Server certificate

Table of contents:

Support

Please contact us via SmartDesk, e-mail servicedesk@id.ethz.ch or by phone at +41 44 632 77 77

Switch to the page in German language

Service Information and Update

Blog eintrag

Create a CSR (Certificate Signing Request)

Warning!

To obtain a TLS/SSL certificate, a so-called csr file must be created first.

On Windows systems this can be done as follows:

First, an inf file must be created. The following content can be used as a template for this:

```
[NewRequest]

Subject = "CN=DemoServer.ethz.ch,O=ETH Zurich,C=CH"

KeyLength =  2048

KeySpec = 1

Exportable = False

ProviderName = "Microsoft Software Key Storage Provider"

HashAlgorithm = SHA256

MachineKeySet = True

SMIME = False

UseExistingKeySet = False

RequestType = PKCS10

KeyUsage = 0xA0

Silent = True

[Extensions]

2.5.29.17 = "{text}"

_continue_ = "dns=Demo.ethz.ch&"

_continue_ = "dns=AuchDemo.ethz.ch&"
```

Customize server name

Please replace the server names in the above example with your own information.

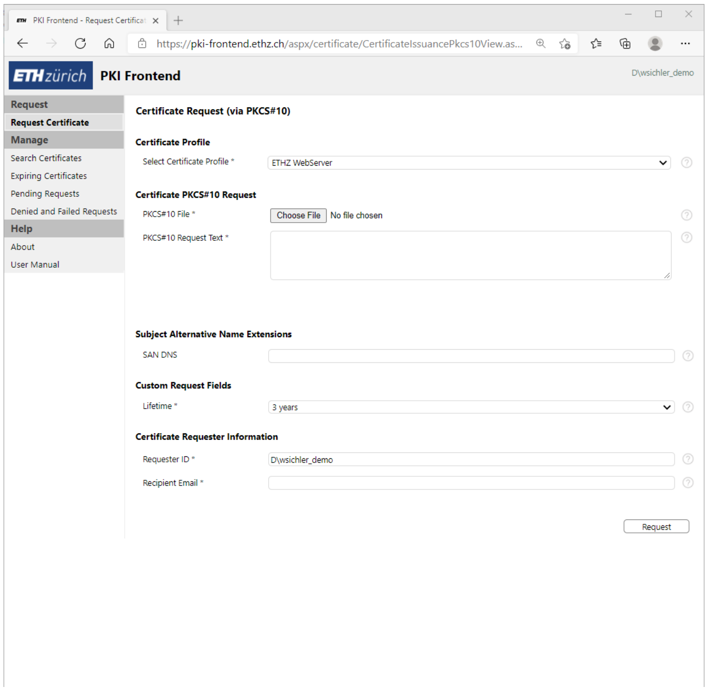
Target server

If the csr file is not created on the system where the certificate is to be used later, the "Exportable" parameter must be set to "True", since it will be necessary to install the certificate first on the Windows system on which the csr file and thus the private key were created.

With "certreq -new Demo.inf Demo.csr" the csr-file is created.

Obtain TLS/SSL certificate

- Log in to https://pki-frontend.ethz.ch
- Press "Request Certificate".



Certificate Request (via PKCS#10)

