CERTIFIKATBESKRIVNING

Befolkningsregistercentralens medborgarcertifikat
v. 1.0

ISO 9001

ISO/IEC 27001

Väestörekisterikeskus

VRK/TS/Keh

03-05-2018

DOKUMENTHANTERING	
Ägare	
Upprättat av	Tuire Saaripuu
Granskat av	
Godkänt av	Joonas Kankaanrinne

VERSIONSHANTERING		
version nr	åtgärder	datum/person
v. 1.0	Godkänd version 1.0., dokument förenligt med eIDAS-förordningen	3.5.2018 TS

Innehållsförteckning

VRK/TS/Keh 03-05-2018

INLEDNING

Detta dokument beskriver certifikatutfärdarens verksamhetskoncept på ett allmänt plan samt villkor och begränsningar för användningen av certifikat.

Detta dokument hänför sig till följande dokument:

Certifikatpolicy för Befolkningsregistercentralens medborgarcertifikat

OID: 1.2.246.517.1.10.202;

Certifieringspraxis för medborgarcertifikat som ingår i elektroniskt ID-kort

OID: 1.2.246.517.1.10.202.1;

När det gäller signeringscertifikat som tillhandahålls allmänheten iakttar Befolkningsregistercentralen en certifikatpolicy förenlig med betrodda tjänster i Förordningen ((EU) 910/2014). Dokumentens referensuppgifter är ETSI EN 319 411-1 [2], 4.3.5., 3 punkten QSCD; OID: 0.4.0.194112.1.2. Signeringscertifikat som utfärdas i enlighet med denna certifikatpolicy kan användas för att bekräfta sådana elektroniska signaturer som motsvarar kvalificerade certifikat och anordningar för framställning av elektroniska signaturer som beskrivits i Förordningen.

1 Certifikatbeskrivning

1.1 Certifikatutfärdarens kontaktuppgifter

Befolkningsregistercentralen

Besöksadress: Fågelviksgränden 4, 00530 Helsingfors
Postadress: PB 123, 00531 Helsingfors

Telefon/växel: +358 295 535 001

Fax: +358 9 876 4369

E-post: fornamn.efternamn@vrk.fi

Registratorskontor: kirjaamo@vrk.fi

www.fineid.fi

FO-nummer: 0245437-2

1.2 Certifikattyp, kontrollförfarande och syfte

Ett medborgarcertifikat är ett certifikat för säker elektronisk kommunikation, vilket kan sparas i olika tekniska underlag utfärdade av myndigheterna, t.ex. på ett elektroniskt ID-kort eller ett USB-token.

Medborgarcertifikat ansöks genom att personligen besöka den polismyndighet som fungerar som registrerare eller en annan registreringsinstans. Vid besöket kontrolleras personens identitet på det sätt som beskrivits i certifieringspraxisen. Om sökanden inte har nämnda handlingar ska polisen kontrollera sökandens identitet 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 en e-kod (SATU) för individualisering av en person. E-koden har skapats särskilt för elektronisk kommunikation och preciseras i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Medborgarcertifikatet innehåller signerings- och autentiseringscertifikat som det finns bestämmelser om i lagen om stark autentisering och betrodda elektroniska tjänster.

Medborgarcertifikat kan användas för stark autentisering av en person, kryptering av ett meddelande och elektroniska signaturer. Signeringscertifikatet som beviljats i enlighet med dokumentet ”Certifikatpolitik för statens medborgarcertifikat” ska uppfylla kraven som ställs i följande rättsakt: Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen). Medborgarcertifikatet kan användas obegränsat i administrativa tillämpningar och tjänster eller sådana tillämpningar och tjänster som tillhandahålls av en enskild organisation.

Ett signeringscertifikat som utfärdats enligt denna policy uppfyller de krav som ställs på kvalificerade signeringscertifikat i Förordningen. Graden av tillförlitlighet på autentiseringscertifikatet är "hög" enligt Förordningen och i förordningen om tillitsnivåer som utfärdats med stöd av Förordningen.

Den som ansöker om ett medborgarcertifikat kan registrera sin e-postadress både på medborgarcertifikatet och i befolkningsdatasystemet. E-postadressen antecknas i den form sökanden anger både på medborgarcertifikatet och i befolkningsdatasystemet. Den e-postadress som antecknats på medborgarcertifikatet införs i det offentliga registret på samma sätt som det övriga datainnehållet i medborgarcertifikatet. E-postadressen kan inte ändras så länge medborgarcertifikatet är i kraft.

