Servicecertifikatens tekniska information

Kundanvisningar

26.2.2024

Servicecertifikatens tekniska information

Innehållsförteckning

1 Allmänt om Myndigheten för digitalisering och befolkningdatas servicecertifikat

Myndigheten för digitalisering och befolkningsdata (MDB) beviljade servicecertifikat är programcertifikat som används för att autentisera serviceleverantörens server eller tjänst.

Servicecertifikaten baserar sig på standarden X.509 och med hjälp av dem är det möjligt att skapa en SSL-skyddad datatrafik mellan webbläsaren och servern eller mellan två servrar.

MDB är den enda finländska certifikatauktoriteten som erbjuder officiellt EU-kvalificerade QWAC-certifikat (Qualified website authentication certificate).

Det finns även testcertifikat för alla servicecertifikat som är avsedda för testmiljöer, förutom e-postcertifikatet. Test-certifikatens datainnehåll är samma som själva produktionscertifikatet.

MDB beviljar inte certifikat för det interna nätverket och inte heller wildcard-certifikat. Från och med 15.9.2023, beviljar inte MDB servercertifikat eller servercertifikat för social- och hälsovården baserat på enbart en IP-adress. På grund av detta måste certifikatansökan innehålla antingen ett domain-namn eller ett domain-namn och IP-adress.

Utöver detta kommer inte MDB bevilja servicecertifikat som innehåller en e-postadress, från och med den 15 september 2023. Denna ändring påverkar inte e-postcertifikat, som är en separat certifikattyp från servercertifikatet.

Det färdiga servicecertifikatet skickas per e-post i DER- och PEM-filformat till tekniska processens e-postadress och tekniska kontaktpersonens e-post som angetts i ansökan.

2. Servicecertifikatprodukters tekniska beskrivningar

I detta dokument beskrivs kortfattat Myndigheten för digitalisering och befolkningdatas servicecertifikatens tekniska specifikationer.

2.1 Servercertifikat

Myndigheten för digitalisering och befolkningsdata är den enda finländska certifikatauktoriteten som erbjuder officiellt EU-kvalificerade QWAC-certifikat (Qualified website authentication certificate).

Med hjälp av servercertifikatet kan den som utnyttjar nättjänsten försäkra sig om att tjänsteleverantören är äkta. Servercertifikaten möjliggör även en kryptering av datatrafiken mellan servern och dess användare.

KaPa autentiseringscertifikat som behövs för att använda informationsleden, beställs via CSC-Tieteen tietotekniikan keskus Oy.

Servercertifikatets tekniska information:

CN (common name)	Domain eller IP-adress	Observera att om det finns en IP-adress i CN-fältet måste minst ett domain hitttas i SAN-fältet
SerialNumber	Inte ett obligatoriskt fält Det tillåtna informationsinnehållet är organisationens FO-nummer.	Undantag: För direkttulldeklarering innehåller detta fält den moms/EORI som deklarerats till Tullen i EDI-ansökan.
O (Organisation)	Organisationens officiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	T.ex. Nyland
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Det får vara max. 3 DNS namn i en certifikatbegäran. Dessa kan vara IP-adresser eller domain-namn.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Certificates G2R eller G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication Client Authentication	
Key length, hash	Nyckelläng i RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.

2.2 Systemsignaturcertifikat

Systemsignaturcertifikatet används för att elektroniskt underteckna sådana handlingar som inte undertecknas med personcertifikat.

KaPa signaturcertifikat som behövs för att använda informationsleden, beställs via CSC-Tieteen tietotekniikan keskus Oy.

CN (common name)	Systemets namn (t.ex. informationssystem för patientuppgifter)	Informationsinnehåll som är även tillåtet: organisationens namn, domain eller IP-adress
SerialNumber	Organisationens FO-nummer	
O (Organisation)	Organisationens officiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	
SubjectAlternativeName (SAN)	Fältet är inte tillåtet för systemsignaturcertifikat	
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Certificates G2R eller G2E	
Key Usages	Digital Signature NonReputation	
Extended Key Usages	-	
Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 24 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.

2.3 BDS-förfrågningsgränssnittens kundcertifikat

BDS-förfrågninsgränssnittens kundcertifikat är ett certifikat för gränssnittets klientanvändning (client) av gränssnittet för MDB:s egna BDS-kunder.

CN (common name)	Systemets namn	Informationsinnehåll som är även tillåtet: organisationens namn, domain eller IP-adress
SerialNumber	Organisationens FO-nummer	
O (Organisation)	Organisationens oficiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	
SubjectAlternativeName (SAN)	Valfritt fält: DNSname1 DNSname2 DNSname3	Det får vara max. 3 DNS namn i en certifikatbegäran. Dessa kan vara IP-adresser eller domain-namn.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Certificates G2R eller G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.

