-kortet och andra tekniska underlag som ingår i medborgarcertifikatet skall hanteras och skyddas med samma omsorgsfullhet som motsvarande kort eller dokument, såsom t.ex. kreditkort, körkort och pass. De personliga koderna skall förvaras fysiskt på ett annat ställe än medborgarcertifikaten.

- Om aktivkortet förkommer eller det finns en möjlighet att kortet missbrukas, bör innehavaren omedelbart underrätta Certifikatutfärdaren därom genom att ringa upp den avgiftsfria spärrtjänsten 0800 162 622. Det finns en motsvarande text-telefontjänst för hörselskadade 0100 2288.

2.5 Förtroende partens skyldigheter gällande kontroll av certifikatet

Om den förtroende parten kopierar spärrlistan från registret, skall parten i fråga förvissa sig om att spärrlistan är äkta genom att kontrollera den elektroniska signaturen av spärrlistans certifikatutfärdare. Därutöver bör spärrlistans giltighetstid kontrolleras.

Om det inte är möjligt att få den senaste spärrlistan från registret p.g.a. en funktionsstörning i apparaturen eller registertjänsten, bör certifikatet inte godkännas, om giltighetstiden för den senast erhållna spärrlistan har gått ut. Alla godkännanden av certifikaten efter dess giltighetstid sker på egen risk av den förtroende parten.

2.6 Begränsning av ansvar

Det skadeståndsansvar som åvilar Befolkningsregistercentralen och som hänför sig till produktionen av certifikattjänster bestäms enligt stadgandena i skadeståndslagen (412/1974). För Befolkningsregistercentralen gäller också certifikatutfärdarens ansvar enligt lagen om stark autentisering och elektroniska signaturer.och lagen om elektronisk kommunikation i myndigheternas verksamhet.

Befolkningsregistercentralen svarar inte för sådana skador som vållas av att koderna, PUK-koden och certifikatinnehavarens privata nycklar avslöjas, om inte avslöjandet direkt beror på Befolkningsregistercentralens omedelbara verksamhet.

Befolkningsregistercentralen svarar inte gentemot certifikatinnehavaren för indirekta skador eller följdskador. Befolkningsregistercentralen svarar inte heller för indirekta eller följdskador som eventuellt vållats den förtroende parten eller annan avtalspart av certifikatinnehavaren.

Certifikatutfärdaren har rätt att avbryta tjänsten under åtgärden för ändringar eller underhåll av systemet. Om ändringar och underhållsarbeten som gäller spärrlistan meddelas i förväg.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Certifikatinnehavaren eller den förtroende parten skall svara för de egna kostnader som detta vållar och certifikatutfärdaren är inte skyldig att till certifikatinnehavaren ersätta sådana kostnader som vållats certifikatinnehavaren eller den förtroende parten av sådan utvecklingsverksamhet av certifikatutfärdaren.

Befolkningsregistercentralen svarar inte för funktionen av de allmänna datakommunikationerna eller för funktionen av datanät, t.ex. Internet, eller för att utförandet av en rättshandling förhindras p.g.a. att den apparat eller programvara som kortinnehavaren använder inte fungerar eller för att certifikaten används mot deras användningssyfte.

Certifikatutfärdaren svarar inte vid användningen av certifikatet för fel i nätservicen eller tillämpningen eller för de kostnader som vållas därav. Certifikatutfärdaren svarar inte vid användningen av certifikatet för sådana fel i nätservicen eller tillämp-

ningen som baserar sig på certifikatet och som tillhandahålls för den slutliga användaren eller för de kostnader som vållas därav.

Certifikatinnehavarens ansvar för användningen av certifikatet upphör då denne meddelat spärrtjänsten de nödvändiga uppgifterna för makulering av certifikatet och efter att av den funktionär som mottagit samtalet ha fått meddelande om att certifikatet upptagits på spärrlistan. För att ansvaret skall upphöra skall anmälan göras omedelbart då anledningen till meddelandet har observerats.

