MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Teknisk information om Servicecertifikat

Kundanvisning

8.7.2026

Tel. **0295 536 000** (växel) | Kontaktuppgifter: **dvv.fi/sv**

Innehållsförteckning

1 Allmänt om MDB:s servicecertifikat

Myndigheten för digitalisering och befolkningsdata (MDB) servicecertifikat är programvarucertifikat som används för att verifiera en tjänsteleverantörs server eller tjänst.

Servicecertifikat är ett allmännamn för alla servicecertifikatprodukter som erbjuds av MDB.

MDB:s produkter baseras på X.509-standarden och gör det möjligt att implementera SSL/TLS-skyddad kommunikation mellan en webbläsare och en server eller mellan två servrar.

MDB är den enda finländska certifikatutfärdaren som officiellt erbjuder EU-kvalificerade servercertifikat (servercertifikat, certifikat för välfärdsapplikationer), dvs. QWAC-certifikat (Qualified Website Authentication Certificate).

För alla servicecertifikat finns även testcertifikat avsedda för testmiljöer. Innehållet i ett testcertifikat är detsamma som i motsvarande produktionscertifikat.

MDB utfärdar inte certifikat för interna nätverk och inte heller wildcard-certifikat. Myndigheten för digitalisering och befolkningsdata utfärdar inte längre servercertifikat eller servercertifikat för social- och hälsovården enbart baserat på en IP-adress från och med den 15 september 2023. Därför måste certifikatansökan innehålla antingen ett domännamn eller både ett domännamn och en IP-adress.

Dessutom utfärdar MDB från och med den 15 september 2023 inte servercertifikat som innehåller en e-postadress. Denna ändring påverkar inte till exempel systemsigneringscertifikat eller klientcertifikat, som är separata certifikattyper och inte EU- kvalificerade produkter.

Det färdiga servicecertifikatet levereras per e-post till den tekniska gruppadress som anges i ansökan samt till den tekniska kontaktpersonen i DER- och PEM-filformat.

Beskrivningar av Informationsledens (palveluväylä) certifikat finns i tjänstens egna kundanvisningar. Kort sagt: Informationsled Autentiseringscertifikatet är ett kundcertifikat och Informationsled Signaturcertifikat är ett signeringscertifikat.

Under 2026 kommer MDB att erbjuda sina kunder möjlighet att börja använda ACME-protokollet för att utfärda certifikat.

2 Tekniska beskrivningar av servicecertifikatprodukter

I detta dokument beskrivs kort de tekniska specifikationerna för Myndigheten för digitalisering och befolkningsdatas servicecertifikat.

2.1 Servercertifikat

Myndigheten för digitalisering och befolkningsdata är den enda finländska certifikatutfärdaren som officiellt erbjuder 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 datatrafi ken mellan servern och dess användare.

Tekniska uppgifter för servercertifikat:

CN (common name)	Domännamn eller IP-adress Ej obligatoriskt fält, tas ur bruk från och med 1.10.2026. I ACME används inte CN-fältet.	Observera att om CN-fältet innehåller en IP-adress måste SAN-fältet innehålla minst ett domännamn.
SerialNumber OrganizationIdentifier	Tillåtet innehåll är organisationens FO-nummer (SerialNumber) samt någon av de organisationsidentifierare som tillåts enligt ETSI EN 319 412-1 (fältet OrganizationIdentifier). Ej obligatoriskt fält. Från och med 1.10.2026, och i ACME omedelbart, ersätts fältet SerialNumber av fältet OrganizationIdentifier.	Undantag: För Tullens direktförtullning ska det VAT/EORI som angetts till Tullen i EDI-ansökan anges i detta fält.
O (Organization)	Organisationens officiella namn	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller region/län	T.ex. Nyland
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas högst 5 domännamn och högst 5 IP-adresser. I ett servercertifikat ska det finnas minst ett domännamn.
CA (intermediate CA / sub-CA)	produktionscertifikat: DVV Service Certificates - G5R eller - G5E	

