CERTIFIERINGSPRAXIS

för servicecertifikatet för Myndigheten för digitalisering och befolkningsdata och servicecertifikatet för social- och hälsovården

OID: 1.2.246.517.1.10.308.1
OID: 1.2.246.517.1.10.358.1
OID: 1.2.246.517.1.10.305.1
OID: 1.2.246.517.1.10.305.2
OID: 1.2.246.517.1.10.305.3
OID: 1.2.246.517.1.10.305.5

OID: 1.2.246.517.1.10.355.1
OID: 1.2.246.517.1.10.355.2
OID: 1.2.246.517.1.10.355.5
OID: 1.2.246.517.1.10.308.2

OID: 1.2.246.517.1.10.358.2
OID: 1.2.246.517.1.10.305.4
OID: 1.2.246.517.1.10.355.4
OID: 1.2.246.517.1.10.309.2
OID: 1.2.246.517.1.10.359.2

1.11.2025

Dokumenthantering

Ägare	
Utarbetats av	Ville Aarnio, Sanni Kytölä, Minna Kuusela
Granskats av	
Godkänts av	Mikko Pitkänen

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Version 1.0	1.6.2021/VA
v 1.1	Tillagd information om abonnentskyldighet, lagt till information ETSI QCP-w, ändrat maximal giltighetstid för ett certifikat, öka databasens CA: s skyldighet att ställa in sökarens domän	1.10.2021/VA
v 1.2	Uppdaterade versionen och länkarna till CPS dokument	29.9.2022/SK
v 1.3	Uppdaterade versionen	15.9.2023/MK
v 1.4	OID och uppgifter för stämpelcertifikatet har lagts till. Tidpunkten för utfärdande av servercertifikatet har korrigerats. Kommunikationsverkets föreskrift har ersatts med Traficoms föreskrift. VAHTI-anvisningen har ersatts med lagen om informationshantering inom den offentliga förvaltningen. I punkt 5.1 har ett omnämnande av stämpelcertifikatet lagts till. Punkterna 5.3.4 och 5.3.5 har lagts till. Till punkt 6.4 har fogats en ansvarsbegränsning som gäller skada till följd av force majeure. Uppdaterat versionerna av standarden FIPS 140. Certifikatets utfärdandetid har korrigerats i punkt 7.3.1. Tillägg av punkten Spärrning av certifikat av Myndigheten för digitalisering och befolkningsdata. Tillägg i punkt 7.3.3.3 Stämpelcertifikat och 7.3.3.4 Stämpeltjänstens gränssnittscertifikat (praxis för namngivning av certifikatinnehavaren).	8.1.2024/AG
v 1.5	Tillagd information om OU-fältet i punkt 7.3.3.1.	31.1.2024/AG

v 1.6	Tillagt information om tidsstämpel certifikat	1.11.2024/ MK
v 1.7	Uppdaterad eIdas2, Nis2, tillagd information om massavstängningsplanen 7.3.7 och förtydligad beskrivning av skapandet av certifikatutfärdarens privata nyckel 7.2.1.	1.11.2025/ MK

Innehållsförteckning

CERTIFIERINGSPRAXIS

1 Allmänt

I detta dokument definieras Myndigheten för digitalisering och befolkningsdatas – här efter certifikatutfärdaren (Certification Authority) – förutsättningar för certifieringsfunktioner enligt öppet nyckelsystem (Public Key Infrastructure; PKI) samt tillämpningsområde och begränsningar för detta dokument. Principerna i detta dokument fastställs på praktisk nivå i denna certifieringspraxis och i de övriga anvisningarna för förfaringssätt som kompletterar detta dokument.

Om myndighetens namnbyte har stadgats i lagen om Myndigheten för digitalisering och be-folkningsdata (304/2019). Befolkningsregistercentralens namn ändrade 1.1.2020 till Myndigheten för digitalisering och befolkningsdata (MDB).

Servercertifikaten beskrivna i detta document uppfyller certifikatpolicyn ETSI QCP-w (0.4.0.194112.1.4) för EU-kvalificerade certifikat för autentisering av webbsidor.

MDB upprätthåller en certifikattjänst på godkänd nivå som tillhandahåller kvalificerade certifikat i enlighet med eIDAS-förordningen för sina följande produkt: servercertifikat. MDB agerar som certifikatutfärdare på den europeiska inre marknaden enligt Europaparlamentets och rådets förordning (EU) 2024/1183, känd som eIDAS2.

Denna certifieringspraxis tar även hänsyn till de krav som ställs i NIS2-säkerhetsdirektivet.

Alla punkter i certifikatpolicyn och certifieringspraxisen kan ändras genom att de huvudsakliga framtida ändringarna anmäls 30 dagar innan ändringarna träder i kraft. Punkter som myndigheten för digitalisering och befolkningsdata anser inte har någon betydande inverkan på certifikatinnehavare och betrodda parter, kan ändras genom att de meddelas 14 dagar tidigare.

2 Referensförteckning

2.1 Riktgivande referenser

I skapandet av utfärdarens PKI har man utgått från följande bestämmelser, standarder och anvisningar:

[1] Lag om stark autentisering och betrodda elektroniska tjänster (617/2009)

[2] Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)

[3] Lag om offentlighet i myndigheternas verksamhet (621/1999)

[4] IETF RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (11/2003)

[5] ETSI TS 102 042 V2.4.1: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (2010-04)

[6] Traficoms föreskrift M 72B/2022

[7] Lag om informationshantering inom den offentliga förvaltningen (906/2019)

[8] ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

Vid tolkningen av dokumentet iakttas följande principer:

1. Rubriker och underrubriker i certifieringspraxisen är i huvudsak översättningar av rekommendationer i internationella standarder [RFC 3647]. Vid tolkning av dokumentet ska själva texten prioriteras framför rubrikerna.

2. Ett allmänt krav för certifikatutfärdare är att de uppfyller samtliga krav på utfärdare av certifikat i denna certifikatpolicy.

2.2 Informativa referenser

De dokument som nämns här näst är inte oumbärliga för användningen av detta dokument, men de kan underlätta för användaren inom vissa ämnesområden. Om referensen inte är specifik tillämpas den senaste versionen av dokumentet (inklusive revisioner).

Europaparlamentets och rådets förordning (EU) nr 2024/1183 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.

3 Definitioner och förkortningar

3.1 Definitioner

Attributdata: permanenta uppgifter som fordras för autentisering av yrkesutbildade personer och konstaterande av yrkesrättigheter.

Elliptisk kurvkryptografi (ECC): metod för kryptering av offentlig nyckel baserad på den algebrala strukturen av elliptiska kurvor över ändliga fält.

Elektronisk stämpel: autentiserar elektroniska innehållets ursprung, samt att innehållet är oförändrat.

Nyckelpar: Nycklar som används tillsammans inom ett öppet nyckelsystem, varav den ena är publik och den andra privat. Nycklarnas användningssyfte är fastställt i certifikatet. OBS! Se kapitel 4.3

Icke-symmetrisk kryptering: Vid icke-symmetrisk kryptering används ett nyckelpar med en publik och en privat nyckel. Ett meddelande som krypterats med publik nyckel kan endast öppnas med den privata nyckeln i nyckelparet i fråga.

Certifikatpolicy som tillämpas på Extended Validity-certifikat (EV): normaliserad certifikatpolicy (NCP), som utvidgats enligt kraven i EVCG [11]-anvisningarna.

Registertjänst: En offentlig webbtjänst som innehåller samtliga certifikat beviljade av utfärdaren samt utfärdarens certifikat och spärrlistor.

Publik nyckel: Den publika delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatutfärdaren bekräftar med sin digitala signatur att den publika nyckeln innehas av certifikatets innehavare. Den publika nyckeln är en del av certifikatets datainnehåll.

Öppet nyckelsystem: Dataskyddsinfrastruktur där dataskyddstjänster produceras med ett öppet nyckelsystem.

Öppet nyckelsystem: Dataskyddstjänst, exempelvis elektronisk identifiering av personer, som produceras genom att använda publika och privata nycklar, certifikat och icke-symmetrisk kryptering.

Förlitande part: Den part som litar på uppgifterna i certifikatet och använder certifikatet för olika dataskyddstjänster, såsom elektronisk autentisering av certifikatets innehavare och konstaterande av digital signatur. OBS! Se RFC 3647.

OCSP-tjänst: Online Certificate Status Protocol. Tjänst där man kan kontrollera certifikatets status i realtid.

Servercertifikat: Servercertifikat, som används för att identifiera servern och skapa en SSL-/TLS-krypterad datatrafikförbindelse mellan servrar. Exempelvis ett certifikat skapat för www-server, som användaren kan använda för att försäkra sig om att servern är pålitlig. En datahelhet som utgörs av serviceproducentens publika nyckel inom ett öppet nyckelsystem och identifieringsuppgifter, som certifikatutfärdaren har skapat och signerat med sin privata nyckel.

Servicecertifikat för kommunikation: Filbaserat certifikat för användning exempelvis för mottagning och sändning av krypterade meddelanden med en gemensam e-postadress.

Servercertifikat: Ett gemensamt namn för server- och e-postservercertifikat

Systemsignaturcertifikat: autentiserar elektroniska innehållets ursprung, samt att innehållet är oförändrat.

Registrerare: Registreraren identifierar i enlighet med den certifikatsökandes certifikatpolicy och certifieringspraxis för utfärdarens del och på dennes ansvar.

RSA-algoritm och RSA-nyckel: RSA-algoritm är en allmänt använd algoritm för publik nyckel. I servercertifikatet ingår privata och publika RSA-nycklar eller ECC-nycklar.

Skyddad användarutrustning: utrustning som förvarar användarnas privata nyckel, skyddar denna nyckel och utför signering eller dekrypteringsfunktioner för användarens del.

Spärrlista (CRL): En förteckning som signeras och publiceras elektroniskt av certifikatutfärdaren över certifikat som spärrats under deras giltighetstid och tidpunkten för spärrning. Av spärrlistan framgår publiceringstidpunkt samt tidpunkten för publiceringen av nästa spärrlista. Spärrade certifikat förs in på spärrlistan. OBS! Se ITU-T Rekommendation X.509.

Spärrtjänst: Utfärdarens tjänst, där utfärdaren tar emot begäranden om att spärra certifikat, spärrar certifikat och förmedlar information om att ett certifikat spärrats till certifikatsystemet.

Digital signatur: en PKI-signatur i samband med ett elektroniskt meddelande, som kan användas för stark autentisering av meddelandets innehåll och signerarens identitet.

Certifikat: Ett elektroniskt intyg som kopplar uppgifterna om verifieringen av en signatur till den som gjort signaturen och bekräftar signeraren. Certifikatet innehåller en medföljande unik kod enligt certifieringspraxis.

Certifikatsystem: Ett datatekniskt system för att skapa certifikat, underteckna spärrlistor och publicera dem i registret.

Certifikatbeskrivning: Dokumentet innehåller de centrala delarna av certifikatpolicyn och certifieringspraxisen.

Certifikatpolicy: Ett dokument där man beskriver principerna för beviljande av certifikat samt ansvarsområdena för de förlitande parterna. Myndigheten för digitalisering och befolkningsdatas publicerade certifikatpolicyer är offentligt tillgängliga. Varje policy identifieras av en egen kod.

Certifikatdatasystem: Ett datatekniskt system som utgörs av certifikatsystem, datatrafik, certifikatregister och spärrlista, rådgivnings- och spärrtjänst samt hantering av certifikat och kort.

Certifieringspraxis: Beskrivning av hur certifikatutfärdaren förverkligar sin certifikatpolicy. Varje certifieringspraxis identifieras av en egen kod. Den identifierande koden inom certifieringspraxisen är en del av certifikatets datainnehåll.

Certifikatutfärdare: Organisationen som beviljar certifikat, som svarar för produktionen av certifikat samt utarbetar certifikatpolicy och certifieringspraxis som beskriver organisationens verksamhet. OBS! Se kapitel 4.1

Certifikatutfärdarens certifikat: Innehåller utfärdarens namn, land och publika nyckel.

