MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Sammanfattning av certifieringspraxis

För Signeringscertifikat för Finlands chipförsedda pass

v.2.2

CERTIFIED SFS ORGANIZATION ISO 9001

kiwa ISO/IEC 27001

Innehållsförteckning

1.Inledning

Detta dokument är en sammanfattning av Certifikatutfärdarens certifieringspraxis i anslutning till certifikatsystemet för Finlands chipförsedda pass som Myndigheten för digitalisering och befolkningsdata och Polisstyrelsen utarbetat. Certifieringspraxisen tillämpas på Signeringscertifikat för chipförsedda pass (nedan Signeringscertifikat) som utfärdas av Myndigheten för digitalisering och befolkningsdata och som beviljas till en myndighet som definieras i passlagen. Certifieringspraxisen är inte ett offentligt dokument, men de offentliga ärenden som ingår i den tas upp i denna sammanfattning. Certifikatpolicyn och certifieringspraxisen är officiella dokument som utarbetats av Certifikatutfärdaren och som ska iakttas mellan parterna.

Detta dokument hänför sig till följande handlingar:

Certifikatpolicy för Signeringscertifikat för Finlands chipförsedda resedokument och uppehållstillståndshandlingar:

OID: 1.2.246.517.2.10.5

Certifieringspraxis för Signeringscertifikat för Finlands chipförsedda pass:

OID: 1.2.246.517.2.10.5.1

2.Certifikatutfärdaren och tillämpningsområden för certifikat

Utfärdaren producerar certifikattjänsterna enligt certificatpolicyn i villkoren i certifieringspraxisen och ansvarar för innehavaren av Signeringscertifikatet. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de tekniska leverantörer som utfärdaren anlitar. Det är en myndighet som upprätthåller ett personregister vars uppdrag enligt passlagen är att producera certifikattjänster för finska chipförsedda resedokument.

2.1 Certifikatutfärdare

Certifikatutfärdarens uppgifter är att

- Erbjuda sådana certifikat-, katalog-, spärr- och registreringstjänster enligt certifikatpolicyn och certifieringspraxisen som avses i passlagen.
- Identifiera den som ansöker om Signeringscertifikat.
- Se till att datainnehållet i certifikaten är felfria.
- Att sörja för spärrning av certifikat och publicering av spärrlistor.
- Iaktta en god dataskyddsnivå vid behandlingen av uppgifter om certifikatinnehavaren samt en god informationsbehandlingssed.

Myndigheten för digitalisering och befolkningsdata fungerar som Certifikatutfärdare.

2.2 Registrerare

Registreringen av ett Signeringscertifikat sker med iakttagande av förfarandena i kapitel 3 i certifieringspraxisen.

- Registreraren handlar på uppdrag och ansvar av Certifikatutfärdaren.
- Registreraren följer Certifikatutfärdarens certifikatpolicy och certifieringspraxis.
- Registreraren identifierar Den som ansöker om Signeringscertifikat enligt certifieringspraxisen. Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med Certifikatutfärdaren.

Myndigheten för digitalisering och befolkningsdata fungerar som registrerare.

2.3 Innehavare av Signeringscertifikat

Ett Signeringscertifikat enligt certifieringspraxis beviljas finska staten, vars företrädare är Polisstyrelsen. Innehavaren av Signeringscertifikatet bör iaktta Certifikatutfärdarens certifikatpolicy och certifieringspraxis.

2.4 Förlitande part

En förlitande part är en person eller en organisation som litar på innehållet i certifikatet och som använder certifikatet för att granska elektroniska signaturer. En förlitande part ska kontrollera att det certifikat som används är i kraft, att certifikatet inte finns på spärrlistan och att certifikatkedjan är enhetlig.

2.5 Registertjänst

Registertjänsten är en offentlig Webbtjänst med ett register där alla beviljade certifikat av Utfärdaren, Signeringscertifikat och spärrlistor finns tillgängliga. Registertjänsten finns på ldap://ldap.fineid.fi.

