Palveluvarmenteiden tekniset tiedot

Asiakasohje

8.7.2026

Palveluvarmenteiden tekniset tiedot

Sisällysluettelo

1 Yleistä Digi- ja väestötietoviraston palveluvarmenteista

Digi- ja väestötietoviraston (DVV) myöntämät palveluvarmenteet ovat ohjelmistovarmenteita, joilla varmennetaan palveluntarjoajan palvelin tai palvelu.

Palveluvarmenne on yleisnimitys kaikille DVV:n tarjoamille palveluvarmennetuotteille.

DVV:n tuotteet perustuvat X.509 standardiin ja niiden avulla on mahdollista toteuttaa selaimen ja palvelimen tai kahden palvelimen välille SSL/TLS-suojattu tietoliikenne.

DVV on ainoa suomalainen varmentaja, joka tarjoaa virallisesti EU-hyväksyttyjä palvelinvarmenteita (palvelinvarmenne, hyvinvointisovellusvarmenne), eli QWAC-varmenteita (Qualified website authentication certificate).

Kaikista palveluvarmenteista on saatavilla myös testiympäristöihin tarkoitetut testivarmenteet. Testivarmenteen tietosisältö on sama kuin varsinaisen tuotantovarmenteen.

DVV ei myönnä varmenteita sisäverkkoon eikä myöskään wildcard-varmenteita. Digi- ja väestötietovirasto ei enää myönnä palvelinvarmenteita tai soten palvelinvarmenteita pelkän IP-osoitteen perusteella 15.9.2023 alkaen. Tämän johdosta varmennehakemuksessa on oltava joko domainnimi tai domainnimi ja IP-osoite.

Tämän lisäksi DVV ei myönnä 15.9.2023 alkaen palvelinvarmenteita, jotka sisältävät sähköpostiosoitteen. Tämä muutos ei vaikuta esim. järjestelmäallekirjoitusvarmenteisiin tai asiakasvarmenteisiin, jotka ovat palvelinvarmenteesta erillinen varmennetyyppejä eivätkä ole EU-hyväksyttyjä tuotteita.

Valmis palveluvarmenne toimitetaan sähköpostitse hakemuksella määriteltyyn tekniseen yhteissähköpostiin sekä tekniselle yhteyshenkilölle DER- ja PEM-tiedostomuodoissa.

Palveluväylän varmenteiden kuvaukset löytyvät palvelun omista asiakasohjeista. Lyhyesti: palveluväylän autentikointivarmenne on asiakasvarmenne ja palveluväylän järjestelmäallekirjoitusvarmenne on järjestelmäallekirjoitusvarmenne.

Vuoden 2026 aikana DVV tulee tarjoamaan asiakkailleen mahdollisuuden ottaa käyttöön ACME-protokolla varmenteiden tuottamiseen.

2 Palveluvarmennetuotteiden tekniset kuvaukset

Tässä dokumentissa kuvataan lyhyesti Digi- ja väestötietoviraston palveluvarmenteiden tekniset määritykset.

2.1 Palvelinvarmenne

Digi- ja väestötietovirasto on ainoa suomalainen varmentaja, joka tarjoaa virallisesti EU-hyväksyttyjä QWAC-varmenteita (Qualified website authentication certificate).

Palvelinvarmenteen (server authentification varmenne) avulla verkkopalvelun käyttäjä voi varmistua palvelun tarjoajan aitoudesta. Palvelinvarmenteet mahdollistavat myös palvelimen ja sen käyttäjän välisen tietoliikenteen salaamisen.