Utfärdarens privata nyckel: En privat nyckel som beviljas av certifikatutfärdaren för signering av utfärdarens beviljade certifikat och publicerade spärrlistor.

Certifikatsökande: Organisation som ansöker om certifikat och pålitligt identifieras i samband med detta.

Innehavare av certifikat: En organisation vars data och publika nyckel har bekräftats med utfärdarens elektroniska signatur och som innehar den privata nyckeln för certifikatet.

Användning och användningssyfte för certifikat: I detta dokument avses med användning av certifikat såväl användning av själva certifikatet som användning av medföljande nycklar. Exempelvis avses med användning av certifikat vid digital signering såväl användning av den privata nyckeln vid signeringen som användning av den publika nyckeln och certifikatet vid autentisering av signatur.

Time Stamp Unit/Time Stamp Server (TSU/TSS): en hård- och mjukvaruenhet som hanteras som en enhet och där en signeringsnyckel för tidsstämpeltoken är aktiv åt gången.

Timestamp Token (TST): Ett dataobjekt som binder tiden till en specifik tid i representationen, vilket indikerar att tiden existerade före den tiden.

Tidstämpelcertifikat: ett tillförlitligt verifierat exakt datum undertecknas med ett tidsstämpelcertifikat.

Privat nyckel: Den privata delen av nyckelparet som används för icke-symmetrisk kryptering i ett öppet nyckelsystem. Certifikatinnehavarens privata nyckel sparas i en trygg miljö för att skydda denna från otillbörlig användning.

3.2 Förkortningar

CA Certification Authority, certifikatutfärdare

CP Certificate Policy, certifieringspolicy

CPS Certification Practise Statement, certifieringspraxis

CRL Certificate Revocation List, spärrlista

CSP Certification Service Provider, certifikatutfärdare

ECC Elliptic Curve Cryptography

FINEID Finnish Electronic Identification, finländskt elektroniskt identifieringssystem

HSM Hardware Security Module, kryptografisk modul

HTTP Hypertext Transfer Protocol

ISO/IEC 27001 Internationell standard för hantering av informationssäkerhet

LDAP Lightweight Directory Access Protocol

OID Object Identifier, identifierande kod

PDS PKI Disclosure Statement, certifikatbeskrivning

PKI Public Key Infrastructure, öppet nyckelsystem

RSA Rivest, Shamir, Adleman, en algoritm för publik nyckel, icke-symmetrisk algoritm

SSL Secure Socket Layer

TSA Timestamp authority – in this document this refers to the Digital and Population Data Services Agency (also CA Certification Authority)

TSS Timestamping service

TLS Transport Layer Security

MDB Myndigheten för digitalisering och befolkningsdata

4 Allmänna begrepp

4.1 Certifikatutfärdare

Utfärdaren är den instans som beviljar och skapar certifikat som användarna av certifikattjänster (dvs. beställarna och de förlitande parterna) litar på. Utfärdaren bär helhetsansvaret för att erbjuda de certifikattjänster som fastställs i punkt 4.2. Utfärdaren är specificerad i certifikatet som beviljare av certifikatet, och kvalificerade certifikat signeras med utfärdarens privata nyckel.

Utfärdaren kan anlita övriga partner inom sina certifikattjänster, som erbjuder delar av tjänsten. Utfärdaren innehar alltid helhetsansvaret och säkerställer att de förfaringssätt som fastställs i detta dokument förverkligas. Utfärdaren kan exempelvis införskaffa samtliga deltjänster av underleverantörer, även tjänster för skapande av certifikat. Nyckeln som används för att signera certifikaten innehas dock av utfärdaren och utfärdaren har helhetsansvaret för att de krav som fastställs i detta dokument uppfylls och för de certifikat som utfärdas för allmänheten.

Utfärdaren beviljar certifikat och uppfyller följande villkor:

- Utfärdaren förbinder sig att iaktta villkoren i certifikatpolicyn.
- Utfärdaren utarbetar certifieringspraxis och övriga förfaringssätt som kompletterar certifikatpolicyn.
- Certifikatutfärdaren ska ha tillräcklig ekonomisk beredskap för att trygga den verksamhet som anges i certifikatpolicyn och certifieringspraxisen. Utfärdaren svarar för certifikatverksamheten och anknytande risker och utgår från att leverantörerna inom certifikatsystemet garderar sig mot risker i verksamheten med hjälp av lämpliga metoder för riskhantering.
- Certifikatutfärdaren för register över registrerare som är godkända av utfärdaren.
- Utfärdaren beslutar om korscertifiering i samråd med övriga utfärdare.

- Certifikatutfärdaren svarar för livscykeln hos nyckelpar som är genererade av utfärdaren (generering, lagring, säkerhetskopiering, publicering och återkallande).

Certifikatutfärdaren förbinder sig att:

1. tillhandahålla de certifikat-, register- och spärrtjänster som fastställs i certifikatpolicyn;
2. erbjuda hanterings- och uppföljningsfunktioner enligt vad som beskrivs i kapitel 4 till 6 i denna certifieringspraxis;
3. pålitligt identifiera certifikatsökande;
4. bevilja certifikat i enlighet med denna certifieringspraxis;
5. efterleva gällande lagar och förordningar och bestämmelser och riktlinjer enligt dessa samt främja rättigheterna för användare av certifikat och förlitande parter;
6. se till att tillräckliga och oberoende kontroller i enlighet med certifieringspraxis utförs;
7. svara för att certifikatutfärdarens verksamhet fungerar; och
8. iaktta alla villkor i certifikatpolicyn och denna certifieringspraxis.

Utfärdaren kan välja att erbjuda extra funktioner eller tjänster som anknyter till certifikatsystemet.

Utfärdaren svarar för att informationen i certifikatet överensstämmer med denna certifieringspraxis.

4.2 Certifikattjänster

4.2.1 Registrerare

Registrerare som stöder sig på denna certifikatpolicy ska uppfylla följande villkor:

- Registreraren förbinder sig till att uppfylla kraven i denna certifieringspraxis.
- Registreraren ska vara godkända och registrerad av utfärdaren.
- Registreraren ansvarar för identifiering av certifikatsökande.
- Registreraren ansvarar för att man kan lita på personalen som arbetar vid registreringsinstansen. Registreraren införskaffar utredningar om personal som anställs enligt utfärdarens krav för att säkerställa att de går att lita på och ser till att ständigt försäkra sig om att man kan lita på den personal man

befullmäktigat. Utfärdaren godkänner personalen vid registreringsinstansen utgående från registrerarens utredningar.

Registrerare ska enligt certifikatpolicyn förbinda sig till att:

1. efterleva gällande lagstiftning samt bestämmelser och riktlinjer enligt denna;
2. erbjuda hanterings- och uppföljningsfunktioner enligt vad som fordras i kapitel 4 till 6 i denna certifieringspraxis;
3. utföra identifieringsförfarande för certifikatsökandet enligt kapitel 4 till 6 i denna certifieringspraxis samt enligt certifikatpolicyn och lämna uppgifterna om certifikatsökanden till utfärdaren för skapande av certifikat;
4. fullfölja avtalade uppdrag och stödja certifikatanvändares och förlitande parters rättigheter; och
5. iaktta alla de villkor i denna certifikatpolicy och certifieringspraxisen som gäller registreringstjänsten.

Registreraren kan erbjuda extra funktioner eller tjänster som har godkänts av certifikatutfärdaren. Registreraren svarar för alla registreringstjänster som tillhandahålls av registreraren. Registrerare för servercertifikatet är Myndigheten för digitalisering och befolkningsdata.

4.2.2 Spärrtjänst

Utfärdarens spärrtjänst spärrar servercertifikat på innehavarens eller utfärdarens önskemål innan certifikatets giltighetstid har löpt ut. Spärrade servercertifikat förs in på spärrlistan. Orsaken till spärrning av servercertifikat kan exempelvis vara att innehavarens privata nyckel har röjts eller att det finns misstanke om detta.

4.2.3 Registertjänst

Registertjänsten är en offentlig webbtjänst som innehåller samtliga certifikat beviljade av utfärdaren samt utfärdarens certifikat och spärrlistor. Registertjänsten är tillgänglig på adressen ldap://ldap.fineid.fi.

4.3 Certifikatpolicy och certifieringspraxis

4.3.1 Syfte

Certifikatpolicy är en beskrivning av förfaringssätt och verksamhetsprinciper som efterlevs vid beviljande av certifikat, som utarbetas av utfärdaren. Certifieringspraxis är en mer detaljerad beskrivning av utfärdarens verksamhet.

4.3.2 Detaljer

I verksamhetspraxis beskrivs mer ingående än i certifikatpolicyn åtgärder som utfärdaren utför vid beviljande av certifikat och inom den övriga förvaltningen. Här fastställs hur en viss utfärdare uppfyller de tekniska kraven i certifikatpolicyn samt kraven på organisationen och förfaranden.

4.3.3 Approach

Certifikatpolicy och certifieringspraxis skiljer sig i hög grad i sin approach. Certifikatpolicyn utarbetas oberoende av detaljerna i en viss utfärdares verksamhetsmiljö. Certifieringspraxisen utarbetas för sin del i enlighet med en viss utfärdares organisationsstruktur, förfaringssätt, verksamhetslokaler och datatekniska miljö. Certifikatpolicyn kan fastslås av användaren av certifikattjänster, men certifieringspraxisen fastställs alltid av leverantören av certifikat.

4.3.4 Övriga dokument som publiceras av utfärdaren

Utöver certifikatpolicyn och certifieringspraxisen kan utfärdaren även publicera övriga dokument som gäller utfärdarens verksamhet. Dessa användarvillkor kan innehålla kommersiella villkor av olika slag eller gälla exempelvis ett visst öppet nyckelsystem. Även om man inte nödvändigtvis informerar kunden om dessa villkor, kan de ändå tillämpas.

Certifikatbeskrivningen är en del av utfärdarens användarvillkor, som gäller verksamheten i ett öppet nyckelsystem. Utfärdaren bör göra certifikatbeskrivningen tillgänglig för såväl beställarna som de förlitande parterna.

4.4 Beställare och signerare

Med "Beställare" avses den instans som ansöker om certifikat av utfärdaren och har ett avtalsförhållande med utfärdaren (organisation eller privatperson). Med "Signerare" avses den instans som beviljats certifikatet (organisation eller privatperson). Beställaren bär ansvar för användningen av den privata nyckeln i anslutning till certifikat med publik nyckel. Signeraren är den person som kan identifieras med den privata nyckeln och som använder den privata nyckeln.

Exempelvis då certifikat beviljas till anställda, är beställaren och signeraren olika instanser. Då kan en arbetsgivare vara beställare och en anställd signerare.

I detta dokument används dessa två termer för att åskådliggöra skillnaden vid behov. I samtliga fall är skillnaden i fråga dock inte tydlig.

5 Inledning om certifikatpolicydokument

5.1 Allmänt

Certifikatpolicy är en beskrivning av förfaringssätt och verksamhetsprinciper som efterlevs vid beviljande av certifikat, som utarbetas av utfärdaren. Certifieringspraxis är en mer detaljerad beskrivning av utfärdarens verksamhet.

Certifieringspraxis tillämpas på Myndigheten för digitalisering och befolkningsdatas servicecertifikat. Servercertifikat är ett certifikat som beviljas av Myndigheten för digitalisering och befolkningsdata och som används för att autentisera serviceleverantörens server eller tjänst.

Ett certifikat är en uppsättning data som kopplar samman identifikationsuppgifter i samband med autentisering eller kryptering med innehavaren av certifikatet och autentiserar innehavaren av servercertifikatet. Certifikatets uppgifter har signeras digitalt med certifikatutfärdarens privata nyckel. Certifikat enligt denna certifieringspraxis utgår från öppet nyckelsystem (PKI). Servercertifikatet för ärendehantering är ett filbaserat certifikat med flera undertyper. Dessa är ett e-postcertifikat som levereras i filformatet PKCS #12 och som är avsett för kryptering och signering av e-post, ett kundcertifikat ör BDS-gränssnittet som är avsett för serverärenden, ett systemsignaturcertifikat för signering av uppgifter, ett stämpelcertifikat för stämpling av uppgifter samt ett gränssnittscertifikat för användning av stämpeltjänsten.