1.3 Certifikatens tillförlitlighet

Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen för varje typ av certifikat och i de användaranvisningar som lämnas till certifikatinnehavaren. Ett certifikat får användas enbart i avsett syfte. Förlitande parter ska kontrollera att giltighetstiden för ett certifikat som ska användas inte har gått ut. Förlitande parter kan inte uppriktigt lita på ett certifikat, om de inte har kontrollerat certifikatet via en OCSP-tjänst eller mot en spärrlista. Förlitande parter är innan de godkänner ett certifikat skyldiga att kontrollera att det är giltigt.

1.4 Certifikatinnehavarens skyldigheter

Syftet med ett certifikat anges i certifikatpolicyn och certifieringspraxisen för varje enskild typ av certifikat samt i användaranvisningarna för certifikatinnehavaren. Ett certifikat får användas enbart i avsett syfte.

Certifikatinnehavaren svarar för att de uppgifter som anges vid ansökan om certifikatet är korrekta.

Certifikatinnehavaren svarar själv för användningen av medborgarcertifikatet, de rättshandlingar som företas med stöd av det och deras ekonomiska följder. När det gäller certifikatet för elektroniska signaturer gäller bestämmelserna i Förordningen och i lagen om stark autentisering och betrodda elektroniska tjänster.

Certifikatinnehavaren ska förvara sina privata nycklar och de koder som behövs för användningen skilt från varandra samt förhindra att de privata nycklarna förkommer, råkar i händerna på utomstående, ändras eller används av obehöriga. Om innehavaren överlåter aktivkortet eller avslöjar PIN-koden för en annan person t.ex. genom utlåning, befrias utfärdare och förlitande parter från det eventuella ansvar som följer av att kortet används.

Det elektroniska ID-kortet och andra tekniska underlag som ingår i medborgarcertifikatet ska hanteras och skyddas med samma omsorgsfullhet som motsvarande kort eller dokument, t.ex. kreditkort, körkort och pass. De personliga koderna ska förvaras fysiskt på ett annat ställe än medborgarcertifikaten.

Om aktivkortet förkommer eller det finns en möjlighet att kortet missbrukas, bör innehavaren omedelbart underrätta certifikatutfärdaren om detta genom att ringa den avgiftsfria spärrtjänsten 0800 162 622. Det finns en motsvarande texttelefontjänst för hörselskadade på numret 0100 2288.

1.5 Förlitande parters skyldighet att kontrollera certifikat

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

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

1.6 Ansvarsbegränsningar

Befolkningsregistercentralen omfattas av det skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet. På verksamheten tillämpas även vissa bestämmelser i skadeståndslagen (412/1974).

Befolkningsregistercentralen ansvarar inte för eventuella skador som orsakas av att koderna, PUK-koden eller certifikatinnehavarens privata nycklar röjs, om inte avslöjandet direkt har orsakats av Befolkningsregistercentralens 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 kortinnehavaren.

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

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 och utfärdaren är inte skyldig att ersätta certifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

Befolkningsregistercentralen ansvarar inte för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel Internet, eller för att en rättshandling inte kan utföras på grund av att kortinnehavarens utrustning inte fungerar eller för att certifikatet används i strid med sitt syfte.

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

Certifikatinnehavarens ansvar för användningen av ett certifikat 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 tagit emot samtalet. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats föreligga skäl för anmälan.

1.7 Tillämpliga avtal, certifieringspraxis och certifikatpolicy

Certifikatsökandes rättigheter och skyldigheter har uppgetts i ansökningshandlingen och i de allmänna användaranvisningarna, vilka tillsammans bildar det avtal som ingås med certifikatsökanden. I ansökningshandlingen finns uppgifter om båda parternas rättigheter och skyldigheter. I ansökningshandlingen och i anvisningarna ska tydligt anges att sökanden av ett medborgarcertifikat genom sin underskrift 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 medborgarcertifikatet och förbinder sig att förvara medborgarcertifikatet och PIN-koderna omsorgsfullt samt att anmäla eventuellt missbruk eller ett förkommet kort.

Certifikatutfärdaren och registreraren, korttillverkaren och andra leverantörer på olika delområden inom certifikattjänsterna har ingått ett avtal som obestridligen uttrycker varje parts rättigheter, ansvar och skyldigheter.