	Testcertifikat: DVV TEST Service Certificates - G2R eller - G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment och Key Agreement tas bort från certifikat från och med 1.10.2026.
Extended Key Usages	Server Authentication Client Authentication	Obs! Client Authentication tas bort från servercertifikat från och med 1.10.2026 och i ACME från och med införandet.
Key length, hash	Nyckellängden är minst 2048 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 6 månader	Från och med 15.3.2027 högst 3 månader

Endast attribut enligt RFC 5280-standarden är tillåtna; certifikatbegäran får inte innehålla några applikations- eller leverantörsspecifika (t.ex. Microsoft) egna attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR).

2.2 Systemsignaturcertifikat

Med ett systemsignaturcertifikat signeras elektroniskt sådana dokument som inte signeras med personcertifikat.

CN (common name)	Systemets namn (t.ex. patientdatasystem)	Även tillåtet innehåll: organisationens namn, domän eller IP-adress
SerialNumber	Organisationens FO-nummer	
O (Organization)	Organisationens originella namn	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas 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 Testcertifikat: DVV TEST Service Certificates - G2R eller - G2E	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	Nyckellängden för RSA är minst 2048 bitar och för ECC minst 256 bitar; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 24 månader	

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Vi godkänner endast certifikatbegäranden i PKCS#10-format (.CSR).

2.3 Kundcertifikat

Kundcertifikat är ett certifikat för kundautentisering i gränssnittsanvändning (client authentication). Denna produkt benämndes som klientcertifikat för VTJ-gränssnittet fram till 28.2.2026.

CN (common name)	Systemets namn	Även tillåtet innehåll: organisationens namn, domän eller IP-adress
SerialNumber	Organisationens FO-nummer	
O (Organization)	Organisationens originella namn	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	
SubjectAlternativeName (SAN)	Frivillig fält: DNSname1 DNSname2 DNSname3 IPaddress1	I en och samma certifikatbegäran får det finnas högst 5 domännamn och högst 5 IP-adresser.

	osv.	Tillåtet värde: gemensam e-postadress
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates - G5R eller - G5E Testcertifikat: DVV TEST Certificates - G2R eller - G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Nyckellängden är minst 2048 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 12 månader	

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) egna attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR).

2.4 Stämpelcertifikat och gränssnittscertifikat för stämpeltjänsten

MDB erbjuder en stämpeltjänst och en teststämpeltjänst. Stämpelcertifikat och gränssnittscertifikat för stämpeltjänsten utfärdas endast till organisationer som har beställt stämpeltjänsten eller teststämpeltjänsten.

2.5 E-postcertifikat

E-postcertifikat är avsett för att verifiera gemensamma e-postadresser som används av organisationer. Med hjälp av ett e-postcertifikat kan du ta emot krypterade meddelanden och signera utgående meddelanden. Krypterade meddelanden som skickas till organisationens e-postadress öppnas med hjälp av e-postcertifikatet.

CN (common name)	Ett namn som beskriver e-postlådan, till exempel “företagets namn” eller “fakturering” eller liknande	
SerialNumber	Organisationens FO-nummer	
O (Organization)	Organisationens officiella namn	

C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	
SubjectAlternativeName (SAN)	eMail	Observera att DVV endast utfärdar e-postcertifikat för gemensamma e-postadresser där domändelen tillhör organisationen.
CA (intermediate CA / sub-CA)	DVV Enterprise Certificates	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	eMail protection	
Key length, hash	Nyckellängden är 2048 eller 4096 bitar; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 24 månader	

E-postcertifikatet är filbaserat och kräver inga kortläsare eller separat programvara för användning. E-postcertifikatet fungerar i de vanligaste e-postprogrammen som stöder S/MIME-meddelanden, såsom Microsoft Outlook.