Certificate Profile

Select Certificate Profile * ETHZ WebServer

Certificate PKCS#10 Request

PKCS#10 File * Choose File No file chosen

PKCS#10 Request Text *

Subject Alternative Name Extensions

SAN DNS

Custom Request Fields

Lifetime * 3 years

Certificate Requester Information

Requester ID * D\wsichler_demo

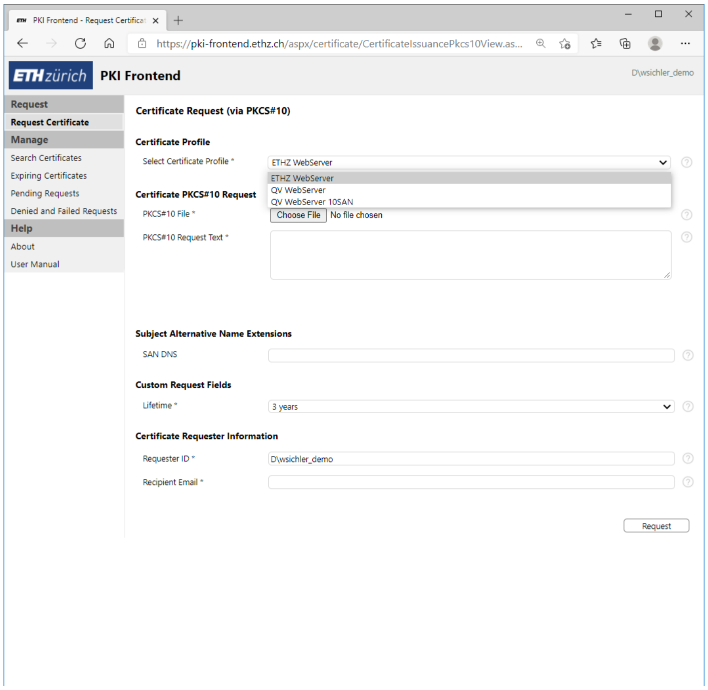
Recipient Email *

Request

There are three profiles to choose from. The names are completed by the support group.

- ETH WebServer:
  internally trusted towards the ETH Root Certification Authority. ETH Root certificate and ETH Issuing certificate must be installed on the systems involved (Download PKI security certificates). No restriction of number of addresses. Can be issued for one, two or three years. Browsers accept only certificates valid for one year, but for web service between two servers longer validity can be used.
- QV WebServer:
  Publicly trusted to the QuoVadis Root Certification Authority. Validity one year. Number of addresses limited to one (if more than one is specified in the CSR, only the first one is used).
- QV WebServer 10SAN:
  Publicly trusted to the QuoVadis Root Certification Authority. Validity one year. Number of addresses limited to ten. Billing distinguishes between certificates with up to three addresses and certificates with four to ten addresses.

Upload the CSR via "Choose File".



Certificate Request (via PKCS#10)

Certificate Profile

Select Certificate Profile * ETHZ WebServer

Certificate PKCS#10 Request

PKCS#10 File * Choose File No file chosen

PKCS#10 Request Text *

Subject Alternative Name Extensions

SAN DNS

Custom Request Fields

Lifetime * 3 years

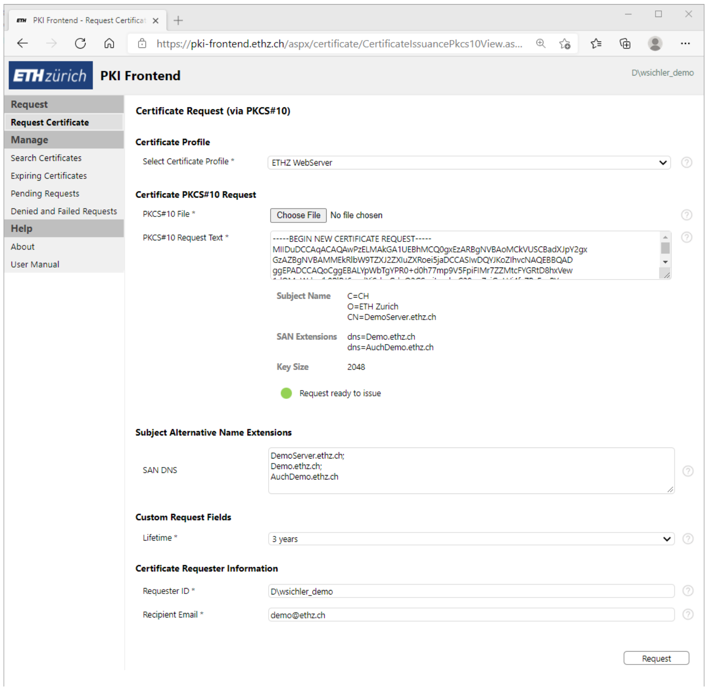
Certificate Requester Information

Requester ID * D\wsichler_demo

Recipient Email *

Request

- Select the validity of the ETH WebServer.
- Insert a valid mail address at "Recipient Email".
- Press the "Request" button.



Certificate Request (via PKCS#10)

