

Kanta-varmennemuutokset tietoliikenteessä ja allekirjoituksissa

Toimittajayhteistyökokous 16.9.2026

Lari Kannisto

Kan
ta

SOTE-varmennemuutokset 1.10.2026 alkaen 1/2



- DVV:n varmennemuutokset koskevat myös SOTE-palveluvarmenteita
 - SOTE-palvelinvarmenne ja hyvinvointisovelluspalvelinvarmenne
 - CN-kenttä poistuu ja sen korvaa SubjectAltName (SAN=DNS) kenttä.
 - Palvelinvarmenteista poistuu Client Authentication ExtendedKeyUsage (EKU).
 - DVV eriyttää nykyiset palvelinvarmenteet kahdeksi erilliseksi tuotteeksi: palvelinvarmenne (Server Auth) ja asiakasvarmenne (Client Auth).
 - SerialNumber-kentän (OID 2.5.4.5) korvaa OrganizationIdentifier-kenttä (OID 2.5.4.97)
 - Samalla kentän sallitun tietosisällön muoto muuttuu.
 - Sosiaali- ja terveydenhuollon varmenteissa OrganizationIdentifier-kentässä käytetään EXC-muotoa.
 - KELA on määritellyt THL:n ylläpitämän kansallisen koodistopalvelimen tunnukseksi "SO:"
 - SO:+maatunnus+liityntäpisteen OID (sama OID joka aikaisemmin oli CN/SerialNumber –kentässä)
 - esimerkki SO:FI-1.2.246.553.....
 - Key Encipherment ja Key Agreement EKU:t poistuvat.
 - Varmenteen voimassaoloaika lyhenee CAB-forumin päätösten mukaisesti
 - 15.3.2026 alkaen TLS-varmenteen maksimi voimassaoloaika on 200 päivää.
 - 15.3.2027 alkaen TLS-varmenteen maksimi voimassaoloaika on 100 päivää.
 - 15.3.2029 alkaen TLS-varmenteen maksimi voimassaoloaika on 47 päivää.
 - VARMENNETTA KÄYTETYYÄN PALVELIMISSA JOIHIN ASIAKKAAT TAI PALVELIMET OTTAVAT YHTEYTTÄ

SOTE-varmennemuutokset 1.10.2026 alkaen 2/2



- UUDET SOTE-VARMENNETYYYPIT:
 - SOTE-asiakasvarmenne
 - CN-kentän lisäksi käytössä SubjectAltName (SAN=DNS) kenttä.
 - Varmenteissa vain Client Authentication ExtendedKeyUsage (EKU).
 - Liityntäpisteen OID on serialNumber-kentässä (OID 2.5.4.5)
 - Varmenteen voimassaoloaika on 12kk
 - Hyvinvointisovellusasiakasvarmenne
 - CN-kentän lisäksi käytössä SubjectAltName (SAN=DNS) kenttä.
 - Varmenteissa vain Client Authentication ExtendedKeyUsage (EKU).
 - Hyvinvointisovelluksen OID on serialNumber-kentässä (OID 2.5.4.5)
 - Varmenteen voimassaoloaika on 12kk
- KÄYTETÄÄN PALVELIMISSA JOTKA OTTAVAT YHTEYTTÄ MUIHIN PALVELIMIIN

Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 01:a0:03:ac:04:71:05:59:06:19:07:e0:08:22:09
 Signature Algorithm: sha512WithRSAEncryption
 Issuer: C=FI, O=Digi- ja vaestotietovirasto TEST, OU=Sosiaali- ja terveydenhuollon testipalveluvarmenteet, CN=DVV TEST
 Social Welfare and Healthcare Service Certs - G3R
 Validity
 Not Before: Aug 11 09:20:11 2026 GMT
 Not After : Aug 11 20:59:59 2027 GMT
Subject: CN=11.22.33.44, C=FI, ST=FINLAND, L=Paikkakunta, O=Organisaatio Oy, serialNumber=1.2.246.yy.xxxxxx.13.0
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (4096 bit)
 Modulus:
 00:b4:31:9c:e1:a8:34:27:58:3c:0f:ed:fa:8c:f6:
 ...
 dd:83:c9
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Authority Key Identifier:
 01:1C:02:D2:03:4F:04:40:05:81:06:F6:07:C2:08:5A:09:98:10:29
 X509v3 Subject Key Identifier:
 01:47:02:78:03:7E:04:A4:04:A4:06:F3:07:2D:08:94:09:E7:10:62
 X509v3 Key Usage: critical
 Digital Signature
 X509v3 Certificate Policies:
 Policy: 0.4.0.2042.1.7
 Policy: 1.2.246.517.99.10.308.6
 CPS: <http://www.fineid.fi/cps99/>
X509v3 Subject Alternative Name:
DNS:xxx.yyy.fi, IP Address:11.22.33.44
 X509v3 Basic Constraints: critical
 CA:FALSE
 X509v3 CRL Distribution Points:
 Full Name:
 URI:<http://proxy.fineid.fi/crl/dvvtshsp3rc.crl>