Myndigheten för digitalisering och befolkningsdatas certifieringspraxis har en egen unik kod (OID). Utfärdarens funktioner är att producera och registrera certifikat-, register- och spärrtjänster. Dessa funktioner beskrivs närmare i kapitel 4.2.

5.2 Individuella koder

I servercertifikatet ingår tre identifierande koder (OID). De övriga certifikattyperna har två identifierande koder. Den ena koden beskriver vilken ETSI TS 102 042 certifikatpolicy som iakttas för certifikatet och den andra är den individuella koden för certifieringspraxisen. Den tredje koden i servercertifikatet beskriver att i certifikatet följs CA/Browser Forum Baseline Requirements -krav.

Dessutom har certifikatpolicyn en egen individuell MDB-kod, som fastställer certifikatpolicyn.

Individuella koder är:

OID för eIDAS (EU 910/2014) ETSI EN 319 401, ETSI EN 319 411-1 ja ETSI EN 319 411-2:

OID för certifieringspraxis för MDB:s servercertifikat: 1.2.246.517.1.10.305.1 och 1.2.246.517.1.10.355.1.

OID för certifikatpolicyn för MDB:s servercertifikat: 1.2.246.517.1.10.305 och 1.2.246.517.1.10.355.

MDB:s social- och hälsovårds servicecertifikat, certifikatpolicys OID: 1.2.246.517.1.10.308 och 1.2.246.517.1.10.358

Myndigheten för digitalisering och befolkningsdatas servercertifikat för uträttande av ärende, certifikatpraxis OID: 1.2.246.517.1.10.305.2

MBD's elektronisk stämpel certifikat OID: 1.2.246.517.1.10.305.5 and 1.2.246.517.1.10.355.5

MBD:s tidsstämpel certifikat OID: 1.2.246.517.1.10.309.2 och 1.2.246.517.1.10.359.2

MDB:s servercertifikat för social- och hälsovårds servercertifikat, certifikatpraxis OID: 1.2.246.517.1.10.308.1 och 1.2.246.517.1.10.358.1

MDB:s för social- och hälsovårds servercertifikat för uträttande av ärende, certifikatpraxis OID: 1.2.246.517.1.10.308.2 och 1.2.246.517.1.10.358.2

MDB:s servercertifikat för hälsoapplikationstjänsters OID: 1.2.246.517.1.10.304.4 och 1.2.246.517.1.10.355.4

0.4.0.194112.1.4 = eIDAS QWAC-servercertifikat = {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web(4)}

0.4.0.2042.1.7 = ETSI Organization Validated Certificate Policy (OVCP) = {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp(7)}

2.23.140.1.2.2 = CA/B Forum Baseline Requirements Organization Validated = {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}

Certifikatpolicyn, dess certifikatbeskrivning och certifieringspraxis finns på adressen https://dvv.fi/sv/certifikatpolicydokument.

5.3 Användarsamfund och tillämpningsbarhet

I enlighet med denna certifieringspraxis är servercertifikatets användningssyften att autentisera servern och kryptera datatrafik. Certifikatet kan användas i enlighet med användningssyftet utan begränsningar inom förvaltningen samt i applikationer och tjänster som erbjuds av organisationer.

Certifikatpolicyn och certifieringspraxisen innehåller krav som gäller skyldigheterna för utfärdaren, registreraren, innehavaren och den förlitande parten samt frågor som gäller lagstiftning och lösning av eventuella konflikter.

5.3.1 Servercertifikat

Servercertifikatens syften är att identifiera servern och kryptera datatrafiken. Certifikatet kan i enlighet med sitt användningsändamål användas utan begränsningar i administrativa applikationer och tjänster.

5.3.2 Servicecertifikat för uträttande av ärenden (Systemsignaturcertifikat)

Servicecertifikaten för uträttande av ärenden är avsedda för att säkerställa det digitala innehållets ursprung och oföränderlighet. Med certifikatet för systemsignaturer signeras elektroniskt sådana dokument som inte signeras med personcertifikat.

5.3.3 BDS-gränssnittets kundcertifikat

BDS-gränssnittets kundcertifikatet är ett certifikat för kundanvändning av gränssnittet (client) för Myndigheten för digitalisering och befolkningsdatas egna BDS-kunder.

5.3.4 Stämpelcertifikat

Stämpelcertifikat är en juridisk persons personcertifikat som används för att stämpla handlingar i elektroniskt format. Med hjälp av stämpelcertifikatet kan man garantera den stämplade informationens ursprung, oföränderlighet och obestridlighet.

5.3.5 Stämpeltjänstens gränssnittscertifikat

Stämpeltjänstens gränssnittscertifikat är ett certifikat för kundanvändning (client) av stämpeltjänstens gränssnitt för MDB:s stämpeltjänstkunder.

5.3.6 Tidsstämpel certifikat

Tidsstämpelcertifikatet används för att signera en tillförlitligt verifierad tidstoken. Tidsstämpelcertifikat utfärdas i MBD:s namn och MBD erbjuder sedan kunderna en tidsstämplingstjänst.

5.4 Överensstämmelse med krav

5.4.1 Allmänt

Utfärdaren producerar certifikattjänster enligt villkoren i certifieringspraxisen och ansvarar för att de fungerar i innehavarens användning. Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar. Denna certifieringspraxis är registrerad av Myndigheten för digitalisering och befolkningsdata. Certifikatpolicydokumenten publiceras på adressen https://dvv.fi/sv/certifikatpolicydokument där de är tillgängliga för allmänheten. Utfärdarens verksamhet auditeras årligen samt vid större förändringar i systemet. En certifikatauditeringsrapport är tillgänglig på begäran.

Dataskyddsgranskning

Myndigheten för digitalisering och befolkningsdata utför en dataskyddsgranskning för de tekniska leverantörernas lokaler, utrustning och verksamhet på ett ändamålsenligt sätt.

Myndigheten för digitalisering och befolkningsdatas dataskyddsgranskning utförs av en utomstående inspektör som är oberoende av utfärdaren.

Målen för granskningen fastställs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller, om Myndigheten för digitalisering och befolkningsdata utför granskningen, i enlighet med informationssäkerhetsstandarden ISO 27001, Myndigheten för digitalisering och befolkningsdatas informationssäkerhetspolicy eller tekniska leveransavtal. Dataskyddsegenskaper som kontrolleras är bl.a. konfidentialitet, integritet och användbarhet.

Vid granskningen kontrolleras överensstämmelsen hos certifikatpolicyn, certifieringspraxis och anvisningar för tillämpning med ETSI TS 102 042-standarden inom hela certifikatorganisationen och certifikatsystemet.

Åtgärder vid avvikelser

Upptäckta avvikelser antecknas i granskningsrapporten och man reagerar på dessa enligt lagen, dataskyddsstandarden ISO 27001 och gällande leveransavtal.

Information om resultatet av granskningen

Man informerar om resultatet av granskningen i enlighet med lagen, dataskyddsstandarden ISO 27001, Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och gällande leveransavtal. Det detaljerade och standardiserade granskningsresultatet avsett för intern användning är konfidentiellt och offentliggörs inte. Rapporter med på förhand bestämd utformning utarbetas separat för användning utanför organisationen.

Arkivering av granskningsmaterial

Utfärdaren arkiverar granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet. Det arkiverade materialet förvaras enligt bestämmelserna för myndigheter som fungerar som utfärdare.

Planer och policy för utfärdarens verksamhet samt utfärdarens skyldigheter vid undantagsfall eller störningar beskrivs i punkt 7.4.8. Hantering av kontinuerlig verksamhet och undantagsfall

5.4.2 Krav på överensstämmelse med krav

Utfärdarens skyldigheter beskrivs i punkt 6.1. Utfärdarens verksamhet uppfyller kraven i punkt 6.1 Dessutom uppfyller utfärdarens verksamhet och tillsynen av verksamheten de krav som specificeras i punkt 7.

6 Skyldigheter, ansvar och ansvarsbegränsningar

6.1 Certifikatutfärdarens skyldigheter

Utfärdaren svarar för att hela certifikatsystemet fungerar samt för de registrerare och tekniska leverantörer som utfärdaren anlitar.

- Myndigheten för digitalisering och befolkningsdata har ett lagstadgat uppdrag att fungera som certifikatutfärdare.
- Utfärdaren efterlever i sin verksamhet gällande lagstiftning.
- Utfärdaren agerar omsorgsfullt, pålitligt och ändamålsenligt.
- Utfärdaren har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt hantera eventuella krav på skadeersättning.
- Utfärdaren svarar för samtliga delområden av certifikatverksamheten, även för pålitligheten och funktionaliteten hos tjänster och produkter som produceras av tekniska leverantörer och personer som man anlitar.
- Utfärdaren utarbetar och upprätthåller en certifikatpolicy, som beskriver förfaringssätt, användarvillkor och ansvarsfördelning för beviljande av servercertifikat samt övriga aspekter av användningen av servercertifikatet på ett allmänt plan.
- Utfärdaren utarbetar och underhåller en certifieringspraxis som beskriver hur utfärdaren tillämpar certifikatpolicyn.
- Utfärdaren uppfyller kraven enligt certifikatpolicyn och certifieringspraxisen.
- Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen och gör dem allmänt tillgängliga.
- Utfärdaren anställer tillräckligt med personal med den expertis, erfarenhet och kompetens som fordras för produktionen av certifikattjänster.
- Utfärdaren använder pålitliga system och produkter som är skyddade från otillbörlig användning.
- Utfärdaren tillhandahåller offentligt information om certifikat och certifikatverksamheten, utgående från vilken utfärdarens verksamhet och pålitlighet kan bedömas.

Registrerarens skyldigheter

Registrerare för servercertifikatet är Myndigheten för digitalisering och befolkningsdata.

- Registreraren efterlever certifikatpolicyn och certifieringspraxisen i samband med registreringen.
- Registreraren identifierar servercertifikatsökanden med stark autentisering på det sätt som beskrivs i certifieringspraxisen, på så sätt att sökandens identitet, rätt att ansöka om servercertifikat samt övriga uppgifter som fordras för beviljande av servercertifikat noga kontrolleras.
- Registreraren ser till att uppgifterna hanteras omsorgsfullt och konfidentiellt.
- Registreraren iakttar de förfaringssätt för registreringen som man kommit överens om med utfärdaren.

6.2 Certifikatbeställarens och certifikatinnehavarens skyldigheter

- Innehavaren av servercertifikatet ansvarar för att certifikatet används i de användningssyften som anges i ansökan om servercertifikat samt i enlighet med certifikatpolicyn, certifieringspraxisen och de bindande avtalsvillkoren för certifikatinnehavare.
- Myndigheten för digitalisering och befolkningsdata kan även bevilja servercertifikatet för egna syften. Då efterföljer den samma krav som de övriga organisationerna.
- Certifikatinnehavaren (serviceleverantören) ansvarar för att de uppgifter som uppges då man ansöker om certifikatet är riktiga.
- Certifikatinnehavaren ska förvara sin privata nyckel i en trygg miljö och sträva efter att förhindra att den försvinner, kommer i obehöriga personer händer, förändrats eller används på otillbörligt sätt.
- Certifikatinnehavaren ska omedelbart informera utfärdaren om man känner till eller misstänker att certifikatinnehavarens privata nyckel har röjts eller att certifikatets informationsinnehåll är felaktigt. I detta fall spärrar utfärdaren certifikatet i fråga och samma privata nyckel kan inte användas för att skapa ett nytt certifikat.
- Certifikatinnehavarens ansvarar för användningen av ett certifikat upphör när innehavaren har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Samtliga gällande servercertifikat som beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade servercertifikatets giltighetstid har löpt ut.

