Varmennepalvelut / Kuusela Minna (DVV)

3.3.2026

Muutokset DVV:n palve-luvarmenteisiin 2026

Tulossa olevat muutokset

3.3.2026

Varmennepalvelut / Kuusela Minna (DVV) 3.3.2026

Sisällysluettelo

Varmennepalvelut / Kuusela Minna (DVV) 3.3.2026

Vuoden 2026 muutoksia palveluvarmenteisiin

Palveluvarmenteisiin on tulossa useita merkittäviä muutoksia vuonna 2026, joista osa vaatii toimenpiteitä asiakkailtamme. Suosittelemme että asiakkaamme tutustuvat muutoksiin hyvissä ajoin, ja testaavat muutosten vaikutusta omissa ympäristöissään tilaamalla sitä varten testipalvelinvarmenteita.

1 Muutoksia palvelinvarmenteisiin 2026

Vuosi 2026 tuo mukanaan useita muutoksia palveluvarmenteisiin.

Kaikki seuraavaksi listatut muutokset toteutetaan palvelinvarmenne tuotannosta 2026 aikana. ACME:ssa kaikki muutokset on toteutettu heti käyttöönotosta lähtien:

- CN-kenttä poistuu ja sen korvaa SubjectAltName (SAN=DNS) kenttä.
- Palvelinvarmenteissa ei saa jatkossa enää olla sekä Client Authentication että Server Authentication EKU:ja. Vuoden 2026 aikana, DVV eriyttää nykyiset palvelinvarmenteet kahdeksi tuotteeksi: palvelinvarmenne (Server Auth) ja asiakasvarmenne (Client Auth).
- SerialNumber-kentän (OID 2.5.4.5) korvaa OrganizationIdentifier-kenttä (OID 2.5.4.97).
- Basic Constraints CA: False -extensio poistuu käytöstä.
- Varmenteen Varmennekäytäntö-kentän huomautusteksti (User Notice Explicit Text) poistuu käytöstä: Huomautusteksti= Varmennepolitiikka on saatavilla - Certifikatpolicy finns - Certificate policy is available http://www.fineid.fi/cps52.
- Sulkulistatiedostoon on lisätty Expired Certs On CRL-extensio: tuotantoon 15.1.2026, testipuolella toteutus oli marraskuussa 2025. Yhteensopivuusongelmia tämä tuottanee asiakkaille vain, jos asiakkaalla on käytössä erittäin räätälöity CRL-toteutus.

Palvelinvarmenteiden voimassaoloaika lyhenee:

- 15.3.2026 alkaen maksimi voimassaoloaika on 6 kk
- 15.3.2027 alkaen maksimi voimassaoloaika on 3 kk
- 15.3.2029 lähtien palvelinvarmenteet saavat olla voimassa enää 47 päivää.

➔ Suosittelemme asiakkaillemme ACME:en siirtymistä. DVV lanseeraa ACME:n arviolta maaliskuussa 2026.

Osa asiakkaistamme voi mahdollisesti siirtyä käyttämään järjestelmäallekirjoitusvarmenteita joiden voimassaoloaikana säilyy 24 kk tai asiakasvarmenteita joiden voimassaoloaika on 12 kk.

Tässä vielä kootusti muutokset palveluvarmennetuotteittain:

Palvelinvarmenteet (palvelinvarmenne, sote palvelinvarmenne, hyvinvointisovellusvarmenne, KaPa autentikointivarmenne): voimassaoloaika lyhenee, Client Auth poistuu käytöstä. Basic constraints CA: False poistuu käytöstä. Myös CN-kenttä poistuu ja SerialNumber-kentän korvaa OrganizationIdentifier-kenttä. Asiakas voi siirtyä ACMEn käyttäjäksi.

Järjestelmäallekirjoitusvarmenne, (VTJ-rajapinnan) asiakasvarmenne: voimassaoloaika säilyy ennallaan, ei muutoksia. Asiakas voi siirtyä ACMEn käyttäjäksi mikäli varmenne sisältää domainnimen.

KaPa varmenteet: palveluväylää käyttäville asiakkaille on luvassa merkittäviä muutoksia. Siitä tulee erikseen tarkempia ohjeita.

Sähköpostivarmenne: ei muutoksia.