X509v3 Extended Key Usage:
TLS Web Client Authentication
 Authority Information Access:
 CA Issuers - URI:<http://proxy.fineid.fi/ca/dvvtshsp3rc.crt>
 OCSP - URI:<http://ocsptest.fineid.fi/dvvtshsp3rc>
 Signature Algorithm: sha512WithRSAEncryption
 Signature Value:
 a7:86:91:f8:57:bf:e3:2e:7d:52:6b:96:6d:be:d2:f6:04:cb:
 ...
 4f:20:59:3b:41:d1:0e:5d

Vanhojen ja uusien SOTE-varmenteiden käyttö



- Lyhyt Q/A uusien varmenteiden osalta
 - **Mitä tapahtuu nykyisille käytössä oleville varmenteille?**
 - Ennen 1.10.2026 myönnetyt vanhanmalliset (samassa varmenteessa Client auth ja Server auth) varmenteet ovat käytössä niiden voimassaoloajan.
 - **Miten menetellään kun varmenne uusitaan ennen 1.10.2026?**
 - Varmenteet voidaan uusia ennen 1.10.2026 vanhanmallisena SOTE-palvelinvarmenteena (Client auth ja server auth).
 - Näitä varmenteita on mahdollista hakea DVV:ltä 30.9.2026 saakka ja niiden voimassaolo voidaan ajoittaa alkamaan 1.10.-30.11.2026 välillä.
 - Varmenteet voidaan uusia uutena SOTE-asiakasvarmenteena, joka voidaan ottaa myös käyttöön jo ennen 1.10.2026.
 - Ennen käyttöönottoa suositellaan testausta uusien SOTE-asiakastestivarmenteiden kanssa AT-ympäristössä.
 - **Miten menetellään kun varmenne uusitaan 1.10.2026 jälkeen?**
 - Kanta-liitynnöissä käytetyt varmenteet uusitaan uusina SOTE-asiakasvarmenteina (Client auth).
 - Käyttötapauksesta riippuen osa varmenteista voi olla tarve uusia uusina SOTE-palvelinvarmenteina. Palvelinvarmennetta ei kuitenkaan käytetä otettaessa yhteyksiä Kanta-palveluihin.
 - Varmenteiden uusiminen voidaan toteuttaa ACME-clientilla tai manuaalisen tilausprosessin kautta.
 - SOTE-asiakasvarmenteiden osalta ACME-käyttöönottovalmius ilmoitetaan erikseen.
 - **Miten menetellään, kun käytössä ACME-client ja sillä haetaan varmenteita DVV:ltä?**
 - ACME-clientin käyttöönotto pakottaa käyttöön uudet varmennemääritykset. Varmenteita voidaan hakea DVV:ltä ACME-clientilla tai manuaalisella palvelupyynnöllä DVV:ltä.
 - Kanta-palveluiden näkökulmasta ACME/manuaalitilaamisella tuotetut varmenteet eivät eroa toisistaan.
 - **Mitä varmenteita käytetään Kanta-palveluiden päässä 1.10.2026 jälkeen?**
 - Kanta-palvelut uusivat nykyiset varmenteet pääsääntöisesti uuden mallisiksi SOTE-palvelinvarmenteiksi (Server auth) vanhojen varmenteiden voimassaolojen päättyttyä.

ECC-varmenteiden käyttö RSA-varmenteiden rinnalla allekirjoituksissa



- Kevään 2026 aikana tehtiin Testaimessa omatoimitestit tehtiin kevään/alkuksesän 2026 aikana
 - Testeissä
 - 19 Potilastietojärjestelmää
 - 15 Lääkemääräys- ja Apteekkijärjestelmää
 - 4 Sosiaalihuollon asiakastietojärjestelmää
 - Testien perusteella EC-varmenteiden käyttö on mahdollista asiakirjojen allekirjoituksissa
 - ECC-algoritmi hyväksytään Kanta käyttöön 1.10.2026 tietoliikenneyhteyksissä ja allekirjoituksissa.



Jatkuvasti kehittyvä Kanta

Lari Kannisto, IT-arkkitehti, Kanta-palvelut

kanta.fi

