CERTIFIKATBESKRIVNING

Befolkningsregistercentralens tillfälliga certifikat

v. 1.0

ISO 9001

ISO/IEC 27001

Väestörekisterikeskus

VRK/TS/Keh 03-05-2018

DOKUMENTHANTERING

Ägare	
Upprättat av	Saaripuu Tuire
Granskat av	
Godkänt av	Kankaanrinne Joonas

VERSIONSHANTERING

version nr	åtgärder	datum/person
v. 1.0	Godkänd version 1.0.	3.5.2018

VRK/TS/Keh

03-05-2018

Innehållsförteckning

VRK/TS/Keh

03-05-2018

1 Inledning

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

Detta dokument hänför sig till följande dokument:

Certifikatpolicy för Befolkningsregistercentralens tillfälliga certifikat

OID: 1.2.246.517.1.10.204

Certifieringspraxis för tillfälliga certifikat

OID: 1.2.246.517.1.10.204.1

och

Certifieringspraxis för tillfälliga certifikat för personal och aktörer inom social- och hälsovården

OID: 1.2.246.517.1.10.204.2

2 Certifikatbeskrivning

2.1 Certifikatutfärdarens kontaktuppgifter

Befolkningsregistercentralen

Besöksadress:

Fågelviksgränden 4

00530 Helsingfors

Postadress:

PB 123

00531 Helsingfors

Telefon/växel: 0295 535 001

Fax: 09 876 4369

E-post: fornamn.efternamn@vrk.fi

Registratorskontor: vaestorekisterikeskus@vrk.fi

www.fineid.fi

FO-nummer: 0245437-2

2.2 Certifikattyp, kontrollförfarande och syfte

Ett tillfälligt certifikat stöder användningen av Befolkningsregistercentralens organisationscertifikat, OID: 1.2.246.517.1.10.203.

Ansökan om tillfälliga certifikat förutsätter personligt besök hos en registreringsinstans.

Vid ansökan om certifikatet ska registreraren identifiera certifikatsökanden på ett tillförlitligt sätt med stöd 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 har 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.

Tillfälliga certifikat kan användas för stark autentisering av en person, kryptering av information och elektroniska signaturer. 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.

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 certifikatkedjan är obruten, att giltighetstiden för ett certifikat som ska användas inte har gått ut och att certifikatet inte har upptagits på någon spärrlista. Förlitande parter är skyldiga att kontrollera ett certifikat mot en spärrlista eller via en OCSP-tjänst. Uppgiften om ett certifikats status kan också kontrolleras i en OCSP-tjänst. Förlitande parter kan inte uppriktigt lita på ett certifikat, om de inte har kontrollerat certifikatet mot en spärrlista eller via en OCSP-tjänst.

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 för stark autentisering av en person, kryptering av information och elektroniska signaturer.

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

- Certifikatinnehavaren svarar för användningen av reservkortet, de rättshandlingar som företas med stöd av kortet och deras ekonomiska följder. I fråga om certifikatet iakttas vad som bestäms i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Om certifikatinnehavaren hör till personalen inom social- och hälsovården eller är en aktör inom social- och hälsovården, iakttas dessutom bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de bestämmelser och villkor som meddelats med stöd av dem.

- Certifikatinnehavaren ska förvara sin privata nyckel och den kod som behövs för användningen skilt från varandra samt förhindra att den privata nyckeln förkommer, råkar i händerna på utomstående, ändras eller används av obehöriga. Om innehavaren överlåter reservkortet 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.

- Reservkortet ska behandlas och skyddas lika omsorgsfullt som andra liknande kort eller dokument, såsom kreditkort, körkort och pass. Den personliga PIN-koden ska förvaras fysiskt åtskild från reservkortet.

2.5 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.

2.6 Ansvarsbegränsningar

Befolkningsregistercentralen omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna i skadeståndslagen (412/1974).

Befolkningsregistercentralen svarar inte för eventuella skador som orsakas av att PIN-koden eller certifikatinnehavarens privata nyckel har röjts, 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 den aktuella kundorganisationens certifikatfakturering för de tre föregående månaderna (andel som redovisas till BRC).

Befolkningsregistercentralen svarar inte för indirekta skador eller följdskador som orsakas innehavare av reservkort. 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 certifikatet upphör när han eller hon har meddelat registreraren i certifikatinnehavarens organisation om behovet av att spärra certifikatet och fått bekräftelse på att begäran om spärrning har emottagits. 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 med sin underskrift bekräftar att de givna uppgifterna är korrekta och godkänner att ett certifikat skapas. Samtidigt godkänner sökanden de bestämmelser och villkor som gäller användningen av tillfälliga certifikat och förbinder sig att sörja för förvaringen av certifikatet och koden samt anmäla eventuellt missbruk eller ett förkommet kort.

Certifikatutfärdaren, 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 tillfälligt certifikat 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 tillfälliga certifikat 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.

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

Befolkningsregistercentralen omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna 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 den aktuella kundorganisationens certifikatfakturering för de tre föregående månaderna (andel som redovisas till BRC).

2.10 Tillämplig lagstiftning och avgörande av tvister

I lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) föreskrivs om certifikat som utfärdas av Befolkningsregistercentralen.

Befolkningsregistercentralen omfattas av bestämmelserna i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och i tillämpliga delar av bestämmelserna i skadeståndslagen (412/1974). Enligt lagen om elektronisk kommunikation i myndigheternas verksamhet kan ärenden hanteras med ett certifikat i alla tjänster som tillhandahålls av myndigheter.

Leverantörerna av identifieringstjänster övervakas av Kommunikationsverket.

Tillfälliga certifikat ska skapas med iakttagande av de förfaranden som anges i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, lagen om stark autentisering och betrodda elektroniska tjänster, certifikatpolicyn och certifieringspraxisen samt i enlighet med de uppgifter som certifikatinnehavaren lämnat. Om det tillfälliga certifikatet har skapats för en medlem av personalen inom social- och hälsovården eller aktörer inom social- och hälsovården, iakttas dessutom bestämmelserna i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) och lagen om elektroniska recept (61/2007) samt de bestämmelser och villkor som meddelats med stöd av dem.

Sedan den 1 december 2010 har Befolkningsregistercentralen varit lagstadgad certifikatutfärdare för hälso- och sjukvården och sedan den 1 april 2015 för socialvården till följd av de ändringar som gjordes i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007), lagen om elektroniska recept (61/2007) samt lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009)). Befolkningsregistercentralens enhet Certifikattjänster ansvarar för ämbetsverkets certifikatverksamhet.

2.11 Granskning av certifikatutfärdarens verksamhet

Kommunikationsverket, som utövar tillsyn över dem som tillhandahåller identifieringstjänster, 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/IEC 27001 och Befolkningsregistercentralens datasäkerhetspolicy eller de tekniska leveransavtalen.

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.

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