rydoo

Finnish Tax Administration (Vero) – Certificate Service

Certificate Creation Guide

Finnish Tax Administration (Vero) – Certificate Service

This guide explains how to create a certificate for using the Finnish Tax Administration's APIs.

Prerequisites

Before you start, ensure that:

- You have access to a macOS / Linux / Windows machine with OpenSSL installed.
- You can log in to the Vero Certificate Service e-service using:
    - online banking credentials, mobile certificate, or certificate card.

Authorizations for Production Certificates

The person managing certificates in the Vero Certificate Service must have the appropriate Suomi.fi mandate granted by the organization.

Without proper authorization:

- Production certificates cannot be requested
- Certificates cannot be renewed
- Certificates cannot be revoked

You can request authorizations through the Suomi.fi e-Authorizations service. For detailed guidance, refer to the instructions on granting mandates as an organization.

Step 1: Generate a Private Key

Open a terminal and generate a new RSA private key.

```
openssl genrsa -out private.key 3072
```

Important

- This file contains your private key, store it securely, do not share it.
- If the private key is lost, a new certificate must be issued.

- Three key sizes are supported: 2048, 3072, and 4096 bits. Large key sizes increase security but also increases certificate size.

Step 2: Create a Certificate Signing Request (CSR)

Create a CSR using the private key generated earlier:

```
openssl req -new -key private.key -out example.csr
```

- Replace the text "example.csr" with the desired file name and path where the CSR will be written.
- The CSR will be generated using the private key you created earlier.
  - OpenSSL will ask for various additional details when creating the CSR, such as country (C), common name (CN), and organization (O). For production certificates, enter the organization's actual business ID and name. Enter FI in the country field. For test certificates, enter a dummy organization business ID in the common name field and dummy organization name in the organization field.
- Optional fields
  - When prompted for:
    - Challenge password
    - Optional company name

    Leave these empty and press Enter.

Step 3: Request the Certificate in Vero e-Service

- For **Test Certificate**: Submit testing start notification:
  - Before requesting a test certificate, your organization must submit a testing start notification through the portal. This specifies the technical contact person who will retrieve the certificate.
- For **Production Certificate**: Ensure Authorizations Suomi.fi:
  - Verify if you have the necessary Suomi.fi mandates to act on behalf of your organization. If you are a person with signing rights, you may not need separate authorization.
- Log in to the Finnish Tax Administration Certificate Service:
  - Access the Testing certificates section or Production certificates section using personal identification (online banking codes, mobile certificate, or certificate card).
- Submit API Application (Follow the same process for test and production
- certificate from this step):
  - You can only request API access rights after submitting test start notification for a test certificate, and you need the artificial identifier received from the Incomes Register for the application.

- Select Request a New Certificate
- Upload or paste the CSR (example.csr)
- Assign a technical contact person

After submission:

- The technical contact will receive:
    - Transfer ID
    - One-time password (valid for 14 days)

Step 4: Retrieve the Certificate

The certificate can be retrieved either:

- via the e-service, or
- via the PKI API

The retrieved certificate is provided in Base64 format.

Save it as a PEM file (certificate.pem), for example:

```
-----BEGIN CERTIFICATE-----
(Base64 certificate content)
-----END CERTIFICATE-----
```

Step 5: Share the Certificate and Private Key

Share the certificate.pem file as well as the private key with your technical Rydoo contact person.

Renewal of certificate

Production and testing certificates are valid for **two years**, after which they must be renewed.

- Renewing a certificate basically means the same thing as ordering a new certificate technically via the PKI web service interface. Renewal can be done up to **60 days before the expiry** of the current certificate. Once expired, the certificate cannot be renewed, and a new certificate must be ordered from the Certificate Service.
- Before renewing a certificate, a new private key is generated to create a new CSR. The original private key used for the existing certificate can no longer be used to create a new CSR.

- The renewal message sent to the PKI web service interface is signed with the original private key of the valid certificate. The signature serves as a strong authentication of the requestor for the certificate renewal.

Requirements

- Valid current certificate and its private key (PFX + password)
- Knowledge of PKI and XML signing
- Access to the Certificate Service PKI interface (WSDL/API)
- Organisation details: Business ID and organisation name
- Tool for sending signed XML requests (e.g., SoapUI, curl, or custom integration code)

1. Generate a New Key Pair

Create a new private key for the certificate signing request (CSR) using a PKI tool like OpenSSL. The private key must be new; you cannot reuse the old one.

2. Create a Renewal Certificate Signing Request (CSR)

Using the new private key, generate a CSR. Include your organisation details (e.g., country, business ID) according to the certificate you are renewing.

3. Build the Renewal XML Message

Create an XML renewal request containing:

- Your environment (test or production)
- Your Business ID and organisation name
- The base64-encoded CSR (without header/footer)

4. Sign the Renewal XML

Sign the XML message using the *current (soon-to-expire) certificate's private key.* This signature proves authentication for the renewal request. You can use an XML signing tool or the example provided by the Tax Administration.

5. Send the Signed Renewal Request

Submit the signed XML to the Certificate Service's PKI API (e.g., using tools like SoapUI or curl). Ensure the signed content remains unchanged.

6. Retrieve the Renewed Certificate

Once the renewal request is accepted, use the certificate retrieval API to fetch the renewed certificate and install it in your environment.

More details and source code example for signing the XML can be found here.

Revoking the certificate:

For revoking production certificates, the organisation must also grant a Suomi.fi authorisation to the organisation's representative that manages its certificates. The authorised representative can revoke the certificate in the e-service.

When to Revoke

Revoke a certificate if:

- The private key is misplaced, disclosed, or at risk.
- The certificate is no longer needed (e.g., replaced or organisation no longer uses it).
- Your organisation has ceased operations.

How to Revoke in the e-Service

1. Log in to the certificate service (production or testing). Identify yourself (online banking codes, mobile certificate, or certificate card).
2. Select the certificate you want to revoke and open its details.
3. Click Revoke certificate.
4. Choose:
    a. Temporary prohibition (can be restored), or
    b. Permanent revocation (cannot be restored).
5. For permanent revocation, select a reason (e.g., private key risk, replaced certificate, no longer used).
6. Send the request – the certificate will be revoked and no longer usable in API services.

Urgent situations

You can call the on-call service number if certificates must be revoked immediately and certificates are at risk.

On-call service number: +358 9427 34834

The on-call service number only processes urgent cases in which certificates are at risk.

References

1. Finnish Tax Administration (Vero). Certificate Service for IT Developers. March 20, 2026. www.vero.fi

2. Finnish Digital and Population Data Services Agency (DVV). Granting mandates as an organisation. March 20, 2026. www.suomi.fi/instructions-and-support

3. Finnish Digital and Population Data Services Agency (DVV). Suomi.fi e-Authorizations. March 20, 2026. www.suomi.fi/e-authorizations

4. Finnish Tax Administration (Vero). Incomes Register: Electronic services for companies and organisations. March 20, 2026. www.vero.fi/en/incomes-register