Kontaktuppgifter till den myndighet som utfärdar pass:

Polisstyrelsen

Postadress

Bergsmansvägen 3

PL 1000 02150 ESBO

Växel 0295 480 181

E-post: CSCA.Finland@govsec.fi

Registratorskontorets e-post: kirjaamo.poliisihallitus@poliisi.fi

2.6 Användning av certifikat

Certifikatpolicyn innehåller krav som gäller skyldigheterna för Utfärdaren, registreraren, Innehavarens av Signeringscertifikatet och den förlitande parten samt frågor som gäller lagstiftning och lösning av eventuella konflikter.

Ändamålet med Signeringscertifikatet för chipförsedda pass är att verifiera den digitala signaturen för de uppgifter som lagras på identitetskortets chip. Den digitala signaturen säkerställer äktheten och integriteten hos de signerade uppgifterna, dvs. att säkerställa uppgifternas ursprung och att de inte har ändrats efter att passet utarbetades. Med Certifikatutfärdarens certifikat kontrolleras äktheten hos Signeringscertifikaten. Myndigheten för digitalisering och befolkningsdata garanterar att certifikatuppgifterna är korrekta.

3.Tekniska säkerhetsarrangemang

De tekniska säkerhetsarrangemangen beskrivs i detalj i certifieringspraxisen.

3.1 Skapa och spara nyckelpar

3.1.1 Skapa nyckelpar

Certifikatutfärdaren skapar sin privata signeringsnyckel och en offentlig nyckel som motsvarar den privata signeringsnyckeln. Utfärdarens privata nycklar förvaras i kryptografiska moduler. Utfärdaren ser till att utfärdarens privata nycklar inte kan röjas eller missbrukas. Säkerhetskopior tas på Certifikatutfärdarens privata nycklar på det sätt som fordras för den kritiska datasäkerheten.

Certifikatinnehavarens nyckelpar skapas och förvaras av certifikatinnehavaren i en kryptografisk modul enligt FIPS 140-2 klass 3.

3.1.2 Förnyande av nyckelpar

Den offentliga nyckeln till Signeringscertifikatet kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt Signeringscertifikat. Vid förnyelse av ett Signeringscertifikat iakttas samma rutiner som vid första ansökan om certifikat.

3.1.3 Förnyelse av nyckelpar efter att ett Signeringscertifikatet införts på spärrlistan

Den offentliga nyckeln till Signeringscertifikatet och motsvarande privata nyckel kan inte förnyas. Ett nytt nyckelpar förutsätter alltid ett nytt Signeringscertifikat. Vid förnyelse av ett Signeringscertifikat iakttas samma rutiner som vid första ansökan om certifikat.

3.1.4 Giltighetstiden för offentliga och privata nycklar

Signeringsnycklarna är giltiga i högst 3 månader. Ett Signeringscertifikats giltighetstid är fem år och tre månader. Ett Signeringscertifikat kan spärras under dess giltighetstid. Ett Signeringscertifikat kan användas för att verifiera en elektronisk signatur efter att certifikatet har gått ut eller spärrats, ifall den certifierade signaturen skapades innan certifikatet spärrades eller gick ut.

3.1.5 Nycklarnas användningsändamål

Fältet som fastställer användningsändamålet i certifikatets datainnehåll anger användningsändamålet för den nyckel som är kopplad till certifikatet (till exempel digital signatur). Användningen av nyckeln begränsas bara till användningsändamålet: en nyckel som är avsedd för digital signering ska således bara användas för detta ändamål.

Både Certifikatutfärdarens certifikat och Signeringscertifikatet avviker till vissa delar från ICAO:s rekommendationer.

Certifikatutfärdarens certifikat:

Ändamål: Signering av certifikat och spärrlistor.

