Sectigo SSL-Zertifikate über den KDD beantragen

Diese Seite richtet sich an DV-Koordinatoren von Instituten und Einrichtungen, die SSL/TLS/HTTPS-Zertifikate (nach dem X.509-Standard) für den Betrieb von Servern benötigen. Die TU Braunschweig setzt Zertifikate aus der DFN-PKI ein. Diese sind für den dienstlichen Einsatz vorgesehen und können kostenfrei beantragt werden.

> Einen Link zur Online-Schnittstelle für DV-Koordinatoren finden Sie im Koordinatoren Daten Dienst (KDD) unter dem Reiter „Serverzertifikate“.

Zertifikat für Server beantragen

Um ein Zertifikat für einen Server zu beantragen, müssen folgende Arbeitsschritte durchgeführt werden:

1. Sie sind **DV-Koordinator** Ihres Instituts/Ihrer Einrichtung.
2. (Sie installieren ggf. openssl auf Ihrem Linux Server/Rechner nach).
3. Sie generieren einen **Zertifikatsantrag** (certification request, certificat signing request (CSR)):
   - Beim ersten Mal mit Erzeugung eines privaten Schlüssels (s.u.)
   - Bei Erneuerung eines bestehenden Zertifikats muss der private Schlüssel nicht neu erzeugt werden. (s.u.)
4. Sie beantragen das Zertifikat über die Online-Schnittstelle für DV-Koordinatoren, deren Link Sie im KDD finden (Login über SAML mit der persönlichen E-Mail-Adresse, bitte keinen Funktionsaccount oder dergleichen nutzen).
   - **Email**: Persönliche E-Mail-Adresse der antragstellenden Person, hierhin werden das Zertifikat und alle weiteren Informationen wie z.B. zum Ablaufen eines Zertifikates geschickt. Diese E-Mail-Adresse ist vorgegeben und darf nicht verändert werden. **Wichtig:** Bei **External Requester** bitte zusätzlich eine Gruppen-E-Mail-Adresse angeben.

- **Certificate Profile**: Hier ist die Auswahl auf das für alle Szenarien nutzbare Profil „OV MultiDomain“ beschränkt. Wenn ein anderes Profil (Liste siehe unten) gewünscht wird, bitte eine Email mit dem CSR und den weiteren notwendigen Angaben (Gruppen-E-Mailadresse und Alternativnamen) an noc@tu-bs.de senden.
- **Certificate Term**: Die Laufzeit des Zertifikates; die vorgegebene Spanne beträgt 1 Jahr.
- **CSR**: Selbst erstellten CSR einfügen.
- **Commom Name**: DNS-Namen des Servers (wird bei Upload eines CSR vorausgefüllt): Bitte prüfen, ob der Name richtig ist und gegebenenfalls den CSR prüfen. Hier ist auch ein Wildcard-Name möglich. Bei Wildcard-Namen haben wir gegebenenfalls Rückfragen.
- **Renew**: Wenn eine automatische Erneuerung gewünscht ist, bitte Option auswählen und angeben, wann die Erneuerung erfolgen soll. Wenn diese Option ausgewählt ist, wird automatisch basierend auf dem genutzten CSR ein neues Zertifikat erzeugt und an die angegebenen E-Mail-Adressen geschickt. Mit der angegebenen Anzahl von Tagen wird gesteuert, wann Sie vor Ablauf des ursprünglichen Zertifikates ein erneuertes Zertifikat erhalten.
- **Subject Alternative Names**: Weitere Namen des Servers. Hier sind auch Wildcard-Namen möglich.
- **Annual Renewal Passphrase** Dieses Passwort ist optional, es wird nicht benötigt für die automatische Verlängerung. Das Passwort ist nur notwendig, um das Zertifikat manuell über den Sectigo Support sperren oder erneuern zu lassen. Für die manuelle Erneuerung oder Sperrung eines Zertifikates durch eine handlungsberechtigte Person der Abteilung Netze ist das Passwort ebenfalls nicht notwendig.
- **Wichtig: External Requester** Hier bitte eine Gruppen-E-Mailadresse angeben, die idealerweise an ein Ticketsystem angeschlossen ist. An diese E-Mail-Adresse werden zusätzlich das Zertifikat und alle weiteren Informationen wie z.B. zum Ablaufen eines Zertifikates verschickt. Bei dieser E-Mail-Adresse darf es sich nicht um eine persönliche E-Mail-Adresse handeln, sondern z.B. um einen Mailverteiler für die IT oder die Kontakt-E-Mail-Adresse des Instituts. Requester und External Requester dürfen nicht identisch sein.