Palvelinvarmenteen tekniset tiedot:

CN (common name)	Domainnimi tai IP osoite Ei pakollinen kenttä, poistuu 1.10.2026 alkaen käytöstä. ACME:ssa ei CN-kenttä ole käytössä.	Huomaa että mikäli CN kentässä on IP-osoite, tulee SAN-kentästä löytyä vähintään yksi domainnimi.
SerialNumber OrganizationIdentifier	Sallittu tietosisältö on organisaation Y-tunnus (SerialNumber) ja jokin ETSI EN 319 412-1 sallimista organisaatiotunnisteista (OrganizationIdentifier-kenttä) Ei pakollinen kenttä. 1.10.2026 lähtien kaikissa ja ACME:ssa heti, SerialNumber-kentän korvaa OrganizationIdentifier-kenttä.	Poikkeus: Tullin suoratullausta varten tähän kenttään tulee Tullille EDI-hakemuksessa ilmoitettu VAT/ EORI.
O (Organization)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Palvelinvarmenteessa tulee olla vähintään 1 domainnimi.

CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates - G5R tai - G5E Testivarmenteet: DVV TEST Service Certificates - G2R tai - G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement ovat poistumassa varmenteista 1.10.2026 alkaen.
Extended Key Usages	Server Authentication Client Authentication	Huom! Client Authentication poistuu palvelinvarmenteista 1.10.2026 ja ACME:ssa käyttöönotosta alkaen.
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 6 kuukautta	15.3.2027 alkaen max 3 kk

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.2 Järjestelmäallekirjoitusvarmenne

Järjestelmäallekirjoitusvarmenteella allekirjoitetaan sähköisesti sellaiset asiakirjat, joita ei allekirjoiteta henkilövarmenteilla.

Palveluväylän käyttöä varten tarvittavat KaPa järjestelmäallekirjoitusvarmenteet tilataan CSC-Tieteen tietotekniikan keskus Oy:n kautta. Tähän on kuitenkin luvassa muutoksia vuoden 2026 aikana. Muutoksista tiedotetaan palveluväylän asiakkaita erikseen.

CN (common name)	Järjestelmän nimi (esim. potilastietojärjestelmä)	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	Organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	

SubjectAlternativeName (SAN)	Vapaaehtoinen kenttä: DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Sallittu arvo: yhteissähköpostiosoite
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates - G5R tai - G5E Testivarmenteet: DVV TEST Service Certificates - G2R tai - G2E	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	Avainpituus RSA on vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.3 Asiakasvarmenne

Asiakasvarmenne on varmenne rajapintojen asiakaskäyttöä (client authentication) varten. Tämä tuote kulki nimellä VTJ-rajapinnan asiakasvarmenne 28.2.2026 asti.

CN (common name)	Järjestelmän nimi	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	Organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	

SubjectAlternativeName (SAN)	Vapaaehtoinen kenttä: DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Sallittu arvo: yhteissähköpostiosoite
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates -G5R tai -G5E Testivarmenteet: DVV TEST Certificates -G2R tai -G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.4 Leimavarmenne ja leimapalvelun rajapintavarmenne

DVV tarjoaa leimapalvelun ja testileimapalvelun. Leimavarmenteita ja leimapalvelun rajapintavarmenteita myönnetään vain leimapalvelun ja testileimapalvelun tilanneille organisaatioille.

2.5 Sähköpostivarmenne

Sähköpostivarmenne on tarkoitettu organisaatioiden käytössä olevien, yhteiskäyttöisten sähköpostiosoitteiden varmentamiseen. Sähköpostivarmenteen avulla voit vastaanottaa salattuja viestejä ja allekirjoittaa lähtevät viestit. Organisaation sähköpostiosoitteeseen saapuneet salatut viestit avataan sähköpostivarmenteen avulla.

CN (common name)	Sähköpostilaatikkoa kuvaava nimi kuten esim. ”yrityksen nimi” tai ”laskutus” tms	

SerialNumber	organisaation y-tunnus	
O (Organisation)	Organisaation virallinen nimi	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	eMail	Huomaa että DVV tuottaa sähköpostivarmenteita vain yhteiskäytösiin sähköposteihin jonka loppuosan domain on organisaation oma.
CA (intermediate CA / sub-CA)	DVV Enterprise Certificates	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	eMail protection	
Key length, hash	Avainpituus on 2048 tai 4096 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Sähköpostivarmenne on tiedostopohjainen, eikä sen käyttämiseen ei tarvita kortinlukijoita tai erillisiä ohjelmistoja. Sähköpostivarmenne toimii yleisemmissä S/MIME-viestejä tukevissa sähköpostiohjelmissa kuten Microsoft Outlook-sähköpostiohjelmassa.