E-postcertifikaten 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 eRecept- och eArkivtjänsterna. Servercertifikatet behövs för att skydda datakommunikationsförbindelsen (TLS-skyddad) mellan den anslutande organisationens server och Kanta-servrarna. Detta certifikat är ett EU- kvalificerat QWAC-certifikat (Qualified Website Authentication Certificate).

CN (common name)	Domain eller IP adress Inte ett obligatoriskt fält. Fältet tas ur bruk den 1.10.2026. I ACME används inte CN-fältet.	Observera att om CN-fältet innehåller en IP-adress måste SAN-fältet innehålla minst ett domännamn.
SerialNumber OrganizationIdentifier	KELA/THL:s nationella kodserver-OID (SerialNumber). I fältet OrganizationIdentifier anges OID i formatet SO:FI-OID.	Från och med 1.10.2026 används fältet OrganizationIdentifier (i ACME redan från

		införandet), före detta används fältet SerialNumber.
O (Organization)	Organisationens officiella namn: KELA/THL:s nationella kodserver	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	T.ex. Nyland
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 osv	I en och samma certifikatbegäran får det finnas högst 5 domännamn och högst 5 IP-adresser. Fältet ska innehålla minst ett domännamn.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Social Welfare and Healthcare Service Certificates - G3R eller - G3E Testcertifikat: DVV TEST Social Welfare and Healthcare Service Certs - G3R eller - G3E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment och Key Agreement kommer att tas bort från certifikaten från och med den 1.10.2026.
Extended Key Usages	Server Authentication Client Authentication	OBS! Client Authentication tas bort från certifikatet från och med 1.10.2026, och i ACME finns användningsändamålet inte tillgängligt redan från införandet.
Key length, hash	Nyckellängden är minst 3072 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max 6 månader	Från och med 15.3.2027 högst 3 månader.

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR).

2.7 Social- och hälsovårdens systemsignaturcertifikat

Vid anslutning som användare av Kanta-tjänsternas patientdataarkiv krävs ett systemsigneringscertifikat.

Med ett systemsigneringscertifikat signeras elektroniskt sådana dokument som inte signeras med hälso- och sjukvårdens personcertifikat.

CN (common name)	Systemets namn, t.ex. patientdatasystem	Även tillåtet innehåll: organisationens namn, domän eller IP-adress.
SerialNumber	KELA/THL:s nationella kodserver-OID	
O (Organization)	Organisationens officiella namn: KELA/THL:s nationella kodserver	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	
SubjectAlternativeName (SAN)	Valfritt fält: DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas 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. Testcertifikat: DVV TEST Social Welfare and Healthcare Service Certs - G3R eller - G3E	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	Nyckellängden är minst 3072 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 24 månader	

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR).

2.8 Kundcertifikat för social- och hälsovården

Kundcertifikat är ett certifikat för kundautentisering i gränssnittsanvändning (client authentication). En del av de organisationer som ansluter sig som användare av Kanta-tjänsterna behöver ett servercertifikat för social- och hälsovården, medan andra behöver ett klientcertifikat för social- och hälsovården (kontakta FPA om det råder osäkerhet om vilket certifikat som behövs). Vissa organisationer kommer att behöva båda ovan nämnda certifikat från och med 1.10.2026, då Client Authentication tas bort från servercertifikaten.

CN (common name)	Systemets namn	Även tillåtet innehåll: organisationens namn, domän eller IP-adress.
SerialNumber	KELA/THL:s nationella kodserver-OID	
O (Organization)	Organisationens officiella namn: KELA/THL:s nationella kodserver	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	
SubjectAlternativeName (SAN)	Valfritt fält: DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas 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 Testcertifikat: DVV TEST Social Welfare and Healthcare Service Certs - G3R eller - G3E	
Key Usages	Key Encipherment Digital Signature	

Extended Key Usages	Client Authentication	
Key length, hash	Nyckellängden är minst 2048 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 12 månader	

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR) accepteras.