2 Uusia tuotteita ja muutoksia olemassa oleviin tuotteisiin

Tulossa 1.3.2026 alkaen:

Asiakasvarmenne. Asiakasvarmenne korvaa VTJrajapinnan asiakasvarmenteen joka aikaisemmin oli tarkoitettu vain VTJ-käyttöön. Uusi asiakasvarmenne on tarjolla kaikille asiakkaillemme. Mikäli tarvitset Client Authentication-varmenteen jo nyt, voit tilata VTJrajapinnan asiakasvarmenteen. Varmenteen tekniset speksit ovat yhteneväiset.

Arviolta toukokuussa 2026 DVV lanseeraa ACME:n. Tutustu aiheeseen täältä: dvv.fi/acme.

3 Näin tilaat testivarmenteen

Mikäli on pieninkään epäilys, että tulossa olevat muutokset vaikuttavat teidän toimintaympäristöönne ja teillä on käytössä DVV:n palvelinvarmenteita (palvelinvarmenne, KaPa autentikointivarmenne, hyvinvointisovellusvarmenne), suosittelemme että tilaatte testipalvelinvarmenteita missä tulevat muutokset on jo sisällytettynä.

Tee tilaus muuten kuten ennenkin, mutta varmennepyynnön OU-kenttään laitetaan teksti "Uusi 2026 varmenneprofiili”. Näin erotamme täällä DVV:ssä nämä testivarmenteet muista testivarmenteista tilausvaiheessa. Itse tuotettuun testipalvelinvarmenteeseen ei tule OU kenttää.

Huomaa että myös seuraavat Key Usage muutokset on toteutettu näissä testipalvelinvarmenteissa. Näiden muutosten osalta lopullisia päätöksiä ja aikatauluja ei ole lyöty lukkoon tuotantopuolella, joten niitä ei löydy varsinaisesta muutoslistauksesta vielä. Kyseiset KU:t on kuitenkin jo poistettu testipalvelinvarmenteesta: RSA-varmenteissa Key Encipherment ja Data Encipherment, ECC-varmenteissa Key Agreement.

4 Kvanttitietokoneaikaan varautuminen

- Termit **PQC** ja **PQ Cryptography** (*Post-Quantum Cryptography*) sekä **QSC** (*Quantum-Safe Cryptography*) viittaavat kvanttiturvallisiin eli kvanttitietokoneen kestäviin kryptografisiin algoritmeihin eli salausmenetelmiin.
- Julkisen avaimen salausjärjestelmissä nykyisin erittäin laajasti käytetyt algoritmit RSA ja ECC (ECDH/ECDSA) ovat matemaattiselta perustaltaan sellaisia, että riittävän kehittynyt kvanttitietokone voisi murtaa ne lyhyessä ajassa käyttäen *Shorin algoritmia*.

Aikatauluvaatimukset:

EU-komissio: “*The protection of critical infrastructures should be transitioned to PQC as soon as possible, no later than by the end of 2030*.”

Traficom: “*Kansallinen kryptotyöryhmä suosittelee, että kansallinen PQC-siirtymä toteutetaan EU:n esittämien aikataulujen mukaisesti:*

- *Korkean riskin järjestelmät tulisi saattaa kvanttiturvallisiksi vuoteen 2030 mennessä.*
- *Kaikkien julkisen avaimen menetelmien tulisi olla kvanttiturvallisia vuoteen 2035 mennessä*.”

Check list minkä läpikäyntiä suosittelemme kaikille asiakkaillemme:

1. Varmistakaa, että organisaatiollanne on *tietoisuus* tulevasta PQC-siirtymästä.
2. Muodostakaa *kryptoinventaario*: kirjatkaa ylös mitä kryptografisia algoritmeja organisaatiossanne on käytössä ja mihin toimintoihin niitä käytetään.
    1. Koneelliset TLS- ja SFTP-rajapinnat eri tietojärjestelmien tai sidosryhmien suuntiin.
    2. Web-palvelimet (HTTPS/TLS) loppukäyttäjän suuntaan.
    3. Allekirjoitetut/todennetut viestirajapinnat, esim. SAML tai OIDC.

4. Allekirjoitetut tokenit, esim. JWT.
5. Varmennekorttikirjautuminen (mTLS).
6. Sähköiset allekirjoitukset.
7. Tietokantojen, varmuuskopioiden ym. datavarantojen salaus.

3. Pyrkikää kehitystyössä edistämään ***kryptoketteryyttä***.

> ”Kyky mukauttaa kryptografisia järjestelmiä nopeasti uusien uhkien tai standardien mukaan.” –VTT