Servicecertifikatens tekniska information

Kundanvisningar

26.1.2026

26.1.2026

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.

Servicecertifikat är en allmän benämning för alla typer av servicecertifikatsprodukter som erbjuds av MDB.

MDB:s produkter bygger på X.509-standarden och med deras hjälp är det möjligt att förverkliga SSL/TLS-säker kommunikation mellan webbläsare och server eller mellan två servrar.

MDB är den enda finska certifieraren som officiellt erbjuder EU-godkända servercertifikat (servercertifikat, KaPa autentiseringscertifikat, välfärdsapplikationscertifikat), alltså 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 servercertifikat som innehåller en e-postadress, från och med den 15 september 2023. Denna ändring påverkar inte tex 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.

Under år 2026 kommer MDB att erbjuda sina kunder möjligheten att använda ACME-protokollet för att skapa certifikat.

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. Här blir det dock ändringar under 2026.

Servercertifikatets tekniska information:

CN (CommonName)	Domännamn eller IP-adress Inte ett obligatoriskt fält, kommer att tas bort under 2026. I ACME används inte CN-fältet längre.	Observera att om det finns en IP-adress i CN-fältet måste minst ett domännamn hittas i SAN-fältet
SerialNumber OrganizationIdentifier	Tillåtet innehåll är organisationens FO-nummer (SerialNumber) och någon av eIDAS tillåtna organisationsidentifierare (OrganizationIdentifier-fältet) Ej obligatoriskt fält. Under 2026 i alla certifikat och I ACME omedelbart, ersätts fältet SerialNumber med fältet OrganizationIdentifier.	Undantag: För direkttulldeklarering innehåller detta fält den moms/EORI som deklarerats till Tullen i EDI-ansökan.
O (Organization)	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 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E	

	Test-certifikat: DVV TEST Service Certificates G2R eller G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement kommer att tas bort i framtiden.
Extended Key Usages	Server Authentication Client Authentication	Observera! Client auth tas bort från servercertifikat under år 2026 och i ACME direkt vid aktivering.
Key length, hash	Nyckelläng i RSA minst 2048 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader till 14.3.2026	Från och med 15.3.2026 max 6 mån

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. Här blir det dock ändringar under 2026.

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)	Valfritt fält: DNS-name1 DNSname2 DNSname3 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser. Tillåtet värde: gemensam e-postadress
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Service 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 Kundcertifikat

Kundcertifikat används i gränssnitt (client authentication). Denna produkt heter VTJ.gränssnittets kundcertifikat fram till den 28.2.2026.

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 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser. Tillåtet värde: gemensam e-postadress
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Service 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.

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 t.ex. Microsoft Outlook.

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 (CommonName)	Domain eller IP-adress Inte ett obligatoriskt fält, kommer att tas bort under 2026. I	Observera att om det finns en IP-adress i CN-fältet måste minst ett domain hittas i SAN-fältet

	ACME används inte CN-fältet längre.	
SerialNumber OrganizationIdentifier	Fpa/THL nationella kod-tjänst OID (SerialNumber) Fpa meddelar senare under 2026 i vilken form OID ska anges i fältet OrganizationIdentifier.	
O (Organisation)	Organisationens officiella namn i Fpa/THL nationalla kodtjänsten.	
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 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser.
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 (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement kommer att tas bort i framtiden.
Extended Key Usages	Server Authentication Client Authentication	Observera! Client auth tas bort från servercertifikat under år 2026 och i ACME direkt vid aktivering.
Key length, hash	Nyckellängd RSA minst 3072 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader till 14.3.2026	Från och med 15.3.2026 max 6 mån

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	Fpa/THL nationella kodtjänst OID	
O (Organisation)	Organisationens officiella namn i Fpa/THL nationella kodtjänsten.	
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 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser. Tillåtet värde: gemensam e-postadress
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 3072 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 Inte ett obligatoriskt fält, kommer att tas bort under 2026. I ACME används inte CN-fältet längre.	Observera att om det finns en IP-adress i CN-fältet måste minst ett domain hittas i SAN-fältet
SerialNumber OrganizationIdentifier	Fpa/THL nationella kod-tjänst OID (SerialNumber) Fpa meddelar senare under 2026 i vilken form OID ska anges i fältet OrganizationIdentifier.	
O (Organisation)	Organisationens oficiella namn i Fpa/THL nationella kodtjänsten	
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 IPaddress1 etc	Det får vara högst högst 5 domännamn och högst 5 IP-adresser.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates G5R eller G5E Test-certifikat: DVV TEST Service Certificates G2R eller G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement kommer att tas bort i framtiden.

Extended Key Usages	Server Authentication Client Authentication	Observera! Client auth tas bort från servercertifikat under år 2026 och i ACME direkt vid aktivering.
Key length, hash	Nyckellängd RSA minst 3072 byte, ECC minst 256 byte; SHA384 (ECC) och SHA512 (RSA)	
Giltighetstid	Max. 12 månader till 14.3.2026	Från och med 15.3.2026 max 6 mån

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.