5. .Durch Klick auf [**Enroll]** den Zertifikatsantrag abschicken
6. Es wird eine Email, dass ein Zertifikat beantragt worden ist, an die Email-Adresse der antragstellenden Person und an die Email-Adresse(n), die als External Requester angegeben worden sind, geschickt. Parallel dazu erscheint der Zertifikatsantrag zur Überprüfung durch eine handlungsberechtigte Person im Zertifikatsmanager. Ein weiteres Zutun der antragstellenden Person ist nicht notwendig.
7. Nachdem eine handlungsberechtigte Person den Zertifikatsantrag genehmigt hat, wird eine Email, dass der Antrag genehmigt worden ist, an die antragstellende Person und an die External Requester geschickt. In einer weiteren Email folgen die Informationen zum Bezug des eigentlichen Zertifikats und der Zertifikatskette. Diese E-Mail enthält auch die **Antragsnummer** für Rückfragen.
8. Sie notieren oder speichern sich die Antragsnummer.
9. Sie installieren das Zertifikat auf dem Server.

10. Hier achten Sie darauf, dass Sie folgende Dateien in den Dienstkonfigurationen referenzieren:
    - Der private Schlüssel.
    - Das von Ihnen heruntergeladene signierte Zertifikat
    - Die von Ihnen heruntergeladene Zertifikatskette

Abweichende CN-Attribute

Das CN-Attribut ist das wichtigste Attribut im Zertifikat. Es muss den vollständigen Namen des Servers beinhalten. Gemeint ist hierbei der vollständige Servername mit Domainangabe (FQDN, „fully qualified domain name“). Dieser ist beispielsweise im KDD nachzuschlagen oder mit den Kommandos nslookup bzw. host per DNS abzufragen. Es ist außerdem möglich, dass der Name gesetzt wird, unter dem der Dienst im Netz erreichbar sein soll (Stichworte „DNS-Alias“, „Virtual Host“). In der Regel werden allerdings Namen, unter denen der Dienst im Netz erreichbar sein soll, nicht als CN über den FQDN angegeben, sondern über sog. alternative Attribute (Subject Alternative Name, SAN).

> Es ist nicht notwendig, Subject Alternative Names („die DNS-Aliase Ihres Servers“) im CSR einzubinden. Sie können die zusätzlichen Namen einfach in das Formular eintragen.

Beispiel: FQDN zur Verwendung als CN-Attribut: server01.inst.misc.tu-bs.de

Beispiel: alternatives Attribut (vom Typ DNS): www.institutsname.tu-bs.de

CN-Attribute müssen zwingend auf eine der auf die TU Braunschweig registrierten Domains "tu-bs.de" oder "tu-braunschweig.de" enden.

Zertifikatsantrag (CSR) erzeugen

Der folgende Abschnitt beschreibt Details zur Erzeugung von privatem Schlüssel und Zertifikatsantrag.

> Wenn Sie mehr Details benötigen, finden Sie eine umfänglichere Anleitung zu diesem Thema auf den Webseiten der DFN-PKI und darüber hinaus die vollständige Anleitung zu OpenSSL unter https://www.openssl.org/docs/

Zertifikatsantrag und privaten Schlüssel erzeugen

Wenn Sie noch kein SSL auf Ihrem Server einsetzen, verfahren Sie bitte, wie im Folgenden beschrieben. Zertifikatsanträge müssen in einem maschinell verarbeitbaren Format bei der RA eingereicht werden, dem Public Key Cryptography Standard Nr 10, PKCS#10, und werden bei Verwendung eines geeigneten Werkzeuges automatisch erstellt. Der Zertifikatsantrag setzt sich

aus vier Teilen zusammen:

1. Dem „Subject Distinguished Name“, kurz DN, die teilweise durch die Policy vorgegeben sind, wie Landesbezeichnung, Country, C=de; die Ortsbezeichnung O=Technische Universitaet Braunschweig.
2. Den optionalen Attributen.
3. Einer digitalen Signatur mit dem privaten Schlüssel (der später auch auf dem Server abgelegt wird).
4. Einer Kennzeichnung des verwendeten Signaturalgorithmus.