Om den privata nyckeln eller annan teknisk metod som använts vid skapandet av Myndigheten för digitalisering och befolkningsdatas certifikat har röjts eller på annat vis blivit oanvändbar ska Myndigheten för digitalisering och befolkningsdata meddela det inträffade till samtliga innehavare av certifikat och Traficom på ändamålsenligt sätt.

Den som ansöker om servercertifikat lämnar in en certifikatbegäran som skapats på den server man vill certifiera till registreraren, utgående från vilken servercertifikatet skapas.

Utfärdarens privata nyckel som använts för signering av servercertifikatet och den motsvarande publika nyckeln är minst 4 096-bitars RSA-nycklar och 384-bitar ECC-nycklar.

Längden på den privata och offentliga nyckeln för ett servicecertifikat kan avgöras av den som ansöker om certifikatet. Nyckellängden för ett servicecertifikat som utfärdas av Myndigheten för digitalisering och befolkningsdata är RSA-certifikatet minst 2048 bitar och 256 bitar ECC-nycklar.
Beställaren av ett servicecertifikat har skyldighet att granska att det levererade certifikatets innehåll uppfyller beställningen och kvittera detta till certifikatets leverantör.

6.3 Den förlitande partens skyldigheter

Den part som litar på servercertifikatet är skyldig att säkerställa att certifikatet används enligt användningssyftet.

Den förlitande parten ska iaktta certifikatpolicyn och certifieringspraxisen.

Den förlitande parten kan i god tro lita på servercertifikatet efter att parten kontrollerat att certifikatet är i kraft och inte finns på spärrlistan. Det är också möjligt att kontrollera certifikatets status i realtid i en OCSP-tjänst. Förlitande parter svarar för kontrollen av gällande spärrlistor. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat de spärrade certifikaten på det sätt som beskrivs nedan.

Förlitande parter som hämtar spärrlistan i registret ska kontrollera spärrlistans integritet och autenticitet med stöd av utfärdarens digitala signatur. Dessutom ska förlitande parter kontrollera spärrlistans giltighetstid.

Om det på grund av störningar i systemet eller tjänsten inte går att få tillgång till en giltig spärrlista, får certifikat enligt denna certifieringspraxis inte godkännas, om giltighetstiden löpt ut för den senaste listan man fått tillgång till. Om en förlitande part ändå godkänner ett certifikat, sker det på den förlitande partens eget ansvar.

6.4 Ansvar och ansvarsbegränsningar

Certifikatutfärdarens ansvar

Myndigheten för digitalisering och befolkningsdata efterlever i sin servercertifikatverksamhet den gällande lagstiftningen i Finland.

Myndigheten för digitalisering och befolkningsdata svarar som utfärdare för säkerheten för hela certifikatsystemet. Utfärdaren svarar för införskaffade tjänster på samma sätt som om utfärdaren själv hade producerat tjänsten.

Myndigheten för digitalisering och befolkningsdata svarar för att servercertifikaten har skapats enligt de förfaranden som beskrivs i certifikatpolicyn och certifieringspraxisen och utgående från de uppgifter som certifikatsökanden lämnat. Myndigheten för digitalisering och befolkningsdata ansvarar endast för den information som man sparat i servercertifikatet.

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande samarbetsavtal och skadeståndslagen (412/1974) . Myndigheten för digitalisering och befolkningsdata omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Myndigheten för digitalisering och befolkningsdata svarar för att servercertifikatet är tillgängligt för användning från att det överlåts under hela dess giltighetstid, förutsatt att certifikatet inte spärras.

Myndigheten för digitalisering och befolkningsdata svarar för att servercertifikatet har överlåtits till en certifikatsökande, som autentiserats på det sätt som förutsätts för servercertifikat.

Vid signering av servercertifikatet med sin privata nyckel intygar certifikatutfärdaren att utfärdaren har kontrollerat uppgifterna i certifikatet med de metoder som beskrivs i servercertifikatpolicyn och certifieringspraxisen.

Utfärdaren ansvarar för att rätt servercertifikat förs in på spärrlistan och att det förs in på spärrlistan inom den tid som fastställs i certifieringspraxisen.

Registrerarens ansvar

Registrerare för servercertifikatet är Myndigheten för digitalisering och befolkningsdata eller dess avtalspartner för Myndigheten för digitalisering och befolkningsdatas räkning och på dess ansvar.

Certifikatinnehavarens ansvar

Innehavaren av servercertifikatet ansvarar för att certifikatet används i de användningssyften som anges i ansökan om servercertifikat.

Certifikatinnehavarens ansvarar för användningen av ett certifikat upphör när innehavaren har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Den förlitande partens ansvar

Den part som litar på servercertifikatet kan inte uppriktigt lita på certifikatet om den förlitande parten inte kontrollerat certifikatets giltighet på spärrlistan. Om servercertifikatet trots allt godkänns frias Myndigheten för digitalisering och befolkningsdata från ansvar. Den part som litar på servercertifikatet ska kontrollera att det beviljade certifikatet motsvarar användningssyftet i det funktioner det används för.

Begränsning av ansvar

Myndigheten för digitalisering och befolkningsdata svarar inte för eventuella skador eller kostnader som orsakas av att certifikatinnehavarens privata nycklar röjs, om inte röjningen direkt har orsakats av Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder.

Myndigheten för digitalisering och befolkningsdatas ansvar gentemot certifikatinnehavare och förlitande parter omfattar högst de direkta skador som har orsakats dem, om skadan beror på Myndigheten för digitalisering och befolkningsdatas omedelbara åtgärder, dock högst 15 procent av certifikatfaktureringen under de föregående tre månaderna (MDB:s andel).

Myndigheten för digitalisering och befolkningsdata svarar inte för indirekta skador eller följdskador som har orsakats certifikatinnehavaren. Myndigheten för digitalisering och befolkningsdata svarar inte heller för eventuella indirekta skador eller följdskador som orsakas förlitande parter eller andra avtalsparter för certifikatinnehavaren.

Myndigheten för digitalisering och befolkningsdata är inte ansvarig för funktionen i de allmänna teleförbindelserna eller datanäten, till exempel Internet, eller för att en rättshandling inte kan utföras på grund av att certifikatinnehavarens utrustning eller kortläsare inte fungerar eller för att certifikatet används i strid med sitt syfte.

Certifikatutfärdaren har rätt att vidareutveckla certifikattjänsten. Certifikatinnehavare eller förlitande parter ska i sådana fall svara för egna kostnader som följer av detta och utfärdaren är inte skyldig att ersätta certifikatinnehavare eller förlitande parter för kostnader som orsakas av utvecklingsarbetet.

Certifikatutfärdaren har rätt att avbryta tjänsten för den tid ändringar eller underhåll av systemet utförs. Om ändringar eller underhåll av spärrlistan meddelas på förhand.

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 detta orsakar.

Certifikatinnehavarens ansvar för användningen av ett certifikat upphör när innehavaren eller en representant för certifikatinnehavarens organisation har anmält till utfärdaren de uppgifter som är nödvändiga för spärrningen av certifikatet och efter att ha fått ett meddelande av den funktionär som mottagit samtalet om att certifikatet har upptagits på en spärrlista. För att ansvaret ska upphöra måste spärranmälan göras omedelbart när det har konstaterats att skäl för anmälan föreligger.

Certifikatutfärdaren ansvarar inte för skada som orsakas av force majeure. Ett sådant hinder som befriar från ansvar kan vara till exempel strejk, eldsvåda, krig, uppror, beslag, valutabegränsningar, myndighetsåtgärder, lagbestämmelser och myndighetsföreskrifter, störningar i den allmänna datakommunikationen eller någon annan till sina verkningar lika betydande och ovanlig orsak som är oberoende av certifikatutfärdaren.

7 Krav på certifikatutfärdarens verksamhet

Utfärdaren ska utföra följande administrativa åtgärder som uppfyller kraven.

I dessa ingår att erbjuda registreringstjänster, skapa certifikat, distribuera certifikat, spärra certifikat och informera om spärrning (se punkt 4.2). Om kravet anknyter till ett visst serviceområde hos utfärdaren presenteras det under motsvarande underrubriker. Om inget serviceområde specificeras eller om man nämner "utfärdaren i allmänhet", gäller kravet utfärdarens allmänna verksamhet.

Syftet med dessa krav på förfaranden är inte att begränsa certifikatutfärdarens möjligheter att ta betalt för sina tjänster.

Kraven som presenteras gäller säkerhetsmål och administrativa åtgärder som vidtas för att uppnå dessa, för vars del specifika krav ställs, om det anses vara nödvändigt för att uppnå målen.

7.1 Certifieringspraxis

Utfärdaren utarbetar certifieringspraxis och övriga förfaringssätt som kompletterar certifikatpolicyn. Utfärdaren svarar för att certifieringspolicyn, certifieringspraxisen och certifieringsbeskrivningar är offentligt tillgängliga på adressen https://dvv.fi/sv/certifikatpolicydokument.

Rättigheterna och skyldigheterna för servercertifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

I ansökningsdokumentet och användarvillkoren nämns tydligt att certifikatsökanden intygar riktigheten hos uppgifterna med sin signatur då certifikatet skapas och att det publiceras i det offentliga registret. Samtidigt godkänner certifikatsökanden reglerna och villkoren för användning av servercertifikatet samt skyldigheten att anmäla eventuellt missbruk eller röjning av den privata nyckeln.

Utfärdaren fastställer och godkänner certifieringspraxisdokumenten.

Utfärdaren svarar för att dess certifieringsverksamhet och certifieringspraxis iakttar certifikatpolicyn.

Certifikatutfärdarens verksamhet granskas minst en gång om året. Vid granskningen jämförs certifikatpolicyn och certifieringspraxisen med utfärdarens verksamhet som helhet. Utfärdaren vidtar utan fördröjning korrigerande åtgärder vid upptäckta avvikelser.

Algoritmer och övriga tekniska detaljer som används i certifikatverksamheten och certifikaten finns beskrivna i kapitel 7.2.

7.2 Hantering av livscykeln för nycklarna inom ett öppet nyckelsystem

7.2.1 Skapande av certifikatutfärdarens nyckel

Utfärdaren skapar privata nycklar för signering och publika nycklar som motsvarar de privata nycklarna för signering. Certifikatutfärdarens privata nycklar förvaras i kryptografiska moduler som administreras av utfärdaren, som överensstämmer med nödvändiga säkerhetsstandarder

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.

Nycklarna förvaras i kryptografiska moduler som administreras av utfärdaren. De överensstämmer till sin säkerhetsnivå med nivå 3 i FIPS 140-2.

MDB förbereder och övervakar en serie kommandon för nyckelskapande. MDB:s nycklar skapas och lagras i hårdvarusäkerhetsmoduler (HSM) som är certifierade enligt minst FIPS 140-2 nivå 3.

MDB skapar och skyddar sina egna privata nycklar säkert med hjälp av en pålitlig HSM-modul certifierad för FIPS 140-2 nivå 3 och vidtar nödvändiga försiktighetsåtgärder för att förhindra deras kompromettering eller otillåten användning.

TSA säkerställer modulernas säkerhet under hela deras användningstid. TSA genomför särskilt de procedurer som krävs för lagning av privata nycklar.

Lagring av privata nycklar i krypteringsmodul: De privata nycklarna skapas och lagras i DVV:s hårdvarusäkerhetsmoduler (HSM), vilka är certifierade enligt minst FIPS 140-2 nivå 3.

Utfärdarens privata nyckel som använts för signering av servicecertifikatet och den motsvarande publika nyckeln är 4 096-bitars RSA-nycklar och 384-bitar ECC-nycklar.

Utfärdaren skapar ett nytt nyckelpar och utfärdarens certifikat senast fem år och tre månader innan det föregående certifikatets giltighetstid löper ut. Utfärdarens certifikat förs in i det offentliga registret enligt kapitel 7.3.5.

För att skapa en privat nyckel fordras att minst två personer samtidigt är närvarande eller aktiverar funktionen.

7.2.2 Lagring, säkerhetskopiering och returnering av utfärdarens privata nyckel

Utfärdarens privata nycklar är skyddade mot röjning och missbruk.

