[de] Zertifikate - Beantragung SSL Zertifikate - Server Zertifikate per Web (mit Sectigo PKI)

08/14/2024 12:45:52

FAQ Article Print

Category:	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	**Votes:**	1
State:	public (all)	**Result:**	100.00 %
Language:	de	**Last update:**	13:50:13 - 11/14/2023

Keywords

Zertifikatsbeantragung ACME CSR

Solution (public)

Zertifikatsbeantragung Sectigo

1. Link zur Beantragungsseite bei Sectigo:
[1]https://cert-manager.com/customer/DFN/idp/ssl/tu-dresden/select

2. „Your Institution“ wählen, im Suchfeld nach „TU Dresden“ suchen und Eintrag auswählen à Weiterleitung zum IdP der TU-Dresden

3. Anmeldung am IdP der TU-Dresden

4. Übersichtsseite Sectigo-Zertifikatsmanagement:

Beantragung

1. „Enroll Certificate“ wählen

2. Certificate Profil (vorgegeben): OV-Multi-Domain

3. Certificate Term (vorgegeben): 1 Year

4. Upload CSR wählen und erzeugten CSR hochladen

5. Common Name und ggf. Subject Alternative Name wird aus dem CSR ausgelesen

6. Zusätzliche Domainnamen können im Feld „Subject Alternative Name“ eingetragen werden

7. Als „External Requesters“ kann eine zusätzliche E-Mail eingetragen werden, welche informiert werden soll (Zertifikatsdownload)

8. Unter „Comments“ kann ein optionaler Kommentar gesetzt werden

9. Aktivierung von „Auto Renew“ – Bei einer festgelegten Zeitspanne bevor das Zertifikat abläuft, wird automatisch ein neuer Zertifikatsantrag eingereicht. Sobald dieser vom ServiceDesk genehmigt wurde, erhalten Sie das neue Zertifikat wie gewohnt per E-Mail

Sperrung

1. Aktives Zertifikat auswählen

2. Button „Revoke“ drücken ► Dialog erscheint

3. Grund der Sperrung und Kommentar eingeben

4. Button „Revoke“ drücken ► Zertifikat wird gesperrt

Hinweis: Es können nur eigene Zertifikate gesperrt werden, andere Administratoren/-innen werden darüber nicht informiert. Sollte die beantragende Person nicht mehr erreichbar sein, ist eine Sperrung über den ServiceDesk möglich.

Erneuerung

1. Aktives Zertifikat auswählen

2. Button „Renew“ drücken und bestätigen

3. Es wird automatisch ein neuer Zertifikatsantrag generiert und eingereicht. Der initiale private Schlüssel bleibt bestehen

Download

1. Aktives Zertifikat auswählen

2. Button „Download“ drücken

3. Liste mit diversen Dateiformaten zum Download wird angezeigt:

- Certificate only, PEM encoded – Nur Zertifikat im PEM Format
- Certificate (/w issuer after), PEM encoded – Zertifikat im PEM Format mit nachfolgenden Ausstellerzertifikat(-en)
- Certificate (/w chain), PEM encoded - Zertifikat im PEM Format, beginnend mit Wurzelzertifikat ► Ausstellerzertifikat(-en) ► Zertifikat
- PKCS#7 – Zertifikat mit Zertifikatskette im PKCS#7 Format, binär
- PKCS#7, PEM encoded - Zertifikat mit Zertifikatskette im PKCS#7 Format

- Intermediate(s)/Root only, PEM encoded - nur Zwischen-CAs und Root-CA
- Root/Intermediate(s), PEM encoded - nur Root-CA und Zwischen-CAs (als Certificate

Zertifikatsformate für verschiedene Server :
- Apache Webserver: Certificate (/w issuer after)
-

Achtung: entfernen Sie den Parameter SSLCertificateChainFile. Die CA-Zertifikate sind bereits in der Zertifikatsdatei enthalten

- 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