Sähköpostivarmenteet ovat PKCS#12-formaatissa.

2.6 Sosiaali- ja terveydenhuollon palvelinvarmenne

Kanta-palvelujen käyttäjäksi liittyvä organisaatio tarvitsee palvelinvarmenteet eResepti- ja eArkisto-palveluiden käyttämistä varten. Palvelinvarmenne tarvitaan suojaamaan tietoliikenneyhteys (TLS-suojattu) liittyvän organisaation palvelimen ja Kanta-palvelimien välille. Tämä varmenne on EU-hyväksytty QWAC-varmenne (Qualified website authentication certificate).

CN (common name)	Domain tai IP osoite Ei pakollinen kenttä, poistuu käytöstä 1.10.2026. ACME:ssa ei CN-kenttä ole käytössä.	Huomaa että mikäli CN-kentässä on IP-osoite, tulee SAN kentästä löytyä vähintään yksi domain
SerialNumber	KELA/THL kansallinen koodistopalvelin OID	1.10.2026 lähtien käytössä on OrganizationIdentifier

OrganizationIdentifier	(SerialNumber), OrganizationIdentifier-kenttään OID viedään muodossa SO:FI-OID.	kenttä (ACME:ssa jo heti käyttöönotosta), sitä ennen käytetään SerialNumber kenttää.
O (Organisation)	Organisaation virallinen nimi KELA/THL Kansallinen Koodistopalvelin	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Kentästä tulee löytyä vähintään 1 domainnimi.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates - G3R tai - G3E Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs - G3R tai - G3E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement ovat poistumassa varmenteista 1.10.2026 lähtien
Extended Key Usages	Server Authentication Client Authentication	HUOM! Client authentification poistuu varmenteesta 1.10.2026 ja ACME:ssa avainta ei löydy heti käyttöönotosta.
Key length, hash	Avainpituus on RSA vähintään 3072 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max 6 kuukautta	15.3.2027 alkaen max 3kk.

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.7 Sosiaali- ja terveydenhuollon järjestelmäallekirjoitusvarmenne

Kanta-palvelujen potilastiedon arkiston käyttäjiksi liityttäessä tarvitaan järjestelmäallekirjoitusvarmenne.

Järjestelmäallekirjoitusvarmenteella allekirjoitetaan sähköisesti sellaiset asiakirjat, joita ei allekirjoiteta terveydenhuollon henkilövarmenteilla.

CN (common name)	Järjestelmän nimi, esim. potilastietojärjestelmä	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	KELA/THL kansallinen koodistopalvelin OID	
O (Organisation)	Organisaation virallinen nimi KELA/THL Kansallinen Koodistopalvelin	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	Vapaaehtoinen kenttä: DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Sallittu arvo: yhteissähköpostiosoite
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates - G3R tai - G3E Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs - G3R tai - G3E	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	Avainpituus on RSA vähintään 3072 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 24 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai eks-tensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.8 Sosiaali- ja terveydenhuollon asiakasvarmenne

Asiakasvarmenne on varmenne rajapintojen asiakaskäyttöä (client authentication) varten. Kanta-palvelujen käyttäjäksi liittyvä organisaatioista osa tarvitsee SoTe palvelinvarmenteen ja osa SoTe asiakasvarmenteen (konsultoi KELA:aa mikäli tässä on epävarmuutta). Jotkut organisaatiot tarvitsevat molemmat edellä mainitut varmenteet 1.10.2026 lähtien kun palvelinvamenteista poistuu Client authentification.

