Creating a DFN server certificate

There are two ways to create a DFN server certificate:

Option 1: Create your own private key (recommended)

If you want to generate your own private key, follow these steps:

Step 1: First, generate a private key, a public key, and a CSR (Certificate Signing Request) file locally. For detailed instructions, see here.

Step 2: Next, upload the CSR file via the DFN-Website. To do this, select the option **“Submit your own CSR file (PKCS#10)**”.

Step 3: Enter your information and set a lock PIN. Be sure to select the correct certificate profile at the top.

Step 4: Continue to Step 5.

Option 2: Key generation by the DFN

If you trust the DFN, you can let your browser generate the private and public keys. The keys will never leave your computer.

Step 1: On the DFN-Website, select the option **“Server Certificate (including key generation).”**

Step 2: Select the correct certificate profile and use **"EC P-384"** as the key type. If the server has problems with this, you can also use the old **"RSA 4096"** format.

Step 3: Enter your information and set a lock PIN.

Step 4: On the next page, review your information and save the application file (.json). Make sure to remember the password; you'll need both later when you're ready to retrieve your certificate.

Step 5: Save and send the application receipt (**the PDF file**) as a signed email to: **ca-btu@b-tu.de** (A signed email is sufficient; a handwritten signature is not required)

Step 6: The request will be reviewed and approved. Depending on the circumstances, this may take until the next business day, as the process is currently still done manually.

Step 7: You will receive an email from DFN (Subject: DFN Association Community CA Certificate Information). Your certificate is included in the email.

Step 8 – Solution 1: If you requested the certificate using Method 1, you can still download the CA certificates via the second link in the email.

Step 8 - Solution 2: If you requested the certificate using Method 2, click the first link. This will open a webpage where you can download the certificates created in Step 2. You can use the second link to download the CA certificates.