Nycklarna förvaras i kryptografiska moduler som administreras av utfärdaren. De överensstämmer till sin säkerhetsnivå med nivå 3 i FIPS 140-2 eller 140-3.

Det görs en säkerhetskopia på certifikatutfärdarens privata nyckel.

Säkerhetsegenskaperna och förvaringen av certifikatutfärdarens säkerhetskopierade privata nyckel motsvarar säkerhetskraven för utfärdarens privata originalnyckel i samtliga situationer.

Privata nycklar och deras säkerhetskopior förvaras med stark kryptering i utrustning som uppfyller kraven på kritisk datasäkerhet.

7.2.3 Distribution av utfärdarens publika nyckel

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren. Utfärdaren publicerar sin publika nyckel i ett offentligt register på adressen ldap://ldap.fineid.fi och på webbplatsen https://dvv.fi/sv.

7.2.4 System för reservnyckel

Signerarens privata signeringsnycklar förvaras inte på ett sätt som möjliggör dekryptering och säkerhetskopiering, varvid de befullmäktigade instanserna i vissa fall kan dekryptera nycklar genom att använda uppgifter lämnade av en eller flera parter.

7.2.5 Användning av certifikatutfärdarens nyckel

Fältet som fastställer användningssyftet i certifikatets datainnehåll anger användningssyftet för nyckeln kopplad till certifikaten.

Med utfärdarens certifikat signeras endast servercertifikat och relaterade spärrlistor. Den tekniska beskrivningen finns i FINEID S 2-bestämmelsen.

Då giltighetstiden för utfärdarens certifikat upphör förstörs certifikatutfärdarens privata nycklar i den kryptografiska modulen och används inte igen.

Utfärdarens privata nycklar förvaras i kryptografiska moduler.

Aktivering av utfärdarens privata nycklar utförs av för uppdraget befullmäktigade personer med kontrollkort i de kryptografiska modulerna. Användningen av certifikatutfärdarens privata nycklar kan förhindras av personer som är behöriga för uppgiften med hjälp av kontrollkort eller genom bortkoppling av strömmen till den kryptografiska modul som innehåller utfärdarens privata nycklar.

Utfärdaren har rätt att flytta utfärdarens privata nycklar till en annan kryptografisk modul vid service eller byte av originalutrustningen.

Utfärdarens privata nycklar förstörs efter att deras giltighetstid har upphört. Bara certifikatutfärdaren kan förstöra utfärdarens privata nycklar. När certifikatutfärdarens verksamhet upphör, ska utfärdarens privata nycklar och kopiorna av dem förstöras.

Utfärdaren skapar vid behov ett nyckelpar för certifikatinnehavaren. I detta fall levereras certifikatet och dess nyckelpar och lösenord till certifikatinnehavaren på så vis att det inte är möjligt för utomstående att komma åt dem.

Den trygga processen för att skapa och lagra nyckelpar förhindrar att nyckeln röjs utanför det system som används för att skapa nyckeln.

7.3 Hantering av livscykeln för certifikat inom ett öppet nyckelsystem

7.3.1 Registrering av signerare

Utfärdaren ska säkerställa att signerarna identifieras och autentiseras på ändamålsenligt sätt och att signerarens begäranden om certifikat är kompletta, riktiga och ändamålsenligt befullmäktigade.

Vid namngivningen av innehavaren av servercertifikatet används offentliga namnuppgifter och övriga uppgifter som uppgetts av certifikatsökanden och kontrollerats av registreraren.

Gruppen av attribut som bildar objektets namnpost i certifikatet är unik och individualiserar
innehavaren av certifikatet i fråga. Alla innehavarorganisationer av servercertifikat ska agera under eget namn.

Certifikatinnehavarens privata nycklar skapas i certifikatutfärdarens server eller dennes tekniska leverantörs server, då det gäller server-, stämpel- eller systemsigneringscertifikat. Då det gäller e-postservercertifikat skapar utfärdaren nyckelparet och certifikatet och levererar dem till certifikatinnehavaren.

Autentisering av organisation som företräder certifikatsökanden

Rättigheterna och skyldigheterna för servercertifikatsökanden ingår i ansökningsdokumentet och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

I ansökningsdokumentet och användarvillkoren nämns tydligt att certifikatsökanden intygar riktigheten hos uppgifter med sin signatur då certifikatet skapas och eventuellt publiceras i det offentliga registret. Samtidigt godkänner certifikatsökanden reglerna och villkoren för användning av servercertifikatet samt skyldigheten att anmäla eventuellt missbruk eller röjning av den privata nyckeln.

Utfärdaren och registreraren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheter för samtliga parter.

Sökanden av servercertifikat svarar för att samtliga uppgifter som är väsentliga för certifikatet och sökanden uppgett till utfärdaren eller registreraren är riktiga. Innehavaren ska använda servercertifikatet endast i enlighet med dess användningssyfte.

Då utfärdaren beviljar servercertifikatet godkänner utfärdaren samtidigt certifikatansökan.

Certifikatinnehavaren ska omedelbart anmäla servercertifikatet till spärrlistan om innehavaren misstänker att användning som strider mot avtalsvillkoren möjliggjorts.

Servicecertifikat ansöks genom Myndigheten för digitalisering och befolkningsdatas elektroniska tjänst, E-tjänster: asiointi.dvv.fi

När ett certifikat utfärdas kontrollerar MDB sökandens uppgifter. Det utfärdade certifikatet levereras till kunden i enlighet med avtalet.

Innan ett certifikat utfärdas ska organisationen ha ett registrerat konto i Myndigheten för digitalisering och befolkningsdatas webbtjänst, E-tjänster. Organisationsdata för kontot för E-tjänster hämtas från FODS-företags och organisationsdatasystemet. Användaren ska identifiera sig starkt för att kunna logga in på organisationskontot för E-tjänster. En ny användare behöver en inbjudan från en användare i organisationen för att få åtkomst till organisationens konto. Användaren ska identifiera sig varje gång hen loggar in på kontot. En servicecertifikatansökan kan enbart inlämnas när du är inloggad. I samband med ansökan lämnas in en fullmakt, ifall den som ansöker om certifikatet (ADB-kontaktperson o.d.) agerar på uppdrag av ett företag eller en organisation.

Ifall kundorganisationen inte kan använda E-tjänster (exempelvis utländska företag vilka saknar de behövda verktygen för stark elektronisk autentisering), kan ansökan påbörjas genom att skicka en förfrågan om ansökans anvisningar per e-post: kirjaamo@dvv.fi.

Om det servicecertifikat som beställs har ett domännamn eller en IP-adress, kontrollerar Myndigheten för digitalisering och befolkningsdata, i samband med behandlingen av ansökan, sökandens rätt att använda domännamnet antingen i ett tillgängligt internetbaserat offentligt register, genom kontroll av DNS/TXT, eller någon annan godtagbar metod. På samma sätt kontrolleras IP-adressens ägare i offentliga register. Myndigheten för digitalisering och befolkningsdata utfärdar endast servercertifikat för IP-adresser eller domäner som används för offentligrättsliga ändamål.

All organisationsdata som kommer på certifikatet, kontrolleras på FODS-företags och organisationsdatasystemet, eller på Patent- och registerstyrelsens Virre-register. OID:n som kommer på Social- och hälsovårdens servicecertifikat, kontrolleras på FPA:s nationella Kanta-kodtjänst, som upprätthålls av Institutet för hälsa och välfärd.

Servercertifikatet beviljas med olika giltighetstider beroende på certifikattyp. Aktuella giltighetstider framgår i samband med ansökan om certifikat.

Förnyelse av certifikat följer samma ansökningsförfarande som den ursprungliga ansökningen. Certifikatets pris utgår från en årlig avgift enligt Myndigheten för digitalisering och befolkningsdatas serviceprislista.

Utfärdaren beviljar servercertifikatet då utfärdaren godkänner certifikatansökan.

Utfärdaren ansvarar vid beviljandet av certifikatet för att datainnehållet i certifikatet är riktigt vid överlåtelsen av certifikatet.

När certifikatbegäran behandlas, testas den offentliga nyckeln gentemot kända svagheter med ett mjukvaruverktyg.

Det beviljade servercertifikatet levereras till kunden enligt avtalet.

Certifikatutfärdaren granskar CAA-poster vid registrering av certifikat, och erkänner utfärdardomännamnet ’dvv.fi’ och ’fineid.fi’.

7.3.2 Förnyande av certifikat, byte av nyckelpar och uppdatering av certifikat

Certifikat ska förnyas när uppgifter om certifikatinnehavaren som påverkar certifikatets datainnehåll ändras. I sådana fall ska certifikatinnehavaren kontakta utfärdaren och ansöka om ett nytt servercertifikat.

Om användningen av certifikatinnehavarens privata nyckel förhindras ska certifikatet anslutet till nyckeln i fråga alltid förnyas.

Endast den organisation som är innehavare för certifikatet eller en organisationen befullmäktigad instans kan ansöka om att förnya certifikatet.

Vid förnyelse av certifikat iakttas samma rutiner som vid första ansökan om certifikat.

Datainnehållet i ett certifikat kan inte ändras efter genereringen av certifikatet. När de uppgifter som påverkar datainnehållet i certifikatet ändras ska certifikatinnehavaren ansöka om ett nytt servercertifikat.

Vid förnyelse av servercertifikatet iakttas samma rutiner som vid första ansökan om certifikat. Då certifikatinnehavaren förnyar sin privata nyckel fordrar detta alltid ny registrering, ny certifikatansökan och nytt servercertifikat.

7.3.3 Skapande av certifikat

Certifikatets datainnehåll är beskrivet i FINEID S2-bestämmelsen, som finns på adressen https://dvv.fi/sv.

Utfärdarens privata nycklar förvaras krypterade i kryptografiska moduler som förvaltas av utfärdaren och som uppfyller kraven enligt nivå 3 i FIPS 140-1 eller 140-2. Utfärdarens privata nycklar är skyddade mot röjning och missbruk.

Utfärdaren av rotcertifikatet signerar utfärdarens certifikat och det förs in i det offentliga registret.

Namngivningspraxis:

CN (Common name) = DVV Gov. Root CA – G3 RSA

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

och

CN (Common name) = DVV Gov. Root CA – G3 ECC

OU (Organizational unit) = Varmennepalvelut

OU (Organizational unit) = Certification Authority Services

O (Organization) = Digi- ja vaestotietovirasto CA

C (Country) = FI

Utfärdare för Myndigheten för digitalisering och befolkningsdatas servercertifikat är:

CN (Common name) = DVV Service Certificates - G5R

OU (Organizational unit) = Palveluvarmenteet

O (Organization) = digi- ja vaestotietovirasto CA

C (Country) = FI

och

CN (Common name) = DVV Service Certificates - G5E

OU (Organizational unit) = Palveluvarmenteet

O (Organization) = digi- ja vaestotietovirasto CA

C (Country) = FI

och

CN = DVV Time Stamp Certificates - G2R

OU = Aikaleimavarmenteet

O = Digi- ja vaestotietovirasto CA

C = FI

och

CN = DVV Time Stamp Certificates - G2E

OU = Aikaleimavarmenteet

O = Digi- ja vaestotietovirasto CA

C = FI

7.3.3.1 Servercertifikat

Servercertifikat kan användas för identifiering av både den offentliga och den privata sektorns tjänster. Med hjälp av servercertifikat, kan tjänstens användare försäkra sig om att tjänstegivaren är korrekt.

De servercertifikat som utfärdas av Myndigheten för digitalisering och befolkningsdata, följer ETSI QCP-w (0.4.0.194112.1.4) certifikatpolicy för EU-giltiga certifikat som används för autentisering av webbplatser.

Registreraren kontrollerar i samband med behandlingen av ansökan, sökandens rätt att använda domännamnet antingen i ett tillgängligt internetbaserat offentligt register, genom kontroll av DNS/TXT, eller någon annan godtagbar metod. På samma sätt kontrolleras IP-adressens ägare i offentliga register. Myndigheten för digitalisering och befolkningsdata utfärdar endast servercertifikat för IP-adresser eller domäner som används för offentligrättsliga ändamål.