CN (common name)	Järjestelmän nimi	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	KELA/THL kansallinen koodistopalvelin OID	
O (Organisation)	Organisaation virallinen nimi KELA/THL Kansallinen Koodistopalvelin	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	
SubjectAlternativeName (SAN)	Vapaaehtoinen kenttä: DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Sallittu arvo: yhteissähköpostiosoite
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates - G3R tai - G3E Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs - G3R tai - G3E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	

Key length, hash	Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.9 Hyvinvointisovelluspalveluvarmenne

Sosiaali- ja terveydenhuollon palvelinvarmenne, joka myönnetään hyvinvointisovellusten sanomaliikenteen suojaamiseksi. Kyseessä ovat esim. mobiilisovellukset joilla käyttäjät keräävät henkilöstä terveystietoja ja välittävät niitä eteenpäin Kelan Omakantaan hyödynnettäväksi. Tämä varmenne on EU-hyväksytty QWAC-varmenne (Qualified website authentication certificate).

CN (CommonName)	Domain tai IP osoite Ei pakollinen kenttä, poistuu 1.10.2026. ACME:ssa ei CN-kenttä ole käytössä.	Huomaa että mikäli CN-kentässä on IP-osoite, tulee SAN-kentästä löytyä vähintään yksi domain
SerialNumber OrganizationIdentifier	KELA/THL kansallinen koodistopalvelin OID (SerialNumber), OrganizatioIdentifier-kenttään OID viedään muodossa SO:FI-OID.	1.10.2026 lähtien käytössä on OrganizationIdentifier kenttä (ACME:ssa jo heti käyttöönotosta), sitä ennen käytetään SerialNumber kenttää.
O (Organisation)	Organisaation virallinen nimi KELA/THL Kansallinen Koodistopalvelin	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	
S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS-nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. Kentässä tulee olla vähintään yksi domainnimi.

CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates - G5R tai - G5E Testivarmenteet: DVV TEST Service Certificates - G2R tai - G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment ja Key Agreement ovat poistumassa varmenteista 1.10.2026.
Extended Key Usages	Server Authentication Client Authentication	Huom! Client Authentification poistuu varmenteesta 1.10.2026 ja ACME:ssa heti käyttöönotossa.
Key length, hash	Avainpituus on RSA vähintään 3072 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 6 kuukautta	15.3.2027 alkaen max 3 kk.

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai ekstensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).

2.10 Hyvinvointisovellusasiakasvarmenne

Sosiaali- ja terveydenhuollon palvelinvarmenne, joka myönnetään hyvinvointisovellusten sanomaliikenteen suojaamiseksi. Kyseessä ovat esim. mobiilisovellukset joilla käyttäjät keräävät henkilöstä terveystietoja ja välittävät niitä eteenpäin Kelan Omakantaan hyödynnettäväksi. Tämä varmenne on EU-hyväksytty QWAC-varmenne (Qualified website authentication certificate).

CN (CommonName)	Järjestelmän nimi	Myös sallittuja tietosisältöjä: organisaation nimi domain tai IP-osoite
SerialNumber	KELA/THL kansallinen koodistopalvelin OID (SerialNumber),	
O (Organisation)	Organisaation virallinen nimi KELA/THL Kansallinen Koodistopalvelin	
C (Country)	Maa missä organisaatio toimii	
L (Location)	Kaupunki tai kunta missä organisaation on kirjoilla	

S (State)	Maa tai maakunta	Esim. Uusimaa
SubjectAlternativeName (SAN)	Valinnainen kenttä: DNSname1 DNSname2 DNSname3 IPaddress1 jne	Näitä DNS-nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta.
CA (intermediate CA / sub-CA)	Tuotantovarmenteet: DVV Service Certificates - G5R tai - G5E Testivarmenteet: DVV TEST Service Certificates - G2R tai - G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	Avainpituus on RSA vähintään 3072 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA)	
Voimassaoloaika	Max. 12 kuukautta	

Vain RFC 5280 standardin mukaiset attribuutit käyvät, varmennepyynnössä ei tule olla sovellusten tai järjestelmätoimittajien (esim. Microsoft) custom attribuutteja- tai eks-tensioita.

Vain PKCS#10-formaatin mukaisia varmennepyyntöjä (.CSR).