2.7 Tillämpade avtal, certifieringspraxis och certifikatpolitik

Certifikatsökandens rättigheter och skyldigheter har angetts i ansökningsdokumentet och de allmänna bruksanvisningarna, vilka utgör avtalet med certifikatsökanden. Ansökningsdokumentet har uppgifter om båda parternas rättigheter och skyldigheter. I ansökningsdokumentet och bruksanvisningarna nämns tydligt att medborgarcertifikatsökanden med sin signatur godkänner de lämnade uppgifternas riktighet samt skapandet och utgivande av certifikatet i en publik katalog. Samtidigt godkänner sökanden de regler och villkor som hänför sig till användningen av medborgarcertifikatet samt sköter om förvaringen av medborgarcertifikatet och dess PIN-koder samt anmälan av eventuellt missbruk av kortet eller förkommet kort.

Mellan Certifikatutfärdaren och Registreraren, Korttillverkaren och andra leverantörer som producerar olika delområden inom certifikattjänsterna har det gjorts upp ett avtal som obestridligen upptar alla parternas rättigheter, ansvar och skyldigheter.

Då Certifikatutfärdaren beviljar medborgarcertifikatet, godkänner denne samtidigt certifikatansökan.

Befolkningsregistercentralen gör upp en särskild certifieringspraxis för varje av centralen beviljad certifikattyp. Certifieringspraxisen hänför sig till certifikatpolitidokumentet, som består av mer allmänna regler och anvisningar och är gemensam för alla medborgarcertifikat oberoende av det tekniska underlag certifikatet ingår i.

Befolkningsregistercentralen publicerar certifikatpolitiken och certifieringspraxisen för de certifikat som beviljats av centralen. Certifikatpolitiken beskriver per certifikattyp de begagnade procedurerna, bruksvillkoren, ansvarsfördelningen och andra aspekter som hänför sig till användningen av certifikaten. Certifieringspraxisen beskriver mer i detalj hur certifikatpolitiken tillämpas på de olika tekniska underlagen.

Både certifikatpolitiken och certifieringspraxisen finns tillgängliga under adressen www.fineid.fi.

2.8 Integritetsskydd

Certifikatutfärdaren och registreraren följer vid behandlingen certifikatinnehavarnas personuppgifter god datahanteringssed och gott dataskydd. Särskild uppmärksamhet fästs på behandlingen av personuppgifterna och Befolkningsregistercentralen har för certifikattjänsterna utfärdat särskilda praxisregler enligt personuppgiftslagen.

2.9 Ersättningsförfarande

Det skadeståndsansvar som åvilar Befolkningsregistercentralen och som hänför sig till produktionen av certifikattjänster bestäms enligt stadgandena i skadeståndslagen (412/1974). För Befolkningsregistercentralen gäller också certifikatutfärdarens

skadeståndsansvar enligt lagen om stark autentisering och elektroniska signaturer. och lagen om elektronisk kommunikation i myndigheternas verksamhet.

Befolkningsregistercentralen svarar gentemot certifikatinnehavaren högst för direkta skador förorsakades, om skadan beror på Befolkningsregistercentralens omedelbara verksamhet.

2.10 Tillämpad lagstiftning och avgörande av tvister

Ett medborgarcertifikat uppfyller de krav som ställts för kvalificerade certifikat, avsedda i Europaparlamentets och rådets direktiv (1999/93/EG) om elektroniska signaturer.

I lagen om stark autentisering och elektroniska signaturer. (617/2009) har stadgats om elektroniska signaturer som gjorts med kvalificerade certifikat. Om elektroniskt ID-kort har stadgats i lagen om identitetskort (829/1999) och om certifikat beviljade av Befolkningsregistercentralen har stadgats i lagen om befolkningsdatasystemet och Befolkningsregistercentralens cetrifikattjänster (661/2009).