När certifikatet registreras, kontrollerar certifikatutfärdaren CAA-posten och säkerställer sin rätt att utfärda ett certifikat till sökanden (dvv.fi eller fineid.fi).

All organisationsdata som kommer på certifikatet, kontrolleras på FODS-företags och organisationsdatasystemet, eller på Patent- och registerstyrelsens Virre-register.

Namngivningspolicy för certifikatinnehavare i servicecertifikat (obligatoriska fält):

CN (Common Name) = domännamn eller IP-adress

O (Organization) = organisationens namn (t.ex. företag Abp)
C (Country) = statens namn (t.ex. FI eller Finland)
L (Locality name) = stad eller kommun (t.ex. Helsingfors)
S (State or Province name) = land eller landskap (t.ex. Finland eller Nyland)
extra DNS (DNS Name) = domän krävs om fältet CN innehåller en IP-adress
SERIALNUMBER (Serial Number) = obligatoriskt fält i social - och hälsovårdscertifikaten: OID enligt Kanta-kodtjänsten

Valfria fält:

SERIALNUMBER (Serial Number) = företags-ID eller organisationsnamn
extra DNS (DNS Name) = domän - eller IP-adress (max 4 st.)

7.3.3.2 Systemsignaturscertifikat

Namngivningspolicy för certifikatinnehavare i systemsignaturcertifikat (obligatoriska fält):
CN (Common Name) = systemnamn (t.ex. patientdatasystem) eller organisationsnamn (får också innehålla en domän eller IP-adress, men det skall då vara möjligt att kontrollera att den hör till organisationen)
O (Organization) = organisationens namn (t.ex. företag Abp)
C (Country) = staten (t.ex. FI eller Finland)
SERIALNUMBER (Serial Number) = företags-ID (I social och hälsovårds certifikat OID enligt Kanta-kodtjänsten)
L (Locality name) = stad eller kommun (t.ex. Helsingfors)
S (State or Province name) = land eller landskap (t.ex. Finland eller Nyland)

7.3.3.3 Stämpelcertifikat

Stämpelcertifikat är en juridisk persons personcertifikat som används för att stämpla handlingar i elektroniskt format. Med hjälp av stämpelcertifikatet kan man garantera den stämplade informationens ursprung, oföränderlighet och obestridlighet.

Certifikatinnehavarens namngivningspraxis för stämpelcertifikat (obligatoriska fält):

CN (Common Name) = Allmänt namn (t.ex. dokumenthanteringssystem)

O (Organization) = Organisationens namn (t.ex. Företaget Abp)

SERIALNUMBER eller OrganizationIdentifier = företagskod

C (Country) = stat (t.ex. FI eller Finland)

Följande fält i stämpelcertifikatet är valfri och innehåller icke-verifierad information som kunden specificerar:

OU (Organization unit) = organisationsenhet

DVV förbehåller sig rätten att ändra eller ta bort information i OU-fältet.

7.3.3.4 Stämpeltjänstens gränssnittscertifikat

Stämpeltjänstens gränssnittscertifikat är client-certifikat som behövs för autentisering mellan kundens system och MDB:s stämpeltjänst.

Certifikatinnehavarens namngivningspraxis för stämpeltjänstens gränssnittscertifikat (obligatoriska fält):

CN (Common Name) = Allmänt namn (t.ex. dokumenthanteringssystem)

OU = Stämpeltjänst (obs. OU-fältet i stämpeltjänstens gränssnittscertifikat måste finnas i denna form)

O (Organization) = Organisationens namn (t.ex. Företaget Abp)

C (Country) = stat (t.ex. FI eller Finland)

7.3.3.5 Social och hälsovårdens servercertifikat

Servicecertifikaten för social - och hälsovården är i övrigt vanliga servicecertifikat, men de har tagits fram endast för FPA: s Kanta-tjänst. Servicecertifikatet för social - och hälsovården kan endast produceras för en organisation som finns aktiv i Institutet för hälsa och välfärds Kanta-kodtjänst.

SERIALNUMBER (Serial Number) = obligatoriskt fält i social - och hälsovårdscertifikaten: OID enligt Kanta-koden

7.3.3.6 Servicecertifikat for hälsoapplikationer

Certifikatinnehavarens namngivningspolicy för välbefinnandeprogramcertifikat (obligatoriska fält):
CN (common name) = domain eller IP-adress
SERIALNUMBER (Serial number) = OID enligt kanta-tjänsten
O (Organization) = organisationens namn (t.ex. företag Abp)
C (Country) = staten (t.ex. FI eller Finland)
L (Locality name) = stad eller kommun (t.ex. Helsingfors)
S (State or Province name) = land eller landskap (t.ex. Finland eller Nyland)

7.3.3.7 BDS-kundcertifikat

Namngivningspolicy för certifikatinnehavare gällande VTJ-klientcertifikat (obligatoriska fält):
CN (Common Name) = systemnamn (t.ex. patientdatasystem) eller organisationsnamn (får också innehålla en domän eller IP-adress, men det skall då vara möjligt att kontrollera att den hör till organisationen)
O (Organization) = organisationens namn (t.ex. företag Abp)
SERIALNUMBER (Serial Number) = företags-ID
C (Country) = staten (t.ex. FI eller Finland)
L (Locality name) = stad eller kommun (t.ex. Helsingfors)
S (State or Province name) = land eller landskap (t.ex. Finland eller Nyland)

Uppgifterna om innehavaren av utfärdarens certifikat anger entydigt certifikatets innehavarorganisation.

Aktivering av utfärdarens privata nycklar utförs av för uppdraget befullmäktigade personer med kontrollkort i de kryptografiska modulerna.

Certifikatinnehavarens privata nycklar är skyddade mot exponering och obehörig användning i certifikatinnehavarens datasystem. Bara interna kommandon i datasystemet ger tillgång till de privata nycklarna.

För att kommandot som gäller de privata nycklarna ska kunna utföras, måste nyckeln i fråga ha aktiverats med rätt lösenord.

Materialet som arkiveras förvaras i lokaler med hög skyddsnivå och passagekontroll.

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren.

7.3.3.8 Tidsstämpelcertifikat

Namngivningsprincip för certifikatinnehavare för tidsstämpelcertifikat (obligatoriska fält):

CN = DVV TSA2

SERIALNUMBER = 0245437-2

OU = Varmennepalvelut

O = Digi- ja vaestotietovirasto

C = FI

7.3.4 Distribution av användarvillkor

Utfärdaren ska se till att användarvillkoren tillhandahålls beställarna och de förlitande parterna.

Utfärdarens certifikat som innehåller certifikatutfärdarens publika nyckel kan sökas i det offentliga registret eller i tjänsten som upprätthålls av utfärdaren.

Certifikatutfärdaren informerar om andra ändringar i certifikatpolicyn än de som anges i kapitel 8 på sin webbplats (https://dvv.fi/sv/certifikatpolicydokument) minst 30 dagar innan ändringen börjar gälla.

Utfärdaren publicerar samtliga servercertifikat och spärrlistor i ett offentligt register som kan användas utan avgift. Utfärdaren publicerar certifikatpolicy, certifieringspraxis, certifikatbeskrivning samt övriga offentliga handlingar med anknytning till produktionen av certifikattjänster på sin webbplats https://dvv.fi/sv/certifikatpolicydokument.

Uppgifternas tillgänglighet

Uppgifterna i registret och spärrlistan är offentligt tillgängliga. Offentliga FINEID-bestämmelser som publicerats av utfärdaren finns på utfärdarens webbplats https://dvv.fi/sv. Certifikatpolicyn och certifieringspraxisen finns även tillgängliga på certifikatutfärdarens webbplats https://dvv.fi/sv/certifikatpolicydokument.

Dataförvaring

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats https://dvv.fi/sv. De konfidentiella uppgifterna i certifikatsystemet är sparade i utfärdarens egna, konfidentiella dataförråd. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Man fäster särskild uppmärksamhet vid hanteringen av personuppgifter och Myndigheten för digitalisering och befolkningsdata har publicerat särskilda regler för produktionen av certifikattjänster i enlighet med personuppgiftslagen. Utfärdaren har även berett en registerbeskrivning för hanteringen av personuppgifter inom varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen, som publicerats på utfärdarens webbplats https://dvv.fi/sv.

7.3.5 Distribution av certifikat

Ett certifikat levereras enligt överenskommelse och publiceras i det offentliga registret genast då det skapats och det finns i registret under hela dess giltighetstid. Utfärdaren publicerar en spärrlista som är giltig två dygn efter publikationen. Denna spärrlista uppdateras varje timme

Uppgifter om register och spärrlista är offentligt tillgängliga ldap://ldap.fineid.fi.

7.3.6 Spärrning och tillfällig spärrning av certifikat

Spärrning och tillfällig spärrning av certifikat

Certifikatutfärdaren administrerar spärrtjänsten för certifikat. Uppgifterna om spärrade certifikat upptas på en spärrlista som utfärdaren
signerar och som publiceras i ett offentligt register. Certifikatet kan inte spärras tillfälligt.

Certifikatutfärdaren informerar inte certifikatinnehavare om spärrade certifikat.

Förutsättningar för spärrning av ett certifikat

Ett certifikat spärras om:

- innehavaren av certifikatet begär att certifikatet spärras
- certifikatinnehavarens uppgifter som påverkar datainnehållet i certifikatet har förändrats
- den privata nyckeln för certifikatet har kommit bort eller röjts
- organisationen som innehar certifikatet har upphört med sin verksamhet.

Det är inte tillåtet att använda eller försöka använda ett certifikat efter att begäran om spärrning har gjorts.

Behörig att begära spärrning

Behörig att begära spärrning av certifikat är:

- representant för organisationen som innehar servercertifikatet;
- innehavaren av servercertifikatet
- utfärdaren av certifikatet om förutsättningarna i punkt 6.2 uppfylls.

Process för spärrning av ett certifikat

Innehavaren av certifikatet begär utfärdaren av certifikatet spärra certifikatet. Begäran görs:

1. E-tjänster genom elektronisk anmälan från kundens eget konto.

2. Om kunden inte har tillgång till organisationens konto för E-tjänster, ska kunden meddela kirjaamo@dvv.fi.

Utfärdaren av certifikat spärrar certifikaten om:

- organisationen som innehar certifikatet upphör med sin verksamhet.

Information som lagras till E-tjänster i samband med en spärrningsförfrågan:

- individuella uppgifter för servercertifikatet
- personuppgifter för personen bakom spärrningsbegäran
- organisationen för personen bakom spärrningsbegäran
- autentiseringssätt för personen bakom spärrningsbegäran
- tidpunkt för spärrningsbegäran
- orsak till spärrningsbegäran
- personuppgifter för mottagaren av spärrningsbegäran
- eventuella övriga uppgifter som certifikatinnehavaren uppgett
- tidpunkten för röjning av nyckelparet, tidpunkten då organisationen som innehar certifikatet har upphört med sin verksamhet etc.
- personuppgifter för den som spärrat certifikatet
- tidpunkten för spärrning av certifikatet.

Certifikatutfärdaren informerar inte separat certifikatinnehavare om spärrade certifikat. Uppgifterna om spärrningen ska förvaras i 5 år från tidpunkten för spärrningen.

Certifikatinnehavarens skyldighet att begära spärrning

Certifikatinnehavaren ska utan dröjsmål lämna en begäran om spärrning till utfärdaren, om de förutsättningar för spärrning som beskrivs i kapitel 6.2 uppfylls.

Hanteringstid för begäran om spärrning av ett certifikat

Utfärdaren behandlar utan dröjsmål begäranden om spärrning av certifikat.

Förlitande parters skyldighet att kontrollera giltigheten för certifikat

Innan ett certifikat godkänns ska den förlitande parten kontrollera att certifikatet gäller och inte är spärrat.

Förlitande part ska kontrollera gällande spärrlista. Ett certifikat är inte tillförlitligt, om inte den förlitande parten har kontrollerat certifikatets status.

Publiceringsfrekvens för spärrlista

En uppdaterad spärrlista publiceras varje timme.