Insbesondere wenn Sie mehrere Zertifikate beantragen, sollten Sie sich beispielsweise eine Konfigurationsdatei für OpenSSL erstellen, in der die wesentlichen Angaben bereits enthalten sind. Im Unterabschnitt „OpenSSL-Konfigurationsdatei“ ist ein Beispiel angegeben.

Zertifikate für einen Windows-Dienst erstellen Sie am besten mit Unterstützung dieses Supportartikels (D307267) von Microsoft.

Falls Sie Ihren Dienst bisher ohne Zertifikat betreiben, müssen Sie ein entsprechendes Schlüsselpaar nach dem RSAVerfahren erzeugen. Das folgende openssl-Kommando führt die Schlüsselgenerierung, die Abfrage eines Passwortes für diesen Schlüssel, die Attribut-Abfrage und die anschliessende Erstellung des Zertifikatsantrages durch:

```
openssl req -config myopenssl.conf -newkey rsa:4096 -outform pem -out certreq.pem
```

Die einzelnen Befehlsteile bedeuten folgendes:

1. openssl: Programmname des Openssl-Kommandos, evtl. muss der komplette Pfad z.B. /usr/local/bin/openssl angegeben werden.
2. req: erstellt einen PKCS#10-Antrag
3. -config: verweist ggf. auf die ssl-Konfig-Datei für Voreinstellungen, siehe Abschnitt „OpenSSL Konfigurationsdatei“
4. -newkey rsa:4096: neues Schlüsselpaar mit RSA und einer Key-Länge von 4096 Bit
5. -outform PEM: Privacy Enhanced Mail Ausgabeformat
6. -out certreq.pem: speichert den Antrag unter certreq.pem. Achtung: die Konfigurationsdatei enthält die Direktive, den neu zu erstellenden privaten Schlüssel in server-key.pem zu speichern. Sollen mehrere Anträge hintereinander erstellt werden, müssen die Dateien nach jedem Durchgang umbenannt werden, um ein Überschreiben zu vermeiden.

Zertifikatsantrag ohne erneute Erzeugung eines privaten Schlüssels erzeugen

Setzen Sie bereits SSL auf Ihrem Server ein und möchten Sie den dafür verwendeten private key weiter verwenden, so erzeugen Sie den Zertifikatsrequest wie in diesem Abschnitt beschrieben.

Läuft der Dienst mit einem selbst signierten Zertifikat und haben Sie bereits einen RSA-Schlüssel erstellt mit einer Länge von 2048 Bit, können Sie diesen Schlüssel für Ihr neues Zertifikat weiter verwenden. Mit folgendem Kommando kann dann eine Zertifizierungsanfrage für den vorhandenen Key (server.key) erstellt werden:

```
openssl req -new -config myopenssl.conf -key server-key.pem -keyform PEM -outform pem -out certreq.pem
```

Mit -keyform PEM bzw. -keyform DER sollten Sie das Format des vorhandenen Schlüssels berücksichtigen.

Entfernen der Passphrase für automatischen Start von Diensten

Beachten Sie bitte auch, dass Sie den Dienst den Sie mit dem so beantragten Zertifikat ausstatten, beim Start/Neustart stets die Angabe der Passphrase erfordert. Um einen Dienst auch ohne manuelle Eingabe der Passphrase starten zu können, muss man ggf. auf die Passphrase verzichten. Für den Betrieb von Diensten, die auch nach einem ungeplanten Neustart des Servers (z.B. Stromausfall, Softwarefehler) sofort und ohne manuelle Intervention erreichbar sein sollen, muss die Passphrase entfernt werden. Darüber hinaus setzen manche Produkte voraus, dass man zuvor die Passphrase entfernt.

Das Entfernen der Passphrase ist kritisch und aus Sicht der IT-Sicherheit nicht empfehlenswert. Das Zertifikat auf dem Server ist dann ungeschützt hinterlegt und kann bei einer Kompromittierung des Servers besonders einfach kopiert und für Angriffe genutzt werden. Grundsätzlich - ob mit oder ohne Passphrase - gilt: Sollte der Server gehackt werden, so ist das Zertifikat samt private key nicht mehr vertrauenswürdig. Das Zertifikat muss dann umgehend gesperrt werden. Sie müssen in einem solchen Fall sowohl einen neuen private key generieren, als auch ein neues Zertifikat beantragen.