I strid med ICAO:s rekommendationer är användningsändamålen för Certifikatutfärdarens certifikat också digitala signaturer och godkännanden.

Certifikatinnehavarens Signeringscertifikat:

Ändamål: Digital signatur

I strid med ICAO:s rekommendationer har Signeringscertifikatet en e-postadress i utvidgningen Subject Alternative Name.

4.Hantering av certifikatsystemets livscykel

Myndigheten för digitalisering och befolkningsdata upprätthåller en klassificering av mål och system för certifikattjänsterna, deras tryggande, prioritering och minimiunderhåll.

4.1. Övervakning av systemutvecklingen

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

4.2 Systemövervakning

För övervakningen av systemet sparar Certifikatutfärdaren loggar över händelserna i certifikatproduktionen, hanteringen av användarrättigheterna till Certifikatutfärdarens certifikatsystem, utrustningen i sin helhet, systemprogrammen och tillämpningarna jämte ändringar, säkerhetskopieringen och återställande av säkerhetskopior. Utfärdaren övervakar även de dokument som gäller verksamheten.

4.3 Hantering av säkerhet

Myndigheten för digitalisering och befolkningsdatas informationssäkerhet hanteras i enlighet med Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy och standarden ISO/IEC 27001. Datasäkerhetschefen hos Myndigheten för digitalisering och befolkningsdata eller en utomstående inspektör som är specialiserad på auditering av tekniska leverantörer i anslutning till certifikattjänster utför dataskyddsgranskningen. Granskningen görs minst en gång om året. Upptäckta avvikelser antecknas i granskningsrapporten och åtgärder vidtas enligt lagen, datasäkerhetsstandarden ISO/IEC 27001 och gällande leveransavtal.

I granskningarna beaktas inte bara den administrativa informationssäkerheten utan även olika serviceleverantörer bl.a. enligt följande indelning:

Spärrtjänst:

- informationssäkerhet
- personalsäkerhet
- fysisk säkerhet

Certifikatproduktion:

- arbetsfördelningar och var och ens uppgifter, personalsäkerhet
- fysisk säkerhet
- Säkerhet i anslutning till Certifikatutfärdarens nycklar
- System för produktion av certifikat och reservsystem
- informationssäkerhet

Registertjänst:

- de komponenter som används
- administrationsförbindelser
- underhåll av registret och verksamhet vid felsituationer
- personalsäkerhet
- informationssäkerhet
- fysisk säkerhet

5.Hantering av verksamhetens kontinuitet och behandling av undantagsfall

Myndigheten för digitalisering och befolkningsdata har en kontinuitets- och beredskapsplan som möjliggör kontinuiteten i Myndigheten för digitalisering och befolkningsdatas verksamhet. Beredskap för undantagssituationer är beskriven i certifieringspraxisen.

5.1 Certifikatutfärdarens privata nyckel har röjts eller Certifikatutfärdarens certifikat har spärrats

Certifikatutfärdaren uppger i certifieringspraxisen de åtgärder som certifikatinnehavarna, de förlitande parterna och registrerarna och Certifikatutfärdarens anställda ska vidta ifall Certifikatutfärdarens privata nyckel har röjts eller på annat sätt blivit oanvändbar.

I ett sådant fall antingen upphör Certifikatutfärdaren med sin verksamhet på det sätt som anges i certifieringspraxisen eller vidtar följande åtgärder:

a) Certifikatutfärdaren meddelar det inträffade till alla certifikatinnehavare, förlitade parter samt alla kunder med vilka utfärdaren har avtal eller som på grund av avtalsförhållandet eller myndighetsverksamheten annars har en sådan ställning gentemot utfärdaren att utfärdaren ska informera om saken.

b) Certifikatutfärdaren skapar en ny nyckel enligt kapitel 6 i certifieringspraxisen.

c) Samtliga gällande Signeringscertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade Signe-

ringscertifikatets giltighetstid har löpt ut. Information om att certifikatet har förts in på spärrlistan är offentligt tillgänglig senast tre vardagsdygn efter att begäran om spärrning har konstaterats vara giltig och godkänd.

d) Utfärdaren arkiverar uppgifterna för den tid som arkivlagen kräver samt följer även i övrigt arkivlagens bestämmelser om arkivering av uppgifter.

