Certificate services / Kuusela Minna (DVV)

26.1.2026

Changes to DVV service certificates 2026

Upcoming changes

26.1.2026

Certificate services / Kuusela Minna (DVV)
26.1.2026

Table of contents

Certificate services / Kuusela Minna (DVV)

26.1.2026

Changes to DVV service certificates 2026

Several significant changes are coming to service certificates in 2026, some of which will require action from our customers. We recommend that our customers familiarize themselves with the changes well in advance and test the impact of the changes in their own environments by ordering test servercertificates for that purpose.

1 Changes to DVV server certificates 2026

The year 2026 will bring several changes to server certificates.

All the changes listed below will be implemented in the server certificate production in 2026. In ACME, all changes have been implemented right from the start:

- The CN field is removed and replaced by the SubjectAltName (SAN=DNS) field.
- In the future, server certificates may no longer contain both Client Authentication and Server Authentication EKUs. During 2026, DVV will differentiate the current server certificates into two products: server certificate (Server Auth) and client certificate (Client Auth).
- The SerialNumber (OID 2.5.4.5) field is replaced by the OrganizationIdentifier field (OID 2.5.4.97).
- Basic Constraints CA: False extension is disabled..
- The notice text (User Notice Explicit Text) of the certificate's Certificate policy field is disabled: Notice text= Certifikatpolitika is available - Certifikatpoli-cy finns - Certificate policy is available http://www.fineid.fi/cps52.
- Expired Certs On CRL extension is added to the blocklist file: for production on 14.1.2026, on the test side this has already been implemented. This will only cause compatibility problems for customers if the customer uses a highly customized CRL implementation.

The validity period of server certificates is reduced:

♣ From 15.3.2026, the maximum validity period is 6 months
♣ From 15.3.2027, the maximum validity period is 3 months
♣ From March 15, 2029, server certificates may only be valid for 47 days.

We recommend to our customers to switch to ACME. DVV will launch ACME on estimate in March 2026.

Some of our customers may switch to using system signature certificates, whose validity period remains 24 months.

Below are listed to changes in 2026 by product:

Server certificates (server certificate, health care server certificate, service certificates for wellbeing applications, KaPa authentication certificate): the validity period is shortened, -Client Auth is deactivated. Basic constraints CA: false disables. The CN field is also removed and the SerialNumber field is replaced by the OrganizationIdentifier field. The customer can switch to ACME.

System signature certificate, client certificate: validity period remains unchanged, no changes. The customer can become an ACME user if the certificate contains a domain name.

KaPa certificates: significant changes are in store for customers. There will be more detailed instructions separately.

Email certificate: no changes.

2 New products and changes to existing products

Upcoming 1st of March 2026:

Client certificate. The client certificate replaces the VTJ interface client certificate, which was previously intended for VTJ use only. The new client certificate is available to all our clients. If you need a Client Auth certificate already, you can order the VTJ interface client certificate. The technical specifications of the certificates are the same.

DVV is estimated to launch the ACME protocol in March 2026. Learn more about the topic here: dvv.fi/en/acme-en.

3 This is how the can order a test server certificate

If there is even the slightest doubt that the upcoming changes will affect your operating environment and you are using DVV server certificates, we recommend that you order test server certificates that already include the upcoming changes.

Make the order otherwise as before, but the text "New 2026 certificate profile" is added to the OU field of the certificate request (CSR). This is how we distinguish these test certificates from other test certificates here at the Digital and Population Data Services Agency at the ordering stage. The produced test server certificate will not have an OU field included.

Please note that the following Key Usage changes have also been implemented in these test server certificates. Regarding these changes, final decisions and schedules have not yet been fixed for production, so they are not yet included in the official change list. However, the said KUs have already been removed from the test server certificates: Key

Encipherment and Data Encipherment for RSA certificates, and Key Agreement for ECC certificates.

4 Getting ready for Quantum Computers

- The terms PQC and PQ Cryptography (Post-Quantum Cryptography) and QSC (Quan-tum-Safe Cryptography) refer to quantum-safe, i.e. quantum computer-resistant cryptographic algorithms, i.e. encryption methods.
- The algorithms RSA and ECC (ECDH/ECDSA), which are currently very widely used in public key encryption systems, have a mathematical basis such that a sufficiently developed quantum computer could break them in a short time using Shor's algorithm.

Time table requirements:

EU Commission: "The protection of critical infrastructures should be transitioned to PQC as soon as possible, no later than by the end of 2030."

Traficom: "The national crypto working group recommends that the national PQC transition be carried out in accordance with the timetables presented by the EU:

• High-risk systems should be made quantum secure by 2030.

• All public key methods should be quantum secure by 2035.”

Check list which we recommend to all our customers to go through:

1. Make sure your organization is aware of the upcoming PQC transition.

2. Create a crypto inventory: write down which cryptographic algorithms are in use in your organization and for which functions they are used.

    1. Mechanical TLS and SFTP interfaces to different information systems or stakeholders.

    2. Web servers (HTTPS/TLS) towards the end user.
    3. Signed/authenticated message interfaces, e.g. SAML or OIDC.
    4. Signed tokens, eg JWT.
    5. Certificate card login (mTLS).
    6. Electronic signatures.
    7. Encryption of databases, backups, etc. data reserves.

3. Strive to promote crypto-agility in development work.

“The ability to adapt cryptographic systems quickly

according to new threats or standards.” –VTT