Certificate Profile

Select Certificate Profile * ETHZ WebServer

Certificate PKCS#10 Request

PKCS#10 File * No file chosen

PKCS#10 Request Text *

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDuDCCAqACAQAwPzELMAkGA1UEBhMCQ0gxEzARBgNVBAoMCkVUSCBadXJpY2gx
GzAZBgNVBAMMEkRlbW9TZXJ2ZXIuZXRoei5jaDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALYpWbTgYPR0+d0h77mp9V5FpiFIMr7ZZMtcFYGRtD8hxVew
```

Subject Name	C=CH
	O=ETH Zurich
	CN=DemoServer.ethz.ch

SAN Extensions	dns=Demo.ethz.ch
	dns=AuchDemo.ethz.ch

Key Size	2048

● Request ready to issue

Subject Alternative Name Extensions

SAN DNS
DemoServer.ethz.ch;
Demo.ethz.ch;
AuchDemo.ethz.ch

Custom Request Fields

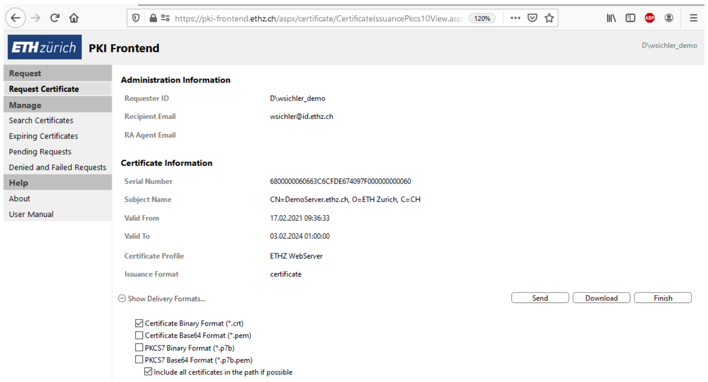
Lifetime * 3 years

Certificate Requester Information

Requester ID * D\wsichler_demo

Recipient Email * demo@ethz.ch

- After a few seconds, the certificate will be ready for download.
- At "Show Delivery Formats ..." the format for downloading can be selected and whether the root and Intermediate certificate is included or not



Administration Information

Requester ID	D\wsichler_demo
Recipient Email	wsichler@id.ethz.ch
RA Agent Email	

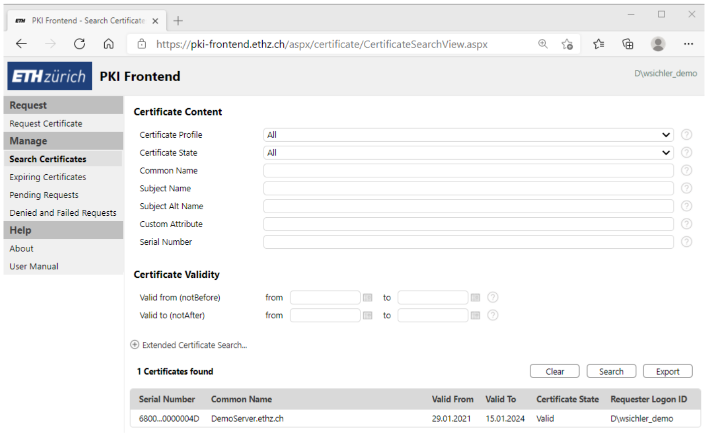
Certificate Information

Serial Number	6800000060663C6CFDE674097F000000000060
Subject Name	CN=DemoServer.ethz.ch, O=ETH Zurich, C=CH
Valid From	17.02.2021 09:36:33
Valid To	03.02.2024 01:00:00
Certificate Profile	ETHZ WebServer
Issuance Format	certificate