2.9 Servicecertifikat för hälsoapplikationer

Ett servercertifikat för social- och hälsovården som utfärdas för att skydda meddelandekommunikationen i välfärdsapplikationer. Det handlar till exempel om mobilapplikationer med vilka användare samlar in hälsouppgifter om en person och förmedlar dem vidare till FPA:s Kanta för vidare användning. Detta certifikat är ett EU-kvalificerat QWAC-certifikat (Qualified Website Authentication Certificate).

CN (CommonName)	Domän eller IP-adress. Inte ett obligatoriskt fält. Fältet tas ur bruk den 1.10.2026. I ACME används inte CN-fältet.	Observera att om CN-fältet innehåller en IP-adress måste SAN-fältet innehålla minst ett domännamn.
SerialNumber OrganizationIdentifier	KELA/THL:s nationella kodserver-OID (SerialNumber). I fältet OrganizationIdentifier anges OID i formatet SO:FI-OID.	Från och med 1.10.2026 används fältet OrganizationIdentifier (i ACME redan från införandet), före detta används fältet SerialNumber.
O (Organization)	Organisationens officiella namn: KELA/THL:s nationella kodserver	
C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	T.ex. Nyland
SubjectAlternativeName (SAN)	Valfritt fält: DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas högst 5 domännamn och högst 5 IP-adresser. Fältet ska innehålla minst ett domännamn.

CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates - G5R eller - G5E. Testcertifikat: DVV TEST Service Certificates - G2R eller - G2E.	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment och Key Agreement kommer att tas bort från certifikaten från och med den 1.10.2026.
Extended Key Usages	Server Authentication Client Authentication	Obs! Client Authentication tas bort från certifikatet från och med 1.10.2026 och i ACME redan från införandet.
Key length, hash	Nyckellängden är minst 3072 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 6 månader	Från och med 15.3.2027 högst 3 månader.

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR).

2.10 Kundcertifikat för hälsoapplikationstjänster

Servercertifikat för social- och hälsovården som utfärdas för att skydda meddelandetrafiken i välfärdsapplikationer. Det handlar till exempel om mobilapplikationer med vilka användare samlar in hälsouppgifter om en person och förmedlar dem vidare till FPA:s Kanta för användning. Detta certifikat är ett EU-kvalificerat QWAC-certifikat (Qualified Website Authentication Certificate).

CN (CommonName)	Systemets namn	Även tillåtet innehåll: organisationens namn, domän eller IP-adress.
SerialNumber	KELA/THL:s nationella kodserver-OID (SerialNumber). I fältet OrganizationIdentifier anges OID i formatet SO:FI-OID.	
O (Organization)	Organisationens officiella namn: KELA/THL:s nationella kodserver	

C (Country)	Land där organisationen verkar	
L (Location)	Stad eller kommun där organisationen är registrerad	
S (State)	Land eller län	T.ex. Nyland
SubjectAlternativeName (SAN)	Valfritt fält: DNSname1 DNSname2 DNSname3 IPaddress1 osv.	I en och samma certifikatbegäran får det finnas högst 5 domännamn och högst 5 IP-adresser.
CA (intermediate CA / sub-CA)	Produktionscertifikat: DVV Service Certificates - G5R eller - G5E Testcertifikat: DVV TEST Service Certificates - G2R eller - G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Nyckellängden är minst 3072 bitar för RSA och minst 256 bitar för ECC; SHA384 (ECC) och SHA512 (RSA).	
Giltighetstid	Max. 12 månader	

Endast attribut enligt RFC 5280-standarden är tillåtna. Certifikatbegäran får inte innehålla några applikations- eller systemleverantörsspecifika (t.ex. Microsoft) anpassade attribut eller extensioner.

Endast certifikatbegäranden i PKCS#10-format (.CSR) accepteras.