Das Entfernen der Passphrase kann mit dem folgenden Kommando durchgeführt werden:

```
openssl rsa -in server-key.pem -out server-key_nopass.pem
```

In Abhängigkeit von der Version von OpenSSL kann die genaue Kommandosyntax leicht abweichen.

OpenSSL Konfigurationsdatei

In manchen der zuvor aufgeführten Kommandos wird eine Konfigurationsdatei referenziert:

```
... -config myopenssl.conf ...
```

(ohne Alternative DNS Names)

Sollte der Server nur über genau einen Hostnamen erreicht werden, könnte der Inhalt einer solchen Datei wie weiter unten beschrieben aussehen.

(mit Alternative DNS Names)

Sollte der Server mehr als einen Namen (z.B. CNAMES/Aliase) haben, so können/sollten alle Namen entsprechend im Zertifikat hinterlegt werden. Zu diesem Zweck benutzen Sie bitte das Eingabefeld „Subject Alternative Names“ des Webformulars wie oben beschrieben.

Alternativ, aber aufwendiger, lassen sich die Alternativnamen auch über die Konfigurationsdatei angeben. Dazu ändern Sie, wie weiter unten beschrieben, am Ende die Beispiel-Hostnamen unterhalb von “[subject_alt_name]„ in die Aliase um, über die der Server zusätzlich zum eigentlichen Hostnamen (wird bei der Erstellung des Zertifikatsantrags erfragt oder kann bei „commonName“ angegeben werden) noch erreicht werden soll. Außerdem können Sie weitere Namen in entsprechender Weise hinzufügen.

Zertifikat anzeigen

Der Datei, die Sie per E-Mail aus der CA zugesendet bekommen, können Sie die in ihr enthaltenen Informationen nicht ansehen. Um die Zertifikatsinformationen einer Zertifikatsdatei anzeigen zu können, verwenden Sie:

```
openssl x509 -text -noout -in server-crt.pem
```

Zertifikat sperren

Durch die Beantragung des Zertifikates akzeptieren Sie Handlungsanweisungen, dass Sie Zertifikate bei Bedarf auch wieder sperren. Gründe für eine Sperrung könnten sein:

- Ein Zertifikat soll ersetzt oder erneuert werden (das vorherige ist zu sperren).
- Der private Key wurde offen gelegt.
- Der Server wurde kompromittiert.

Durch die Sperrung eines Zertifikats wird dessen eindeutige Seriennummer auf einer Sperrliste/Widerrufsliste (certificate revocation list, CRL) veröffentlicht. Bezüglich der Umsetzung der Sperrung von Zertifikaten bei Clients ist zur Zeit in manchen Fällen noch einiges im Argen. Im Idealfall ist bei einem gesperrten Zertifikat die weitere Verwendung des Zertifikates aufgrund der Prüfung der Sperrliste seitens der Clients verhindert.

Die Sperrung eines Zertifikats lässt sich nicht rückgängig machen. Sollte ein Zertifikat irrtümlich gesperrt worden sein, müssen Sie ein neues Zertifikat beantragen.

Für die Durchführung einer Sperrung gibt es drei Möglichkeiten:

1. Sperren über Webformular: Hier müssen Sie die sogenannte „certificate ID“ angeben. Diese ID finden Sie als „Self-Enrollment Certificate ID“ in der ersten E-Mail, die Sie nach Beantragung über das Webformular erhalten haben (Betreff: GÉANT TCS: Awaiting approval for certificate *FQDN*). Weiterhin benötigen Sie die „Annual Renewal Passphrase“, die Sie bei Beantragung über das Webformular vergeben haben (siehe oben).
2. Sperrantrag im KDD über den entsprechenden Reiter (verfügbar ab Ende 2022)
3. Kontakt zum IT-Service-Desk. Geben Sie die Antragsnummer und/oder die Seriennummer und den Common Name an.

