CERTIFIKATBESKRIVNING

Befolkningsregistercentralens organisationscertifikat
v. 1.0

ISO 9001

ISO/IEC 27001

Väestörekisterikeskus

VRK/TS/2018 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

VRK/TS/2018 03-05-2018

Innehållsförteckning

VRK/TS/2018 03-05-2018

1 Inledning

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

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) tillämpas på signeringscertifikat inom betrodda tjänster från och med den 1 juli 2016.

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.

I detta dokument fastställs kraven på verksamheten och förvaltningspraxisen hos dem som utfärdar autentiserings- och signeringscertifikat enligt Förordningen. I kraven på förfaringssätt i detta dokument beskrivs användningen av anordningar för signaturframställning.

När det gäller signaturcertifikat 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 artikel 28 och 29 i Förordningen.

2. Certifikatbeskrivning

2.1 Certifikatutfärdarens kontaktuppgifter

Befolkningsregistercentralen (BRC)

Certifikattjänster

Postadress:

PB 123 (Fågelviksgränden 4)

00531 HELSINGFORS

FO-nummer: 0245437-2

VRK/TS/2018

03-05-2018

Telefon: +358 295 535 001

Fax: +358 9 876 4369

E-post: vaestorekisterikeskus@vrk.fi

Internet: www.fineid.fi

2.2 Certifikattyp, kontrollförfarande och syfte

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

I detta dokument fastställs kraven på förfaranden som gäller utfärdare av signeringscertifikat samt Befolkningsregistercentralen i egenskap av leverantör av verktyg för stark autentisering. Kraven ställs på verksamheten och förvaltningspraxisen hos dem som utfärdar certifikat för att de som beställer certifikat, de undertecknare som certifikatutfärdaren har certifierat samt de förlitande parterna ska kunna lita på att elektroniska signaturer kan styrkas med certifikatet.

Ansökan om organisationscertifikat förutsätter personligt besök hos en registreringsinstans. Registreraren ska identifiera certifikatsökanden på ett tillförlitligt sätt med hjälp av en giltig, godkänd handling som har utfärdats av polisen. En sådan handling är identitetskort (utfärdat efter den 1 mars 1999), pass samt körkort som utfärdats efter den 1 oktober 1990. Godtagbara identifieringshandlingar är också ett giltigt pass eller identitetskort som utfärdats av en myndighet i en medlemsstat inom EES, Schweiz eller San Marino, ett giltigt körkort som utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat inom EES och ett giltigt pass som utfärdats av en myndighet i någon annan stat. Identifikationssättet ska antecknas i ansökningsblanketten och tjänstemannen vid registreringsinstansen styrker med sin underskrift att personen har identifierats. Enligt ett avtal med kundorganisationen kan certifikat sökas också med ett certifikat som Befolkningsregistercentralen har beviljat efter den 1 mars 2010.

Organisationscertifikat kan användas för stark autentisering av en person, kryptering av information och elektroniska signaturer. Signeringscertifikat som beviljats med stöd av dokumentet "Certifikatpolicy för organisationscertifikat" uppfyller de krav som ställs på sådana signeringscertifikat som avses i Förordningen och dess bilagor. Certifikaten får användas obegränsat i enlighet med sitt syfte i administrativa tillämpningar och tjänster eller sådana tillämpningar och tjänster som tillhandahålls av en enskild organisation.

Från och med den 1 december 2010 är Befolkningsregistercentralen också lagstadgad certifikatutfärdare för hälso- och sjukvården med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) och lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

2.3 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 och att certifikatet inte har upptagits på någon spärrlista. Förlitande parter kan inte uppriktigt lita på ett certifikat, om de inte har kontrollerat certifikatets giltighet mot en spärrlista. Med tanke på en eventuell spärrning är förlitande parter skyldiga att kontrollera certifikaten mot en spärrlista innan de godkänner dem.

2.4 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 bara användas i avsett syfte för elektroniska signaturer, autentisering eller kryptering av information.

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

- Certifikatinnehavaren svarar för användningen av aktivkortet, de rättshandlingar som företas med stöd av kortet 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.

- Aktivkortet ska behandlas och skyddas lika omsorgsfullt som andra liknande kort eller dokument, såsom kreditkort, körkort och pass. De personliga koderna ska förvaras fysiskt åtskilda från aktivkortet.

2.5 Förlitande parters skyldighet att kontrollera certifikat

En förlitande part ska kontrollera att det certifikat som används är i kraft och att det inte tagits upp på spärrlistan. 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. Spärrlistan gäller i åtta timmar.

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.

2.6 Ansvarsbegränsningar

Befolkningsregistercentralens skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. 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.

Befolkningsregistercentralens ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har åsamkats dem, om skadan beror på Befolkningsregistercentralens omedelbara åtgärder. Ansvaret uppgår dock till högst 15 procent av certifikatfaktureringen för de tre föregående månaderna (andel som redovisas till BRC).

Befolkningsregistercentralen svarar inte för indirekta skador eller följdskador som orsakas innehavare av aktivkort. Befolkningsregistercentralen svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter till kortinnehavaren.

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

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

Certifikatinnehavarens ansvar för användningen av ett organisationscertifikat upphör när innehavaren eller en företrädare för innehavarens organisation 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.

2.7 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 certifikatsökanden genom sin underskrift bekräftar att de givna uppgifterna är korrekta och godkänner att ett certifikat skapas och publiceras i ett offentligt register eller att förlitande parter i övrigt informeras enligt det avtal som ingåtts med kundorganisationen. Samtidigt godkänner sökanden de bestämmelser och villkor som gäller användningen av certifikatet och förbinder sig att förvara organisationscertifikatet och 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 organisationscertifikat 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 organisationscertifikat 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 http://www.fineid.fi.

2.8 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.

2.9 Ersättningspraxis

Befolkningsregistercentralens skadeståndsansvar i anslutning till produktionen av certifikattjänster fastställs i det tjänsteavtal som ingåtts med certifikatsökanden. 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 och förlitande parter omfattar högst de direkta skador som har åsamkats dem, om skadan beror på Befolkningsregistercentralens omedelbara åtgärder. Ansvaret uppgår dock till högst 15 procent av certifikatfaktureringen för de tre föregående månaderna (andel som redovisas till BRC).

2.10 Tillämplig lagstiftning och avgörande av tvister

Organisationscertifikaten uppfyller de krav som ställs på signeringscertifikat i Förordningen.

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) föreskrivs om elektroniska signaturer som görs med certifikat. I lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) föreskrivs om certifikat som utfärdas av Befolkningsregistercentralen.

Befolkningsregistercentralens skadeståndsansvar i anslutning till produktionen av certifikattjänster regleras i skadeståndslagen (412/1974). Befolkningsregistercentralen omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet kan ärenden hanteras med ett certifikat i alla tjänster som tillhandahålls av myndigheter.

Utfärdarna övervakas av Kommunikationsverket.

Organisationscertifikaten har skapats med iakttagande av de förfaranden som anges i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, lagen om stark autentisering och betrodda elektroniska tjänster, lagen om elektronisk kommunikation i myndigheternas verksamhet och certifikatpolicyn samt i enlighet med de uppgifter som certifikatinnehavaren lämnat.

2.11 Granskning av certifikatutfärdarens verksamhet

Kommunikationsverket 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 le-

verantörerna. 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/IEC 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.