Av spärrlistan ska framgå den planerade publiceringstidpunkten för nästa spärrlista. En ny spärrlista kan också publiceras tidigare än planerat.

Maximal giltighetstid för spärrlista

En uppdaterad spärrlista gäller i högst 48 timmar. I varje spärrlista anges när giltighetstiden går ut.

Certifikatinnehavaren kan begära att certifikatet spärras innan dess giltighetstid löpt ut.

Förfarande vid begäran om spärrning

Innehavaren av ett servicecertifikat eller den behöriga representanten för certifikatinnehavarorganisationen ska meddela Myndigheten för digitalisering och befolkningsdatas certifikattjänsters verksamhet, om det är känt eller misstänkt att certifikatinnehavarens privata nyckel har avslöjats. Anmälan görs i första hand vid E-tjänster på organisationens konto från vilket servicecertifikatet har beställts eller, om detta inte är möjligt, per e-post med ett kvalificerat certifikat som Myndigheten för digitalisering och befolkningsdata har utfärdat, undertecknat på adressen kirjaamo@dvv.fi. Anmälan ska innehålla följande uppgifter: anmälarens namn och organisation, serienumret på det certifikat som ska spärras. Efter att ha fått meddelandet stänger certifikatutfärdaren certifikatet i fråga. När certifikatinnehavaren har begärt att certifikatutfärdaren ska spärra certifikatet, upphör certifikatinnehavarens ansvar för användningen av certifikatet.

7.3.7 Spärrning av certifikat av Myndigheten för digitalisering och befolkningsdata

Certifikatutfärdaren kan spärra ett certifikat om det har använts i strid med certifikatpolicyn, certifieringspraxisen eller de krav och anvisningar som utfärdats med stöd av dem.

Det är inte tillåtet att använda eller försöka använda ett certifikat efter att begäran om spärrning har gjorts.

Myndigheten för digitalisering och befolkningsdata spärrar också certifikat ifall fel upptäcks i datainnehållet.

Myndigheten för digitalisering och befolkningsdata kan spärra certifikat som signerats med myndighetens hemliga nyckel om det finns anledning att misstänka att myndighetens hemliga nycklar har röjts eller råkat i fel händer.

Samtliga giltiga certifikat som utfärdats med den röjda nyckeln ska spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade certifikatets giltighetstid har löpt ut.

Om en privat nyckel eller annan teknisk metod som Myndigheten för digitalisering och befolkningsdata använder vid skapandet av certifikat har röjts eller annars blivit oanvändbar, ska Myndigheten för digitalisering och befolkningsdata underrätta alla kortinnehavare och Transport- och kommunikationsverket (Traficom) som fungerar som tillsynsmyndighet om händelsen på behörigt sätt.

Myndigheten för digitalisering och befolkningsdata kan spärra ett certifikat av särskild anledning.

7.4 Utfärdarens lednings- och verksamhetspraxis

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

7.4.1 Hantering av säkerhet

Myndigheten för digitalisering och befolkningsdatas datasäkerhet administreras i enlighet med Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och standarden ISO 27001.

7.4.2 Klassificering och hantering av reserver

Myndigheten för digitalisering och befolkningsdata är ett ämbetsverk underställt finansministeriet, vars certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Myndigheten för digitalisering och befolkningsdata ekonomiska förvaltning utgår från lagar och förordningar om statens ekonomi samt finansministeriets och Statskontorets bestämmelser. Statens revisionsverk sköter granskningen av ekonomin. Utöver detta beskrivs verksamhetens resultat med fokus på effekter, ekonomi och lönsamhet.

Myndigheten för digitalisering och befolkningsdata svarar i enlighet med de allmänna avtalsvillkoren för IT-anskaffningar inom den offentliga förvaltningen för att man har tillräckliga ekonomiska resurser för att arrangera certifikatverksamheten på ett ändamålsenligt sätt samt hantera eventuella krav på skadeersättning (JIT 2007).

7.4.3 Personal och dataskydd

Myndigheten för digitalisering och befolkningsdata fungerar som certifikatutfärdare och svarar för certifikatverksamheten. De tekniska underleverantörerna har anlitats genom upphandling och agerar för Myndigheten för digitalisering och befolkningsdatas räkning och på Myndigheten för digitalisering och befolkningsdatas ansvar.

Myndigheten för digitalisering och befolkningsdata fäster särskild uppmärksamhet vid såväl den egna personalens som leverantörernas och registrerarnas pålitlighet och kompetens för att utföra uppgifterna.

Utförande av bakgrundskontroll

Myndigheten för digitalisering och befolkningsdata utför en mindre säkerhetskontroll av den egna personalen samt personer som arbetar i de tekniska leverantörernas certifikatmiljö.

Förfarande vid utförande av bakgrundskontroll

Personalens arbetserfarenhet kartläggs vid rekryteringen. En mindre säkerhetsutredning utförs för personen utgående från de uppgifter han eller hon uppger på ett standardiserat formulär.

Samtliga personer som arbetar med centrala uppgifter hos utfärdaren, certifikattjänsterna, producenterna av registertjänster och spärrtjänsten ska:

- fylla i en blankett som lämnas in till skyddspolisen, som används för att utföra en mindre säkerhetsutredning för personen
- avstå från uppgifter som strider mot deras skyldigheter och ansvarsområden
- vara personer som inte tidigare har avfärdats på grund av att de försummat eller misskött sina uppgifter
- ha lämplig utbildning för att utföra sina uppgifter.

Krav på utbildning

Personalen på Myndigheten för digitalisering och befolkningsdata ska ha sådan utbildning att de kan utföra sina uppgifter på bästa möjliga sätt. Vid Myndigheten för digitalisering och befolkningsdata finns en utbildningsplan. För förverkligandet av planen svarar Myndigheten för digitalisering och befolkningsdatas administrativa enhet.

Underhåll av expertis och kompetens

Utbildningen för personalen planeras och underhålls på så vis att de anställda alltid besitter den kompetens som fordras för att utföra uppgifterna på bästa möjliga sätt.

Krav på uppgiftsrotation

Då utfärdaren planerar arbetsrotation inom sin verksamhet ska uppgifterna organiseras på så vis att den anställda kan utföra sina nya uppgifter på bästa möjliga sätt. I planeringen av arbetsrotationen beaktas iakttagande av god dataadministration och bevarande av tillräcklig kompetensnivå för de olika uppgifterna.

Även inom arbetsrotationen efterlevs Myndigheten för digitalisering och befolkningsdatas dataskyddspolicy och dataskyddsplan samt Myndigheten för digitalisering och befolkningsdatas övriga allmänna anvisningar.

Åtgärder vid avvikelser

Myndigheten för digitalisering och befolkningsdatas personal agerar i sitt uppdrag med ämbetsmannaansvar och i enlighet med Myndigheten för digitalisering och befolkningsdatas interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

Personal som representerar organisationen

Vid rekryteringen av personal ska man se till att personalen innehar den kompetens som fordras för uppgifterna och att inget sådant framgår vid utredningen av personens bakgrund som står i konflikt med produktionen av certifikattjänster.

Handlingar som tillhandahålls personalen

Personalen har alltid tillgång till Myndigheten för digitalisering och befolkningsdatas kvalitets- och säkerhetsdokument.

7.4.4 Fysisk säkerhet och omgivningens säkerhet

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för att utföra datatekniska uppdrag inom certifikatverksamheten. MDB svarar i egenskap av certifikatutfärdare för säkerheten inom certifikatproduktionen och själva produktionen på ett ändamålsenligt sätt inom samtliga delområden.

Läge och lokalernas egenskaper

Utfärdarens system finns i maskinsalar med hög säkerhetsnivå och uppfyller anvisningarna och bestämmelserna för säkerheten i maskinsalar.

Säkerheten i verksamhetslokalerna är förverkligad på så vis att obehöriga inte har tillträde till lokalerna.

Fysisk tillgång till verksamhetslokalen

Lokaler där produktionsmässiga uppgifter inom certifikatsystemet utförs är försedda med passagekontroll. Passerkontrollsystemet upptäcker både tillåtet och otillåtet tillträde. Tillträde till maskinsal fordrar autentisering av personen, varvid personen identifieras och hans eller hennes passagerättigheter kontrolleras och händelsen registreras. Maskinsalarna övervakas dygnet runt.

Reservarrangemang

Utrustningslösningarna är förverkligade i enlighet med god dataadministrationssed på så vis att man vid problem med systemet kan övergå till att använda reservsystemet utan att riskera konfidentialiteten, integriteten och användbarheten hos uppgifterna i systemet.

Tillgången till reservdelar och service för viktig utrustning är säkrad.

7.4.5 Hantering av verksamheten

Myndigheten för digitalisering och befolkningsdata anlitar tekniska leverantörer för registrering och datatekniska uppdrag inom produktionen av certifikat. Myndigheten för digitalisering och befolkningsdata fungerar som certifikatutfärdare och svarar för certifikatverksamheten.

Utfärdarens uppgifter delas in i följande ansvarsområden:

- Datasäkerhetsansvarig
- Registreringsansvarig
- Administratör för systemet
- Användare av systemet
- Övervakare av systemet

Certifikatutfärdaren och den tekniska leverantören har ingått ett leveransavtal, där leverantörens uppgifter, metoder och ansvarsområden samt anordnandet av datasäkerheten beskrivs detaljerat.

7.4.6 Hantering av tillgång till systemet

Skapande, aktivering, säkerhetskopiering och returnering av utfärdarens privata nyckel är åtgärder som utförs med två personer som fungerar som administratörer för systemet närvarande.

Vid formateringen av den kryptografiska modulen för utfärdarens privata nyckel närvarar minst två personer som fungerar som administratörer för systemet.

Användning av systemet fordrar närvaron av en person som innehar rättigheterna för uppgiften.

Registrering och autentisering av servercertifikat fordrar närvaron av en person.

7.4.7 Ibruktagning och underhåll av pålitliga system

Registreraren av servicecertifikatet: Registrerare är funktionen Certifikattjänster vid Myndigheten för digitalisering och befolkningsdata.

Administratör av certifikatsystemet: Autentiseras med ett personligt kontrollkort för administration av systemet. Administratörer för systemet är certifikatsystemleverantörens systemexperter samt personer som befullmäktigats för uppdraget av Myndigheten för digitalisering och befolkningsdata.

Användare av certifikatsystemet: Autentiseras med ett personligt personkort för användning av systemet. Användare av certifikatsystemet är maskinsalsverksamheten, initiativtagare till tekniska certifikatbegäranden och spärrtjänsten.

7.4.8 Hantering av kontinuerlig affärsverksamhet och störningar

Myndigheten för digitalisering och befolkningsdata har en kontinuitets- och beredskapsplan för att verksamheten ska kunna bedrivas ostört utan avbrott.

Utfärdarens privata nyckel har röjts eller certifikatet har spärrats

Utfärdaren av rotcertifikatet uppger i varje certifieringspraxis de åtgärder som utfärdaren, innehavarna av utfärdarens certifikat, parterna som litar på utfärdarens certifikat, registrerarna och utfärdarens personer ska vidta om utfärdarens privata nyckel har röjts eller blivit oanvändbar på annat vis.

I detta fall ska utfärdaren av rotcertifikatet antingen upphöra med sin verksamhet på det sätt som beskrivs i kapitel 7.4.9 eller utföra följande åtgärder:

a) Utfärdaren av rotcertifikatet meddelar det inträffade till samtliga innehavare, förlitade parter och avtalskunder eller i övrigt har ett sådant förhållande till utfärdaren på grund av avtalsförhållande eller myndighetsverksamhet att utfärdaren måste informera om det inträffade.

b) Utfärdaren av rotcertifikatet skapar en ny nyckel i enlighet med kapitel 7.3.3

c) Utfärdarens samtliga gällande certifikat och certifikat för slutanvändare om beviljats med den röjda nyckeln spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan giltighetstiden har löpt ut för det av utfärdarens certifikat som spärrats senast.