Installation eines Zertifikats für Apache

Die Konfiguration der Zertifikate ist prinzipiell bei allen Apache-Installationen sehr ähnlich – hier wird nur grundlegend dargelegt, wie dies vorzunehmen ist. Für versionsspezifische Abweichungen konsultieren Sie bitte die Hilfe über die man-pages Ihrer Linux-Distribution. Folgende Dateien werden benötigt:

- common_name.pem: Die Zertifikatsdatei, die Sie von einem der Links in der E-Mail bezogen haben. Für Apache nutzen Sie bitten den zweiten Link in der E-Mail („as Certificate (w/issuer after), PEM encoded“).
- common_name_interm.cer: Diese Datei enthält alle „über“ dem Server liegenden Zertifikate bis zum Root Zertifikat des Zertifikatanbieters. Einen Link zu dieser Zertifikatskette erhalten Sie sie mit der E-Mail, in der auch die Links zu verschiedenen Zertifikatsformaten enthalten sind (Betreff:„GÉANT TCS certificate information: *Common name ihres Servers*“). Bitte nutzen Sie dazu den vorletzten Link („as Root/Intermediate(s) only, PEM encoded“) in der E-Mail, die Sie erhalten haben.
- privkey.pem: Der private Schlüssel des Servers, den Sie zur Erstellung des Zertikatantrags (CSR) genutzt haben.

Zur Installation sind die folgenden Schritte nötig:

1. Stoppen Sie den eventuell gestarteten Apache Webserver Dienst (z.B. „service httpd stop“).
2. Kopieren Sie die drei Zertifikatsdateien in einen Unterordner des Apache Webservers (z.B. :/etc/apache2/ssl.key/).
3. Editieren Sie bzw. legen Sie eine neue V-Hosts-Datei unter “/etc/apache2/vhosts.d„ an. In der Konfigurationsdatei des V-Hosts werden unter anderem die Zertifikate mit angegeben.
4. Wichtig ist, dass „ServerName“ genau mit dem Namen angegeben wird, für den Sie das Zertifikat beantragt haben.
5. Den Aufbau der Datei (Beispielkonfiguration) finden Sie weiter unten.

6. Aktivieren Sie ggf. noch MOD_SSL für den Apache-Webserver.
7. Starten Sie den Apache neu.
8. Besuchen Sie die Startseite Ihres Servers, kontrollieren Sie die Logfiles.

Installation eines Zertifikats für NGINX

Folgen Sie prinzipiell den Anweisungen zur Installation bei Apache (siehe oben). Lediglich die Dateien, die Sie herunterladen müssen unterscheiden sich.

- common_name_cert.cer: Eine Zertifikatsdatei nur für Ihren Server, die Sie von einem der Links in der E-Mail bezogen haben. Für NGINX nutzen Sie bitte den ersten Link in der E-Mail („as Certificate only, PEM encoded“).
- common_name_interm.cer: Diese Datei enthält alle „über“ dem Server liegenden Zertifikate vom Root Zertifikat des Zertifikatanbieters abwärts. Einen Link zu dieser Zertifikatskette erhalten Sie sie mit der E-Mail, in der auch die Links zu verschiedenen Zertifikatsformaten enthalten sind (Betreff:„GÉANT TCS certificate information: *Common name ihres Servers*“). Bitte nutzen Sie dazu den vorletzten Link („as Root/Intermediate(s) only, PEM encoded“) in der E-Mail, die sie erhalten haben.
- privkey.pem: Der private Schlüssel des Servers, den Sie zur Erstellung des Zertikatantrags (CSR) genutzt haben.

Fügen Sie nun die beiden erhaltenen Zertifikatsdateien mittels „cat“ im Linux Terminal oder einem ähnlichen Programm zusammen:

cat common_name.cer common_name_interm.cer > common_name_cert_chain.cer

Bitte nutzen Sie zum Zusammenfügen der beiden Dateien keine Office-Programme, wie MS Office, Open Office oder Libre Office. In Ihrer NGINX Konfigurationsdatei geben Sie nun den Pfad zu der neu erstellten Datei (common_name_cert_chain.cer) als SSL_CERTIFICATE_PATH und den Pfad zur privaten Schlüsseldatei Ihres Servers (privkey.pem) als SSL_KEY_PATH an.

