# Palveluvarmenteiden tekniset tiedot

## Asiakasohje

26.1.2026

# Palveluvarmenteiden tekniset tiedot

## Sisällysluettelo

**1 Yleistä Digi- ja väestötietoviraston palveluvarmenteista ..... 3**
**2 Palveluvarmennetuotteiden tekniset kuvaukset ..... 3**
**2.1 Palvelinvarmenne ..... 3**
2.2 Järjestelmäallekirjoitusvarmenne ..... 5
2.3 Asiakasvarmenne ..... 6
**2.4 Leimavarmenne ja leimapalvelu rajapintavarmenne ..... 7**
**2.5 Sähköpostivarmenne ..... 7**
**2.6 Soten palvelinvarmenne ..... 8**
**2.7 Soten järjestelmäallekirjoitusvarmenne ..... 10**
**2.8 Hyvinvointisovellusvarmenne ..... 11**

# 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, KaPa autentikointivarmenne), eli QWAC-varmenteita (Qualified website authentication certificate).

Kaikista palveluvarmenteista on saatavilla myös testiympäristöihin tarkoitetut testivarmenteet, pois lukien sähköpostivarmenteet. 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 domain-nimi tai domain-nimi ja IP-osoite.

Tämän lisäksi DVV ei myönnä 15.9.2023 alkaen palvelinvarmenteita, jotka sisältävät sähköpostiosoitteen. Tämä muutos ei vaikuta esim. sähköpostivarmenteisiin, jotka ovat palvelinvarmenteesta erillinen varmennetyyppi.

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

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 avulla verkkopalvelun käyttäjä voi varmistua palvelun tarjoajan aitoudesta. Palvelinvarmenteet mahdollistavat myös palvelimen ja sen käyttäjän välisen tietoliikenteen salaamisen.

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

Palvelinvarmenteen tekniset tiedot:

| | | |
|---|---|---|
| CN (common name) | Domain tai IP osoite<br><br>Ei pakollinen kenttä, poistuu 2026 aikana. ACME:ssa ei CN-kenttä ole enää käytössä. | Huomaa että mikäli CN kentässä on IP-osoite, tulee SAN-kentästä löytyä vähintään yksi domain |
| SerialNumber<br><br>OrganizationIdentifier | Sallittu tietosisältö on organisaation Y-tunnus (SerialNumber) ja jokin ETSI EN 319 412-1 sallimista organisaatiotunnisteista (OrganizationIdentifier-kenttä)<br><br>Ei pakollinen kenttä. Vuoden 2026 aikana 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<br>DNSname2<br>DNSname3<br>IPaddress1<br>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<br>Testivarmenteet: DVV TEST Service Certificates G2R tai G2E | |
| Key Usages | Key Encipherment (RSA)<br>Key Agreement (ECC)<br><br>Digital Signature | Key Encipherment ja Key Agreement ovat poistumassa varmenteista tulevaisuudessa. |

| | | |
|---|---|---|
| Extended Key Usages | Server Authentication<br><br>Client Authentication | Huom! Client Authentication poistuu palvelinvarmenteista vuoden 2026 aikana ja ACME:ssa heti käyttöönotossa. |
| Key length, hash | Avainpituus on RSA vähintään 2048 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA) | |
| Voimassaoloaika | Max. 12 kuukautta 14.3.2026 asti | 15.3.2026 alkaen max 6 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:<br>organisaation nimi<br>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:<br>DNSname1<br>DNSname2<br>DNSname3<br>IPaddress1<br>jne | Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta.<br><br>Sallittu arvo: yhteissähköpostiosoite |

| | | |
|---|---|---|
| CA (intermediate CA / sub-CA) | Tuotantovarmenteet: DVV Service Certificates G5R tai G5E<br>Testivarmenteet: DVV TEST Service Certificates G2R tai G2E | |
| Key Usages | Digital Signature<br><br>NonReputation | |
| 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 eks-tensioita.

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

## 2.3 Asiakasvarmenne

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

| | | |
|---|---|---|
| CN (common name) | Järjestelmän nimi | Myös sallittuja tietosisältöjä:<br>organisaation nimi<br>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:<br>DNSname1<br>DNSname2<br>DNSname3<br>IPaddress1<br>jne | Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta.<br><br>Sallittu arvo: yhteissähköpostiosoite |

| | | |
|---|---|---|
| CA (intermediate CA / sub-CA) | Tuotantovarmenteet: DVV Service Certificates G5R tai G5E<br>Testivarmenteet: DVV TEST Certificates G2R tai G2E | |
| Key Usages | Key Encipherment<br>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 käyttöönottajalle.