5.2 Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas datasäkerhetspolicy beaktas åtgärder som förorsakas av problem med den externa säkerheten. Myndigheten för digitalisering och befolkningsdata har fått informationssäkerhetscertifikatet ISO 27001, som ställer krav på Myndigheten för digitalisering och befolkningsdatas verksamhet även vid en eventuell katastrof. Myndigheten för digitalisering och befolkningsdata efterföljer i utfärdandet och underhållet av certifikat de förfaringssätt som fastställts för datasäkerheten.

6 Certifikat- och spärrlistprofiler

6.1 Tekniska uppgifter om certifikat

6.1.1 Certifikatutfärdarens certifikat

Certifikatutfärdarens certifikat utfärdas av CSCA Finland "Finland Country CA 5". Det är fråga om ett self signed-certifikat enligt den s.k. flat-modellen som rekommenderas av ICAO. Myndigheten för digitalisering och befolkningsdata sparar Certifikatutfärdarens certifikat i ett öppet nationellt register.

Nyckelparet i Certifikatutfärdarens certifikat är 512 bitar långt, signaturfunktionen är ECC och UTF8-kodning har använts i teckenuppsättningen, med undantag av C-fältet som är PrintableString.

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Subject:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Giltighet = 10 år, 3 månader (3650+92=3742 dygn)

Certifikatserienummers talområde = 10.400.000-

CRL-url = http://proxy.fineid.fi/crl/cscafinc.crl

6.1.2 Signeringscertifikat

Ett Signeringscertifikat för att signera pass, dvs. "Document Signer Certificate". Myndigheten för digitalisering och befolkningsdata sparar Signeringscertifikaten i ett öppet nationellt register.

ECC-nyckelparet på Signeringscertifikatet är 512 bitar långt, signaturfunktionen är BrainpoolP512r1 och UTF8-kod har använts i teckenuppsättningen

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Subject:

CN = ICAO Compliant Document Signer for Passports

O = Finland

C = FI

CPS-URL = Används inte

Giltighet = 5 år, 3 månader (1825+1+92+1=1919 dygn)

Användningstid för privat nyckel = högst 3 månader

Certifikatserienummers talområde = 10.400.000-

Primär CRL-url = http://proxy.fineid.fi/crl/cscafinc.crl

Sekundär CRL-url = https://pkddownload1.icao.int/CRLs/FIN.crl

6.1.3 Spärrlistprofil

Myndigheten för digitalisering och befolkningsdata sparar spärrlistorna i ett öppet nationellt register. Spärrlistorna undertecknas med CA:s nycklar och på dem används samma signaturalgoritm som den som används för CA. CA vid signering av ett CA-certifikat.

Issuer:

CN = CSCA Finland

OU = VRK

O = Finland

C = FI

Giltighetstid = 30 dygn

Next Update = 40 dygn

Den nya spärrlistan publiceras senast när den gällande spärrlistan upphör att gälla. Spärrlistan innehåller en uppgift om tidpunkten för publiceringen av nästa spärrlista.

7 Versionshantering

Sammanfattning av certifieringspraxis för Signeringscertifikat för Finlands chipförsedda pass, version 2.2.

Version	**Datum**	**Beskrivning / ändringar**
v 1.0	17.08.2006	Godkänd version 1.0.
v 2.0	27.05.2011	Godkänd version 2.0.
v 2.1	02.11.2023	Myndighetens namn har ändrats. De tekniska uppgifterna har uppdaterats, bl.a. 512-bit ECC-nyckel.
v 2.2	01.02.2024	Polisstyrelsens kommentarer har beaktats.