Installation eines Zertifikats (allgemein)

Für die Konfiguration eines Zertifikates sollten Sie sich zuerst mit den Konfigurationsdateien Ihres Webservers vertraut machen. Diese finden Sie in der Regel unter */etc/<Produkt>/* . *(/etc/nginx, /etc/apache2, /etc/httpd, ...).*
Welche Änderungen Sie zur Absicherung Ihres Webservers an Ihrer Konfigurationsdatei vornehmen müssen, können Sie im kostenlosen Konfigurationsgenerator von Mozilla (https://ssl-config.mozilla.org/) sich anzeigen lassen. Nachdem Sie im Konfigurationsgenerator Ihre

Einstellungen ausgewählt haben, können Sie mit der angezeigte Konfiguration Ihre Webserver-Konfigurationsdatei anpassen.
Die Webserver-Konfigurationsdatei finden Sie direkt in Ihrem Konfigurationsordner, meist werden auch hier Produktnamen als Dateinamen verwendet. *(apache2.conf, htttpd.conf, nginx.conf, ...)*
Nach der Anpassung Ihrer Konfiguration sollten Sie die verwendeten Platzhalter *(/path/to/...)* an Ihre lokalen Gegebenheiten anpassen.
Anschließend können Sie die Syntax Ihrer Konfiguration mit einem Test *(apachectl configtest , nginx -t , ...)* überprüfen und bei Erfolg den Webserver neu starten.

Skizze einer Beispielkonfiguration: vhost-ssl.conf

```
[...]
<VirtualHost _default_:443>
DocumentRoot "/srv/www/htdocs"
ServerName example.inst.tu-bs.de:443
[...]
SSLEngine on
SSLCertificateFile etc/apache2/ssl.key/common_name.pem
SSLCertificateKeyFile /etc/apache2/ssl.key/privkey.pem
SSLCertificateChainFile /etc/apache2/ssl.key/common_name_interm.cer
[...]
</VirtualHost>
[...]
```

OpenSSL Konfigurationsdatei ohne Alternativnamen

```
#
# myopenssl.conf
#
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd
[ req ]
default_bits              = 4096
default_keyfile         = server-key.pem
distinguished_name        = req_distinguished_name
attributes              = req_attributes
string_mask = nombstr
req_extensions = v3_req
```

```
[ req_distinguished_name ]
countryName = Laendername (bitte nicht aendern)
countryName_default = DE
countryName_min = 2
countryName_max = 2

0.organizationName = Name der Organisation (bitte nicht aendern)
0.organizationName_default = Technische Universitaet Braunschweig

0.organizationalUnitName = Offizieller Einrichtungsname (ohne Umlaute)
0.organizationalUnitName_default =

1.organizationalUnitName = Optional Abteilung oder AG im Institut
1.organizationalUnitName_default =

stateOrProvinceName = Bundesland (ausgeschrieben)
stateOrProvinceName_default = Niedersachsen
localityName = Locality Name - Stadt (Sitz der TU Braunschweig)
localityName_default = Braunschweig

commonName  = Voller DNS-Name unter dem der Service erreichbar ist
commonName_max = 64

emailAddress = Support E-Mail Adresse der Einrichtung (bevorzugt)
emailAddress_max = 40
emailAddress_default =

[ req_attributes ]
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

OpenSSL Konfigurationsdatei mit Alternativnamen

```
#
# myopenssl.conf
#
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd
[ req ]
default_bits              = 4096
default_keyfile         = server-key.pem
distinguished_name        = req_distinguished_name
attributes              = req_attributes
string_mask = nombstr
req_extensions = v3_req
```

```
[ req_distinguished_name ]
countryName = Laendername (bitte nicht aendern)
countryName_default = DE
countryName_min = 2
countryName_max = 2

0.organizationName = Name der Organisation (bitte nicht aendern)
0.organizationName_default = Technische Universitaet Braunschweig

0.organizationalUnitName = Offizieller Einrichtungsname (ohne Umlaute)
0.organizationalUnitName_default =

1.organizationalUnitName = Optional Abteilung oder AG im Institut
1.organizationalUnitName_default =

stateOrProvinceName = Bundesland (ausgeschrieben)
stateOrProvinceName_default = Niedersachsen
localityName = Locality Name - Stadt (Sitz der TU Braunschweig)
localityName_default = Braunschweig

commonName  = Voller DNS-Name unter dem der Service erreichbar ist
commonName_max = 64

emailAddress = Support E-Mail Adresse der Einrichtung (bevorzugt)
emailAddress_max = 40
emailAddress_default =

[ req_attributes ]
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName=@subject_alt_name

[ subject_alt_name ]
DNS.1=*.tu-bs.de
DNS.2=*.tu-braunschweig.de
```

Revision #7
Created 25 January 2024 11:06:28 by Tina Strauf
Updated 25 October 2024 09:15:12 by Sandra Ulbrich