⊖ Show Delivery Formats...

☑ Certificate Binary Format (*.crt)
☐ Certificate Base64 Format (*.pem)
☐ PKCS7 Binary Format (*.p7b)
☐ PKCS7 Base64 Format (*.p7b.pem)
☑ Include all certificates in the path if possible

- If the certificate is needed again later, it can be downloaded again at any time.



Certificate Content

Certificate Profile	All
Certificate State	All
Common Name	
Subject Name	
Subject Alt Name	
Custom Attribute	
Serial Number	

Certificate Validity

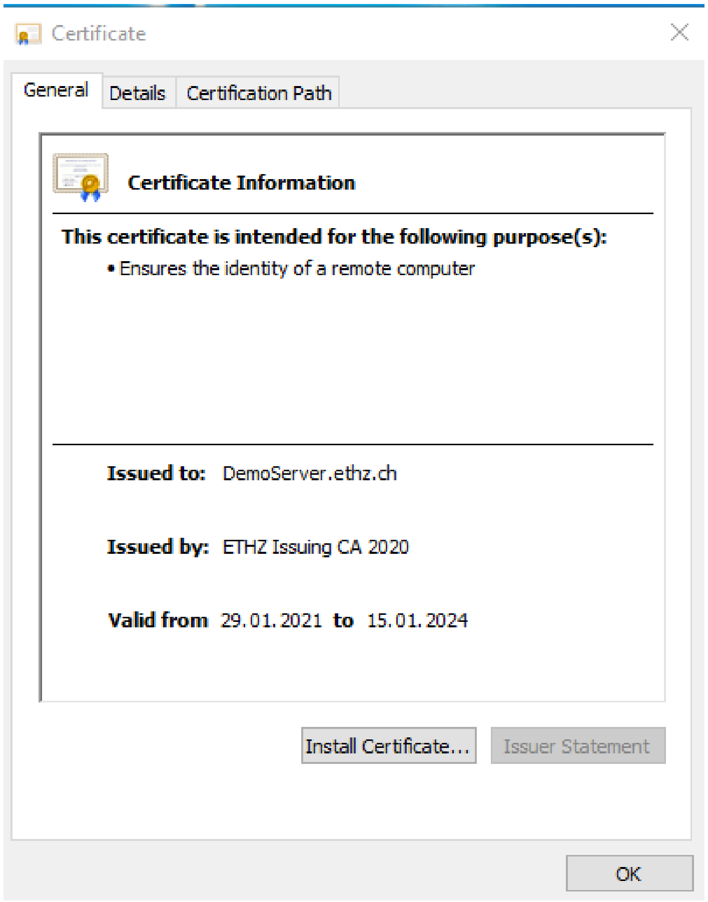
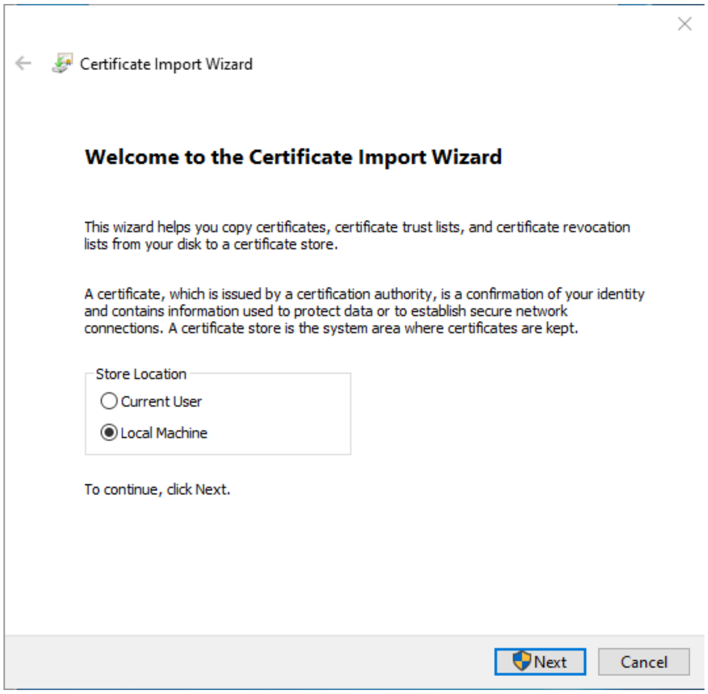
Valid from (notBefore) from to
Valid to (notAfter) from to

⊕ Extended Certificate Search...

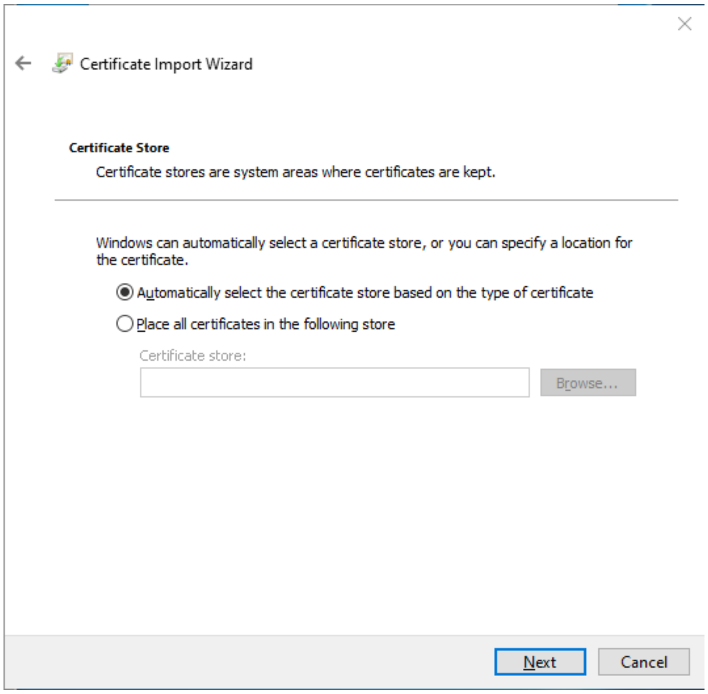
1 Certificates found

Serial Number	Common Name	Valid From	Valid To	Certificate State	Requester Logon ID
6800...0000004D	DemoServer.ethz.ch	29.01.2021	15.01.2024	Valid	D\wsichler_demo

Installation TLS/SSL-Zertifikat

- Open file. - Press Install Certificate.	 Certificate General Details Certification Path **Certificate Information** **This certificate is intended for the following purpose(s):** • Ensures the identity of a remote computer **Issued to:** DemoServer.ethz.ch **Issued by:** ETHZ Issuing CA 2020 **Valid from** 29.01.2021 **to** 15.01.2024 Install Certificate... Issuer Statement OK
- Local Machine. Next. - Possibly user and password of an administrator are requested.	 Certificate Import Wizard **Welcome to the Certificate Import Wizard** This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. Store Location ○ Current User ● Local Machine To continue, click Next.

- Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

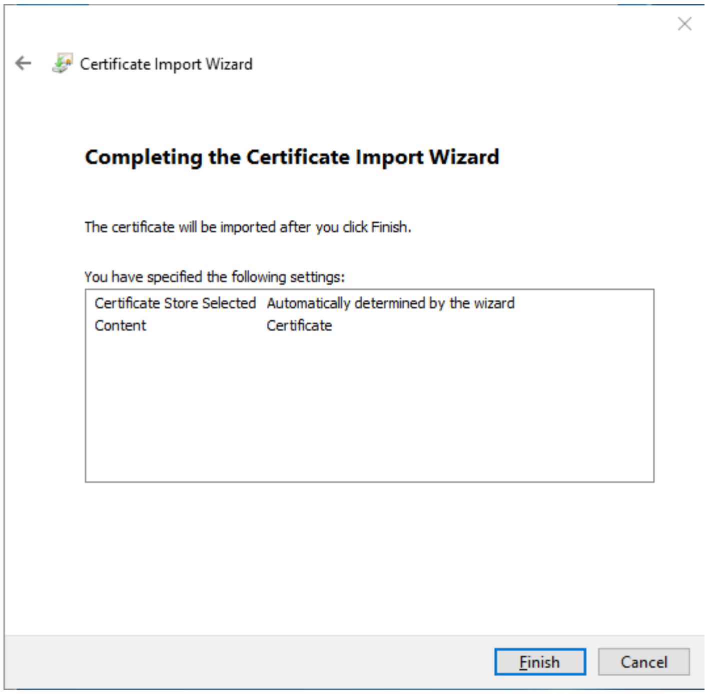
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

- Finish.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

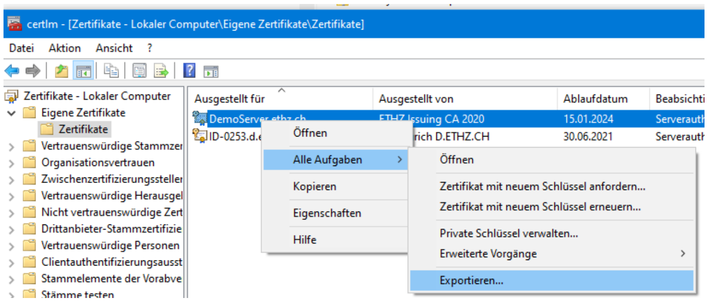
You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

⚠ If the certificate is used on another server, then the certificate including the private key must be exported.

Call the certificate management with certlm.msc.

Export the server certificate with private key.



certlm - [Zertifikate - Lokaler Computer\Eigene Zertifikate\Zertifikate]

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichti
DemoServer.ethz.ch	ETHZ Issuing CA 2020	15.01.2024	Serverauth
ID-0253.d.e	rich D.ETHZ.CH	30.06.2021	Serverauth

Datei
Aktion
Ansicht
?
Zertifikate - Lokaler Computer
Eigene Zertifikate
Zertifikate
Vertrauenswürdige Stammzer
Organisationsvertrauen
Zwischenzertifizierungssteller
Vertrauenswürdige Herausgel
Nicht vertrauenswürdige Zert
Drittanbieter-Stammzertifizie
Vertrauenswürdige Personen
Clientauthentifizierungsausst
Stammelemente der Vorabve
Stämme testen
Öffnen
Alle Aufgaben
Kopieren
Eigenschaften
Hilfe
Öffnen
Zertifikat mit neuem Schlüssel anfordern...
Zertifikat mit neuem Schlüssel erneuern...
Private Schlüssel verwalten...
Erweiterte Vorgänge
Exportieren...