2.4 Stämpelcertifikat och stämpeltjänstens gränssnittscertifikat

MDB erbjuder stämpeltjänst och teststämpeltjänst. Stämpelcertifikat och stämpeltjänstens gränssnittcertifikat beviljas endast för stämpeltjänstens och teststämpeltjänstens användare. Läs mera:

2.5 E-postcertifikat

E-postcertifikat är avsedda för delade e-postadresser som används av flera personer inom en organisation. Med hjälp av e-postcertifikatet kan du ta emot krypterade meddelanden och använda signatur för utgående meddelanden. Krypterade meddelanden som inkommit till organisationens e-postadress öppnas med hjälp av e-postcertifikatet.

CN (common name)	Ett beskrivande namn för e-postlådan, t.ex. "företags-namn" informationshantering	
SerialNumber	Organisationens FO-nummer	
O (Organisation)	Organisationens officiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	
SubjectAlternativeName (SAN)	eMail	Observera att MDB producerar e-postcertifikat endast för delade e-postar, vars slutdel av domain inte är organisationens egna.
CA (intermediate CA / sub-CA)	DVV Enterprise Certificates	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	eMail protection	
Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 24 månader	

E-postcertifikatet är filbaserat och ingen kortläsare eller några separata program

behövs för att använda det. E-postcertifikatet fungerar i de vanligaste e-postprogrammen med stöd för S/MIME-meddelanden, som i Internet Explorer webbläsare.

E-postcertifikat är i PKCS#12-format.

2.6 Servercertifikat för social- och hälsovården

En organisation som ansluter sig som användare av Kanta-tjänsterna behöver servercertifikat för att använda tjänsterna eReceptet och eArkivet. Servercertifikatet behövs för att skydda datakommunikationen (TLS-kryptering) mellan den anslutande organisationens server och Kanta-servern.

CN (common name)	Domain eller IP-adress	Observera att om det finns en IP-adress i CN-fältet måste minst ett domain hittas i SAN-fältet
SerialNumber	OID enligt Kanta-kodtjänsten	
O (Organisation)	Organisationens officiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	T.ex. Nyland
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Det får vara max. 3 DNS namn i en certifikatbegäran. Dessa kan vara IP-adresser eller domain-namn.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Social Welfare and Healthcare Service Certificates G3R eller G3E Test-certifikat: DVV TEST Social Welfare and Healthcare Service Certs G3R eller G3E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication Client Authentication	

Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.

2.7 Social- och hälsovårdens systemsignaturcertifikat

Vid anslutning som användare i Kanta-tjänsternas patientuppgiftsarkiv behövs ett systemsignaturcertifikat.

Systemsignaturcertifikatet används för att elektroniskt underteckna sådana handlingar som inte undertecknas med personcertifikat för hälsovården.

CN (common name)	Systemets namn t.ex. informationssystem för patientuppgifter	Informationsinnehåll som är även tillåtet: organisationens namn, domain eller IP-adress
SerialNumber	OID enligt Kanta-kodtjänsten	
O (Organisation)	Organisationens officiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	
SubjectAlternativeName (SAN)	Fältet är inte tillåtet för systemsignaturcertifikat	
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Social Welfare and Healthcare Service Certificates G3R eller G3E Test-certifikat: DVV TEST Social Welfare and Healthcare Service Certs G3R eller G3E	
Key Usages	Digital Signature NonReputation	

Extended Key Usages	-	
Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 24 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.

2.8 Servicecertifikat för hälsoapplikationer

Servicecertifikat för hälsoapplikationer är avsett för att skydda meddelandetrafiken i hälsoapplikationer. Till exempel mobilapplikationer vars användare samlar hälsoinformation om personer och vidarebefordrar informationen till FPAs MittKanta för användning.

CN (common name)	Domain eller IP-adress	Observera att om det finns en IP-adress i CN-fältet måste minst ett domain hittas i SAN-fältet
SerialNumber	OID enligt Kanta-kodtjänsten	
O (Organisation)	Organisationens oficiella namn	
C (Country)	Landet där organisationen är verksam	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller landskap	T.ex. Nyland
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3	Det får vara max. 3 DNS namn i en certifikatbegäran. Dessa kan vara IP-adresser eller domain-namn.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Certificates G2R eller G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Server Authentication	

	Client Authentication	
Key length, hash	Nyckellängd RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader	

Endast RFC 5280-standardattribut är giltiga, certifikatbegäran ska inte innehålla applikationer eller systemleverantörers (t.ex. Microsoft) custom-attribut eller extensioner.

Endast certifikatbegäran (.CSR) enligt formatet PKCS #10.