Säkerhetsproblem förorsakade av naturkatastrof eller annan katastrof

I Myndigheten för digitalisering och befolkningsdatas säkerhetspolicy 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.

7.4.9 Då utfärdarens verksamhet upphör

Utfärdarens verksamhet anses upphöra då samtliga tjänster med anknytning till utfärdarens beviljande av certifikat upphör permanent. Utfärdarens verksamhet anses inte upphöra om certifieringstjänsten överförs från en organisation till en annan.

Utfärdaren meddelar om att certifikattjänsterna upphör så snart som möjligt, dock minst en månad innan tidpunkten för detta.

Innan utfärdarens verksamhet upphör utförs minst följande åtgärder:

a) Samtliga gällande servercertifikat spärras på en eller flera spärrlistor, vars giltighetstid inte upphör innan det senast spärrade servercertifikatets giltighetstid har löpt ut.

b) Utfärdaren upphäver samtliga avtalspartners befogenheter för att utföra åtgärder med anknytning till processen för beviljande av certifikat för utfärdarens del.

c) Utfärdaren ser till att tillgången till utfärdarens arkiv bevaras även efter att utfärdarens verksamhet har upphört.

7.4.10 Tillämplig lagstiftning

Myndigheten för digitalisering och befolkningsdata efterlever i sin servercertifikatverksamhet den gällande lagstiftningen i Finland.

Bestämmelser om av Myndigheten för digitalisering och befolkningsdata beviljade certifikat fastställs i lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009).

Myndigheten för digitalisering och befolkningsdatas skadeståndsansvar för produktionen av certifikattjänster bestäms enligt gällande samarbetsavtal och skadeståndslagen (412/1974) . Myndigheten för digitalisering och befolkningsdata omfattas också av kraven i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

7.4.11 Förvaring av information om certifikat

Offentliga uppgifter som publicerats av utfärdaren finns på utfärdarens webbplats. De konfidentiella uppgifterna i certifikatsystemet är sparade i utfärdarens egna, konfidentiella dataförråd. Utfärdarens data arkiveras i enlighet med gällande arkivbestämmelser. Man fäster särskild uppmärksamhet vid hanteringen av personuppgifter och Myndigheten för digitalisering och befolkningsdata har publicerat särskilda regler för produktionen av certifikattjänster i enlighet med personuppgiftslagen. Utfärdaren har även berett en registerbeskrivning för hanteringen av personuppgifter inom varje delområde inom certifikatsystemet i enlighet med personuppgiftslagen.

Vid arkivering tillämpas som allmän lag bestämmelserna i arkivlagen (831/1994). Rätten till inhämtande av information fastställs i lagen om offentlighet i myndigheternas

verksamhet (621/1999). Vid arkiveringen av certifikat tillämpas för en del dessutom bestämmelserna om arkivering i lagstiftningen om elektronisk kommunikation. Uppgifterna i certifikatregistret ska förvaras i 5 år från tidpunkten då certifikaten upphört att gälla. Utfärdaren arkiverar följande uppgifter:

a) Certifikatsökandens undertecknade ansökningsblankett, verifikat för mottagande av servercertifikatet och de allmänna användarvillkoren för certifikatet

b) Beviljade servicecertifikat, deras datainnehåll och extra uppgifter med anknytning till hanteringen av deras livscykel från att servicecertifikatets giltighetstid har löpt ut eller certifikatet har spärrats

c) Åtgärder med anknytning till skapande och förnyande av utfärdarens privata nyckel

d) Begäranden om spärrning av servicecertifikat

e) Spärrlistor sparade i det offentliga registret och övrig information om spärrningen av servicecertifikat

f) Gällande certifikatpolicy och tidigare certifikatpolicyn och motsvarande certifieringspraxis

g) Åtgärder utförda av användare som registrerats som administratörer för certifikatsystemet och användare av certifikatsystemet sparas loggfiler

h) Granskningsrapporterna och protokollen, inklusive dataskyddsgranskningar och auditering av systemet.

Det arkiverade materialet förvaras enligt bestämmelserna för myndighet som fungerar som utfärdare av kvalificerade certifikat.

Skydd av arkiv

Utfärdaren förvarar handlingar med anknytning till ansökning om servicecertifikat, autentisering av personer och överlåtelse av servicecertifikat som arkiveras i ändamålsenliga lokaler.

Materialet som arkiveras förvaras i lokaler med hög skyddsnivå och passagekontroll.

Säkerhetsförfaranden för arkiverat material

Säkerhetskopiorna förvaras i ett annat fysiskt utrymme än originalmaterialet.

Metoder för införskaffning och tryggande av arkiverat material

Om utfärdarens verksamhet avbryts eller upphör ska utfärdaren meddela samtliga kunder att arkivet fortfarande är tillgängligt. Samtliga förfrågningar om arkiverade uppgifter skickas till utfärdaren eller den instans som utfärdaren uppgett innan utfärdarens verksamhet har upphört.

Utfärdaren ser till att arkiven är tillgängliga och läsbara även utifall att utfärdarens verksamhet avbryts eller upphör.

Uppgifter kan överlåtas ur arkivet i den mån detta är motiverat med tanke på certifikatinnehavaren eller den förlitande parten.

Sökanden kan se sina egna elektroniskt gjorda ansökningar och beslut i Myndigheten för digitalisering och befolkningsdatas E-tjänster.

7.5 Krav på organisationen

Myndigheten för digitalisering och befolkningsdata är en myndighet som upprätthåller ett personregister, vars uppdrag enligt lagen om Myndigheten för digitalisering och befolkningsdata certifikattjänster (661/2009) är att utöver övriga tjänster producera tjänster inom certifierad elektronisk kommunikation.

Myndigheten för digitalisering och befolkningsdata beviljar certifikat utgående från ansökan. Rättigheterna och skyldigheterna för certifikatsökanden ingår i Myndigheten för digitalisering och befolkningsdatas ansökningsdokument för servercertifikat och i de allmänna användarvillkoren, som utgör avtalet som ingås med certifikatsökanden.

Myndigheten för digitalisering och befolkningsdata och registreraren samt leverantörer av övriga delområden av certifikattjänsterna har ingått ett avtal som obestridligen fastställer rättigheterna, ansvarsområdena och skyldigheterna för samtliga parter.

Myndigheten för digitalisering och befolkningsdatas certifikattjänster omfattas av ett separat lagstadgat system för ekonomisk förvaltning och tillsyn. Myndigheten för digitalisering och befolkningsdata är ett ämbetsverk underställt finansministeriet. Myndigheten för digitalisering och befolkningsdata ekonomiska förvaltning utgår från lagar och förordningar om statens ekonomi samt finansministeriets och Statskontorets bestämmelser. Statens revisionsverk sköter granskningen av ekonomin. Utöver detta beskrivs verksamhetens resultat med fokus på effekter, ekonomi och lönsamhet.

Myndigheten för digitalisering och befolkningsdata efterlever i sin servercertifikatverksamhet den gällande lagstiftningen i Finland. Myndigheten för digitalisering och befolkningsdata agerar omsorgsfullt, pålitligt och ändamålsenligt. Utfärdaren ser till att uppgifter om certifikat och certifikatverksamhet utgående från vilka utfärdarens verksamhet och pålitlighet kan bedömas är offentligt tillgängliga.

Myndigheten för digitalisering och befolkningsdata fäster särskild uppmärksamhet vid såväl den egna personalens som leverantörernas och registrerarnas pålitlighet och kompetens för att utföra uppgifterna. Myndigheten för digitalisering och befolkningsdata har tillräckliga tekniska färdigheter och ekonomiska resurser för att på ett ändamålsenligt sätt driva certifikatverksamheten samt täcka eventuellt skadeersättningsansvar. Myndigheten för digitalisering och befolkningsdatas personal agerar i sitt uppdrag med ämbetsmannaansvar och i enlighet med Myndigheten för digitalisering och befolkningsdatas interna anvisningar. Bestämmelser om tjänstemannens ställning finns i statstjänstemannalagen (750/1994).

Eventuella tvister löses enligt rättssystemet i Finland. Vid lösningen av klagomål och tvister samt i den administrativa tillsynen och rättstillämpningen tillämpas gällande lagstiftning.

Denna certifieringspraxis har registrerats av Befolkningscentralen och upphovsrätten tillfaller Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata äger samtliga uppgifter som anknyter till certifikaten och dokumentationen i enlighet med de tekniska leveransavtalen. Myndigheten för digitalisering och befolkningsdata äger samtliga ägande- och användarrättigheter för denna certifieringspraxis. Myndigheten för digitalisering och befolkningsdata svarar för administrationen och uppdateringen av denna certifieringspraxis.

8 Definitionsramar för övriga certifikatpolicydokument

I denna punkt fastställs de övriga allmänna ramarna för certifikatpolicyn för certifikatutfärdare. Utfärdaren kan uppge att man iakttar dessa allmänna definitionsramar enligt kraven i punkt 8.3. Allmänt taget förutsätter överensstämmelse med kraven att man iakttar kraven i punkt 6 och 7 med undantag för de krav som endast tillämpas för utfärdare som beviljar certifikat till allmänheten.

8.1 Hantering av dokument innehållande bestämmelser

Ändring av bestämmelser

Utfärdaren kan ändra bestämmelserna utgående från juridiska, verksamhetsmässiga eller tekniska krav. Ändringar i bestämmelserna ska föras in i certifikatpolicy- och certifieringspraxishandlingarna på det sätt som beskrivs här näst.

Publicering och information

Utfärdaren publicerar certifikatpolicyn och certifieringspraxisen, som är tillgängliga på adressen https://dvv.fi/sv/certifikatpolicydokument.

Offentliga bestämmelser relaterade till utfärdarens produktion av certifikat är tillgängliga på samma webbplats.

Avtal som ingåtts med datatekniska leverantörer om leverans av certifikat samt beskrivningar av produktionssystem och bestämmelser om produkter är konfidentiella.

Förfarande för ändring och godkännande av certifieringspraxis

Myndigheten för digitalisering och befolkningsdata godkänner såväl certifikatpolicyn som certifieringspraxisen för servercertifikatet. Handlingarna kan ändras med Myndigheten för digitalisering och befolkningsdatas interna ändringsförfarande.

Myndigheten för digitalisering och befolkningsdata informerar om ändringar i god tid innan de träder i kraft till Traficom och på sin egen webbplats.

Myndigheten för digitalisering och befolkningsdata förvaltar de olika versionerna av dokument och arkiverar samtliga certifikatpolicy- och certifieringspraxishandlingar. Typografiska korrigeringar och ändringar av kontaktuppgifter kan göras omedelbart.

1. Samtliga punkter i certifikatpolicyn och certifieringspraxisen kan ändras så att kommande väsentliga ändringar meddelas 30 dagar innan de träder i kraft.

2. Sådana punkter som enligt Myndigheten för digitalisering och befolkningsdata inte har någon väsentlig betydelse för certifikatinnehavare och förlitande parter kan ändras så att ändringarna meddelas 14 dagar innan de träder i kraft.

8.2 Ytterligare krav

Vid verkställandet av kraven som fastställs i punkt 7.3.4 ska beställare och förlitande parter informeras vad varje policy medför eller begränsar då det gäller kraven i certifikatpolicyn så som de fastställs i detta dokument.

8.3 Överensstämmelse med krav

Utfärdaren får uppge att man iakttar denna certifieringspraxis endast,

a) om utfärdaren uttrycker att man iakttar den specifika certifikatpolicyn och på begäran lämnar intyg till beställaren och de förlitande parterna om överensstämmelse med kraven. Intyget kan exempelvis vara auditerarens berättelse som bekräftar att utfärdaren uppfyller kraven i den specifika certifikatpolicyn. Det kan röra sig om en intern auditerare inom organisationen, men auditeraren får inte vara över- eller underordnat med avdelningen som utför utfärdarens verksamhet.

b) om en behörig och oberoende part inom den senaste tiden har bedömt uppfyllningen av kraven i den specifika certifikatpolicyn hos utfärdaren. Resultaten av granskningen ska på begäran göras tillgängligt för beställarna och de förlitande parterna.