Vid beviljandet av ett medborgarcertifikat godkänner utfärdaren samtidigt certifikatansökan.

Befolkningsregistercentralen ska utarbeta en särskild certifieringspraxis för varje typ av certifikat som den beviljar. Certifieringspraxisen hänför sig till certifikatpolicydokumentet, som består av mer allmänna regler och anvisningar och är gemensamt för alla medborgarcertifikat oberoende av i vilket tekniskt medium certifikatet är lagrat.

Befolkningsregistercentralen ska publicera en certifikatpolicy och en certifieringspraxis för de certifikat som den har beviljat. Certifikatpolicyn beskriver förfaranden, användarvillkor och ansvarsfördelning för den aktuella certifikattypens del liksom andra aspekter på certifikatanvändningen. Certifieringspraxisen beskriver närmare hur certifikatpolicyn tillämpas på olika tekniska plattformar.

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

1.8 Integritetsskydd

Vid behandlingen av certifikatinnehavarens personuppgifter ska certifikatutfärdaren och registreraren iaktta principerna om god informationshantering och datasekretess. Särskild vikt ska fästas vid en omsorgsfull behandling av personuppgifter. För certifikattjänsternas del har Befolkningsregistercentralen gett ut särskilda uppförandekoder som följer personuppgiftslagen.

1.9 Ersättningspraxis

Befolkningsregistercentralen omfattas av det skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet. På verksamheten tillämpas även vissa bestämmelser i skadeståndslagen (412/1974).

Befolkningsregistercentralens ansvar gentemot certifikatinnehavare omfattar högst de direkta skador som har åsamkats dem, om skadan beror på Befolkningsregistercentralens omedelbara åtgärder.

1.10 Tillämplig lagstiftning och avgörande av tvister

Medborgarcertifikaten uppfyller de krav som ställts på signeringscertifikat i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (Förordningen).

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som görs med signeringscertifikat. Om elektroniska identitetskort föreskrivs i lagen om identitetskort (829/1999) och om certifikat utfärdade av Befolkningsregistercentralen i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009). Om förvaltningsmässiga frågor bestäms också i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Befolkningsregistercentralen omfattas av det skadeståndsansvar som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster och i lagen om elektronisk kommunikation i myndigheternas verksamhet. På verksamheten tillämpas även vissa bestämmelser i skadeståndslagen (412/1974).

Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet kan ärenden hanteras med signeringscertifikat i alla tjänster inom den offentliga förvaltningen.

Medborgarcertifikaten har skapats med iakttagande av de förfaranden som anges i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, lagen om stark au-

tentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet och certifikatpolicyn samt i enlighet med de uppgifter som certifikatinnehavaren lämnat.

1.11 Granskning av certifikatutfärdarens verksamhet

Kommunikationsverket, som utövar tillsyn över dem som utfärdar signeringscertifikat och över leverantörer av identifieringstjänster och verktyg för stark autentisering, har rätt att granska utfärdarens verksamhet på de villkor som anges i lagen om stark autentisering och betrodda elektroniska tjänster. Befolkningsregistercentralen har rätt att granska sina tekniska leverantörer i enlighet med de rutiner som finns inskrivna i de leveransavtal som har ingåtts med leverantörerna. Granskningar ska utföras minst en gång om året och alltid när en ny avtalsperiod inleds.

Med hjälp av granskningarna klarläggs om leverantörerna följer avtalen och beaktar kraven i informationssäkerhetsstandarderna. Som regel bedöms de tekniska leverantörerna med stöd av standarden ISO 27001 och Kommunikationsverkets föreskrifter.

Granskningarna utförs av Befolkningsregistercentralens datasäkerhetschef eller av en utomstående inspektör som har anlitats av ämbetsverket och som är specialiserad på auditering av tekniska leverantörer av certifikattjänster. Granskningarna ska genomföras med beaktande av de åtta delområdena inom informationssäkerheten. Egenskaper som granskas är konfidentialitet, integritet och tillgänglighet.

Granskningarna omfattar de föreskrifter om informationssäkerhet som Kommunikationsverket meddelat utfärdaren.

Vid granskningarna bedöms policyn och tillämpningsanvisningarna i relation till hela verksamheten inom certifikatorganisationen och certifikatsystemet. Befolkningsregistercentralen ansvarar för att tillämpningsanvisningarna är förenliga med certifikatpolicyn.