

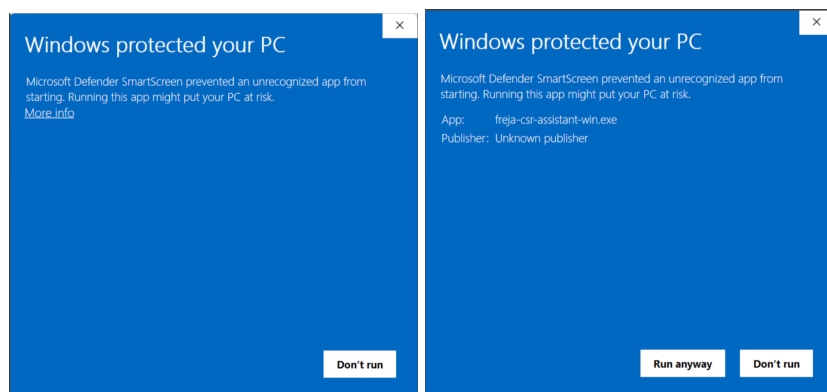
Freja CSR assistant tool

This guide walks you through the Freja CSR assistant tool. It is used to make it easier to obtain the certificates and keystore needed to access Freja's production environment.

Starting the tool

The tool comes as a simple executable file named `freja-csr-assistant-win.exe`. Double-click it to run the tool.

Because the executable is unsigned, Windows may show a security warning like in the image below. If this happens, click **Yes** (or **More info** and then **Run anyway**) to continue.



Accept the Freja eID Terms shown on the first screen and you are ready to go.

Generating CSR

When the tool starts, the **Generate CSR** screen is opened by default.

INFO

A CSR means Certificate Signing Request. It contains information about your company and your public key. Freja uses it to create and sign your client certificate.

Once you receive your client certificate, you will be able to access Freja services in production protected with mutual TLS (mTLS).

Fill in the form in two parts.

Certificate request details

In this section you enter the company details that will be included in the certificate request.

- **Common Name (CN)**

This field is optional. You can use a descriptive name for your integration.

Example: `Freja eID Production API`

- **Organisational Unit (OU)**

This field is optional. You can use it to describe the team or environment.

Example: `IT Department`

- **Organisation Name (O)**

Enter your legal company name.

Example: **Acme komun**

- **Organisation Identifier**

Enter your company registration number or organisation number in the format requested by Freja.

Example: **212000-0142**

- **Country (C)**

Enter the two-letter country code in uppercase.

Example: **SE**

- **Key Size**

Leave the default value unless you have a specific need for shorter key size.

Recommended value: **4096 bits**

Key protection and output

In this section you choose the password for the private key and where the generated files will be saved.

- **Password-protect private key**

This option is enabled by default and we strongly recommend leaving it enabled.

- **Password**

Enter the password that will protect the private key file.

Example: **AcmeKomun2026!**

- **Confirm Password**

Enter the same password again.

- **Output Folder**

Select the folder where the generated files will be saved. By default, the files are saved in the user's Documents folder.

Example: **C:\Users\john.doe\Documents\AcmeKomun**

- **File Name Prefix**

Enter the base file name to use for the generated files. By default, it is created from the organisation name entered earlier.

Example: **acme-komun**

If you use the example above, the tool will create:

- **acme-komun.key**
- **acme-komun.csr**

When all fields are filled in, click **Generate Key and CSR**.

If everything is correct, the tool shows a success message and a box with information about the generated files.

You will find the files in the output folder you selected:

- the CSR file, for example `acme-komun.csr`
- the private key file, for example `acme-komun.key`

The screenshot shows the 'Freja eID CSR Assistant' web application. It has a teal header with the title and window controls. Below the header are two tabs: 'Generate CSR' (active) and 'Create keystore'. The main content area is divided into three sections:

- Freja eID CSR Assistant**: A blue banner with the text: 'Generate a Freja-compatible RSA private key and CSR without requiring OpenSSL or any other software installed on the your machine. Designed around Freja certificate specifications for a faster onboarding flow.'
- Certificate Request Details**: A form with the following fields:
 - Common Name (CN):
 - Organisational Unit (OU):
 - Organisation Name (O) *:
 - Organisation Identifier *:
 - Country (C) *:
 - Key Size:
 A note below the fields says: '* Mandatory fields — hover a label for examples'
- Key Protection and Output**: A form with the following fields:
 - ☒ Password-protect private key Enabled by default
 - Password:
 - Confirm Password:
 - Output Folder:
 - File Name Prefix: Files saved as <prefix>.key and <prefix>.csr
 At the bottom of this section are two buttons: 'Generate Key and CSR' and 'Reset Form'.
- Validation rules**: A list of rules:
 1. O, organisationIdentifier (OID 2.5.4.97), and C are mandatory.
 2. C must be exactly two uppercase letters.
 3. O and OU cannot contain: < > ~ ! @ # \$ % ^ * / \ () ? , . & — CN is optional and unrestricted.
 4. Defaults to 4096-bit RSA; 2048 and 3072 also accepted.
 5. Private key is AES-256 encrypted when a password is supplied (min. 8 chars).

Send the CSR to Freja's partner support

After the CSR file has been generated, send it to Freja partner support at partnersupport@frejaeid.com.

Attach the `.csr` file to the email. In the example above, this is the file `acme-komun.csr`.

Freja will reply by email when your production setup is ready. The reply will contain:

- one signed certificate for your company
- two CA certificates: root CA and intermediate certificate

The email body will look similar to this:

Hello Acme komun,

We have now setup you in PRODUCTION.

Here is your signed certificate:

-----BEGIN CERTIFICATE-----

cert content.

-----END CERTIFICATE-----

Here is Root CA and intermediate certificate:

-----BEGIN CERTIFICATE-----

cert content.

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

cert content.

-----END CERTIFICATE-----

Generate keystore file

Start **freja-csr-assistant-win.exe** again then click the **Create keystore** in the top menu of the tool.

Fill in the fields as follows:

- **Private Key File**

Select the private key file that was generated in the first step.

Example: **C:\Users\john.doe\Documents\AcmeKomun\acme-komun.key**

- **Private Key Password**

Enter the same password that you used when the private key was generated.

Example: **AcmeKomun2026!**

- **Signed Certificate**

Copy only the signed certificate from Freja's email and paste it into this box.

This is the part starting with -----BEGIN CERTIFICATE----- under the text **Here is your signed certificate:** and ending with -----END CERTIFICATE-----.

- **Root CA and Intermediate Certificate**

Copy the two CA certificates from Freja's email and paste them into this box.

This is the part under the text **Here is Root CA and intermediate certificate:.**

Paste both certificates into the same box, one after another.

When all fields are filled in, click **Create keystore**.

If everything is correct, the tool shows the message **Keystore created successfully** and an info box named **Created Keystore**.

Freja CSR Assistant

Generate CSR Create keystore

Create PKCS#12 Keystore

Generates keystore in PKCS#12 format by combining the private key you generated earlier, and certificates you received from Freja's partner support.

Private Key and Certificate Chain

Private Key File * C:\Users\vebrpav\Documents\wd.key Browse...

Private Key Password *

Signed Certificate *

```
-----BEGIN CERTIFICATE-----L
//lines skipped for brevity
-----END CERTIFICATE-----
```

Root CA and Intermediate Certificate *

```
-----BEGIN CERTIFICATE-----
//lines skipped for brevity
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
//lines skipped for brevity
-----END CERTIFICATE-----
```

* Mandatory fields — hover a label for examples

Create keystore

Validation rules

1. The signed certificate field must contain exactly 1 PEM certificate.
2. The signed certificate must match the selected private key.
3. The root CA and intermediate certificate field must contain exactly 2 PEM certificates.
4. The .pfx file is saved next to the private key using the same password.
5. If the target file name already exists, the app adds -2, -3, and so on.

The info box shows the full path to the generated keystore file.

The keystore file is saved in the same folder as the private key file. If your private key file is named **acme-komun.key**, the generated keystore file will normally be named **acme-komun-keystore.pfx**.

The keystore is now ready to use. The **.pfx** file itself is protected with the same password as the private key. The private key entry inside the keystore is protected with the same password as well.

Partner support

If you need help, you can contact our technical support at partnersupport@frejaeid.com.