[en] Certificate -SSL Certificate Request - Server certificates via web (with Sectigo PKI)

06.05.2024 17:51:46

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Bewertungen:**	1
Status:	öffentlich (Alle)	**Ergebnis:**	75.00 %
Sprache:	en	**Letzte Aktualisierung:**	13:52:09 - 14.11.2023

Schlüsselwörter

Zertifikat Zertifikatsbeantragung ACME CSR

Lösung (öffentlich)

Sectigo certificate application

1. Link to the application page at Sectigo:
[1]https://cert-manager.com/customer/DFN/idp/ssl/tu-dresden/select

2. Select "Your Institution", search for "TU Dresden" in the search field and select entry à Forward to the IdP of TU-Dresden

3. Registration at the IdP of TU-Dresden

4. Sectigo certificate management overview page

Application

1. Select "Enroll Certificate"

2. Certificate Profile (default): OV-Multi-Domain

3. Certificate Term (default): 1 Year

4. Select Upload CSR and upload generated CSR

5. Common Name and if necessary Subject Alternative Name will be read from the CSR

6. Additional domain names can be entered in the "Subject Alternative Name" field

7. An additional email can be registered as "External Requesters", which should be informed (certificate download)

8. An optional comment can be placed in the "Comments”.

9. Enable Auto Renew - At a specified time period before the certificate expires, a new certificate request will be submitted automatically. As soon as this has been approved by the ServiceDesk, you will receive the new certificate by email as usual

Revoking

1. Select active certificate

2. Press "Revoke" button ► dialog appears

3. Enter reason for blocking and comment

4. Press "Revoke" button ► certificate will be revoked

Note: Only your own certificates can be revoked, other administrators will not be informed. If the person making the request can not be reached, revoking is possible via the ServiceDesk.

Renewal

1. Select active certificate

2. Press the "Renew " button and confirm

3. A new certificate request will be automatically generated and submitted. The initial private key remains valid

Download

1. Select active certificate

2. Press "Download" button

3. A list with various file formats for download is displayed:

- Certificate only, PEM encoded – certificate in PEM format only
- Certificate (/w issuer after), PEM encoded – certificate in PEM format with following issuer certificate(s)
- Certificate (/w chain), PEM encoded - certificate in PEM format, starting with root certificate ► issuer certificate(s) ► certificate
- PKCS#7 – certificate with certificate chain in PKCS#7 Format, binary
- PKCS#7 - PEM encoded - certificate with certificate chain in PKCS#7 format,

- Intermediate(s)/Root only, PEM encoded - intermediate CAs and root CA only
- Root/Intermediate(s), PEM encoded - Root CA and intermediate CAs only

Certificate formats for commonly used servers:
- Apache Server: Certificate(/w issuer after)
- Please note: remove the parameter SSLCertificateChainFile from the configuration. Intermediate CA certificates are already contained in the certificate file.

- NGINX: Certificate (/w issuer after)
- IIS-Server: Certificate (/w issuer after)
- Windows/Java Tomcat: PKCS#7

[1] https://cert-manager.com/customer/DFN/idp/ssl/tu-dresden/select