Det skadeståndsansvar som åvilar Befolkningsregistercentralen och som hänför sig till produktionen av certifikattjänster bestäms enligt stadgandena i skadeståndslagen (412/1974). För Befolkningsregistercentralen gäller också kraven enligt lagen om stark autentisering och elektroniska signaturer.(617/2009) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet är det i myndighetsförvaltningen alltid möjligt att uträtta ärenden med kvalificerade certifikat.

Certifikatutfärdarna av kvalificerade certifikat står under tillsyn av Kommunikationsverket.

Medborgarcertifikaten har skapats enligt de procedurer som framställts i lagen om befolkningsdatasystemet och Befolkningsregistercentralens cetrifikattjänster (661/2009), lagen om stark autentisering och elektroniska signaturer. och lagen om elektronisk kommunikation i förvaltningsärenden och de procedurer som framförts i certifikatpolitiken och i enlighet med de uppgifter som certifikatinnehavaren lämnat.

2.11 Förfarande för kontroll av certifikatutfärdarens verksamheten

Kommunikationsverket, som har tillsyn över certifikatutfärdarna av kvalificerade certifikat, kan kontrollera certifikatutfärdarens verksamhet under de förutsättningar som fastställts i lagen om stark autentisering och elektroniska signaturer.. Befolkningsregistercentralen kan kontrollera de tekniska leverantörerna enligt vad som avtalats i de tekniska leveransavtalen som ingåtts med de tekniska leverantörerna. Kontrollen sker åtminstone en gång per år och alltid då en ny avtalsperiod inleds.

Med hjälp av kontrollen utreds om den tekniska leverantören fungerar enligt avtalet med beaktande av datasäkerhetsstandardens krav. I regel bedöms den tekniska leverantören enligt standard ISO 27001 samt Kommunikationsverkets bestämmelser.

Kontrollen utförs av Befolkningsregistercentralens datasäkerhetschef eller en Befolkningsregistercentralen anlitad utomstående inspektör som är specialiserad på auditering av sådana tekniska leverantörer som hänför sig till certifikattjänster. In-

spektionen utförs genom att beakta genomförandet av de åtta delområdena inom datasäkerheten. Sådana egenskaper inom datasäkerheten som skall kontrolleras omfattar tillförlitlighet, integritet och användbarhet.

Inspektionen omfattar Kommunikationsverkets bestämmelser om datasäkerheten för certifikatutfärdaren.

Vid inspektionen jämförs politiken och tillämpningsanvisningarna med hela certifikatorganisationens och -systemets verksamhet. Befolkningsregistercentralen är ansvarlig för att tillämpningsanvisningarna är förenliga med certifikatpolitiken.

3. Version kontroll

PKI Disclosure Statement för Befolkningsregistercentralens medborgarcertifikat, v.1.7

Version	**Datum**	**Beskrivning/ändringar**
v.1.0.	1.4.2003	Godkänt version 1.0.
V 1.1.	1.9.2003	Ändringar av lag om personkort(829/1999) , träder i kraft 1.9.2003
v.1.2.	7.1.2004	Bank kort
v.1.3.	1.6.2004	Redaktionella ändringar.
v.1.4.	1.7.2004	Redaktionella ändringar.
v.1.5.	1.7.2007	Ändringar av lagstiftning; Statsrådets förordning om identitetshandlingar som utfärdas av polisen (707/2006), trädde i kraft 21.8.2006. Editoriella ändringar. Uppdatering av adressuppgifter. Redaktionel ändring.
v.1.6.	1.5.2008	Ändringar av förvandlingar i offentlig förvaltningen; förtydligandena.
v.1.7.	1.3.2010	Lagen om befolkningsdatasystemet och Befolkningsregistercentralens cetrifikattjänster (661/2009), lagen träder i kraft 1.3.2010. Befolkningsdatalagen (507/1993) är upphä-

		vad. Lagen om stark autentisering och elektroniska signaturer (617/2009), lagen trädde i kraft 1.9.2009. Lagen om elektroniska signaturer (14/2003) är upphävad.