## 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<br>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 Soten palvelinvarmenne

Kanta-palvelujen käyttäjäksi liittyvä organisaatio tarvitsee palvelinvarmenteet eReseptija eArkisto-palveluiden käyttämistä varten. Palvelinvarmenne tarvitaan suojaamaan tietoliikenneyhteys (TLS-suojattu) liittyvän organisaation palvelimen ja Kanta-palvelimien välille.

| | | |
|---|---|---|
| CN (common name) | Domain tai IP osoite<br><br>Ei pakollinen kenttä, poistuu 2026 aikana. ACME:ssa ei CN-kenttä ole enää käytössä. | Huomaa että mikäli CN-kentässä on IP-osoite, tulee SAN kentästä löytyä vähintään yksi domain |
| SerialNumber<br><br>OrganizationIdentifier | KELA/THL kansallinen koodistopalvelin OID (SerialNumber)<br>KELA ilmoittaa myöhemmin 2026 vuoden aikana, millaiseen muotoon OID viedään OrganizatioIdentifier-kentässä. | |

| | | |
|---|---|---|
| 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<br>DNSname2<br>DNSname3<br>IPaddress1<br>jne | Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta. |
| CA (intermediate CA / sub-CA) | Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates G3R tai G3E<br>Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs G3R tai G3E | |
| Key Usages | Key Encipherment (RSA)<br>Key Agreement (ECC)<br><br>Digital Signature | Key Encipherment ja Key Agreement ovat poistumassa varmenteista tulevaisuudessa. |
| Extended Key Usages | Server Authentication<br><br>Client Authentication | HUOM! Client authentification poistuu varmenteesta vuoden 2026 aikana ja ACME:ssa heti käyttöönotosta. |
| Key length, hash | Avainpituus on RSA vähintään 3072 bittiä, ECC vähintään 256 bittiä; SHA384 (ECC) ja SHA512 (RSA) | |
| Voimassaoloaika | Max 12 kuukautta 14.3.2026 asti | 15.3.2026 alkaen max 6kk. |

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 Soten 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:<br>organisaation nimi<br>domain tai IP-osoite |
| SerialNumber | KELA/THL kansallinen koodistopalvelin OID | |
| O (Organisation) | Organisaation virallinen nimi<br>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:<br>DNSname1<br>DNSname2<br>DNSname3<br>IPaddress1<br>jne | Näitä DNS nimiä saa yhdessä varmennepyynnössä olla max. 5 domain-nimeä ja max. 5 IP-osoitetta.<br><br>Sallittu arvo: yhteissähköpostiosoite |
| CA (intermediate CA / sub-CA) | Tuotantovarmenteet: DVV Social Welfare and Healthcare Service Certificates G3R tai G3E<br>Testivarmenteet: DVV TEST Social Welfare and Healthcare Service Certs G3R tai G3E | |
| Key Usages | Digital Signature<br><br>NonReputation | |
| 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 Hyvinvointisovellusvarmenne

Sosiaali- ja terveydenhuollon palvelinvarmenne, joka myönnetään hyvinvointisovellus-ten sanomaliikenteen suojaamiseksi. Kyseessä ovat esim. mobiilisovellukset joilla käyt-täjät keräävät henkilöstä terveystietoja ja välittävät niitä eteenpäin Kelan Omakantaan hyödynnettäväksi.

| | | |
|---|---|---|
| CN (CommonName) | Domain tai IP osoite<br><br>Ei pakollinen kenttä, poistuu 2026 aikana. ACME:ssa ei CN-kenttä ole enää käytössä. | Huomaa että mikäli CN-kentässä on IP-osoite, tulee SAN-kentästä löytyä vähintään yksi domain |
| 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 | Esim. Uusimaa |
| SubjectAlternativeName (SAN) | DNSname1<br>DNSname2<br>DNSname3<br>IPaddress1<br>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<br>Testivarmenteet: DVV TEST Service Certificates G2R tai G2E | |
| Key Usages | Key Encipherment (RSA)<br>Key Agreement (ECC)<br><br>Digital Signature | Key Encipherment ja Key Agreement ovat poistumassa varmenteista tulevaisuudessa. |
| Extended Key Usages | Server Authentication<br><br>Client Authentication | Huom! Client Authentification poistuu varmenteesta vuoden 2026 aikana 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. 12 kuukautta 14.3.2026 asti | 15.3.2026 alkaen max 6 kk. |

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).