

Serverzertifikat beantragen

Stand: 01.03.2024

Inhalt

Requesterstellung.....	1
Zertifikat beantragen.....	2
Serverzertifikate automatisiert verwalten – ACME / Certbot.....	5

Requesterstellung

Um ein Serverzertifikat der HS-Harz-CA zu beantragen, erstellen Sie zuerst einen Request auf Ihrem Server. Eine Anleitung zur Requesterstellung finden Sie unter:

https://www.hs-harz.de/dokumente/extern/Rechenzentrum/Webseitendateien/Erstellung_eines_Requests_mit_OpenSSL.pdf.

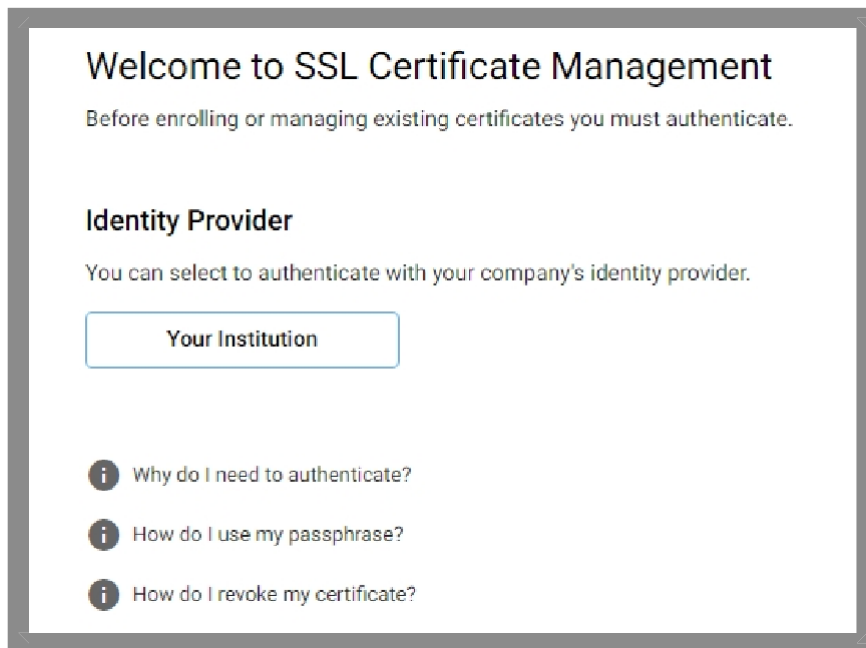
Eine Schlüsselgenerierung im Browser ist mit dem Certificate Manager von Sectigo derzeit leider noch nicht möglich.

Zertifikat beantragen

Danach beantragen Sie das Serverzertifikat auf der Seite des CertificateManagers von Sectigo.

<https://cert-manager.com/customer/DFN/ssl/TdXR2-eS-F5BXOPvsuch>

Im ersten Fenster wählen Sie den Identity Provider der Hochschule Harz aus und autorisieren sich am Campus-Login.



Welcome to SSL Certificate Management

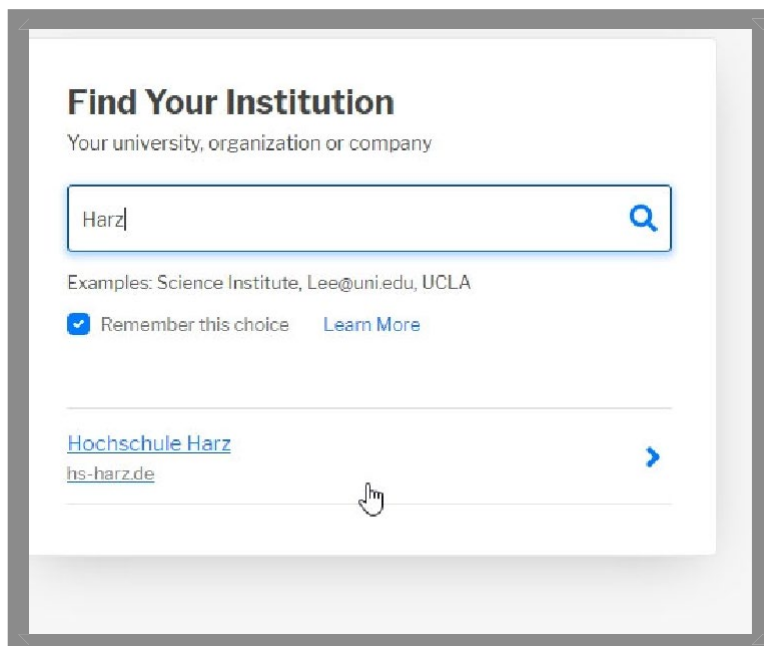
Before enrolling or managing existing certificates you must authenticate.

Identity Provider

You can select to authenticate with your company's identity provider.

[Your Institution](#)

- i** Why do I need to authenticate?
- i** How do I use my passphrase?
- i** How do I revoke my certificate?



Find Your Institution

Your university, organization or company

Harz

Examples: Science Institute, Lee@uni.edu, UCLA

Remember this choice [Learn More](#)

[Hochschule Harz](#)

hs-harz.de

Nach erfolgreichem Campus-Login die Attributübergaben bestätigen.

Es erscheint die Auswahl des Antragsformulars (SSL Certificate Enrollment).

Haben Sie schon Zertifikate dann erscheint Ihre Zertifikatsliste. Über den Button

Enroll Certificate

kommen Sie weiter zum Antragsformular.

SSL Certificate Enrollment

Enroll with Access Code

An access code will grant you access to a protected enrollment account.

Access code

Select Enrollment Account

Select from the following enrollment accounts to continue.

Account

Select an account or provide access code.

Next

Ignorieren Sie den ersten Punkt Enroll per Access Code.

Unter dem zweiten Punkt Select Enrollment Account finden Sie die Antragsformularauswahl.

Wählen Sie hier Hochschule Harz Serverzertifikat beantragen aus.

Select Enrollment Account

Select from the following enrollment accounts to continue.

Select...

Hochschule Harz Serverzertifikat beantragen

Next

Im nächsten Schritt wird der erstellte Request hochgeladen.

Das Certificate Profile auf OV Multi-Domain stellen.

An der Gültigkeitsdauer kann nichts geändert werden, diese ist voreingestellt.

SSL Certificate Enrollment

Please complete this form to enroll for a certificate. Your certificate will be associated with the organization/department shown below.

If the certificate can be issued immediately you will be able to download it after submitting. If the certificate requires approval you will be notified by email to the address below when its issued.

Organization	Hochschule Harz, Hochschule für angewandte Wissenschaften
Department	None
Email	sthielert@hs-harz.de

Certificate Profile *
OV Multi-Domain

Certificate Term *
1 Year

Den Request hochladen.

Unter Subject Alternatives Names können weitere DNS Namen angegeben werden.

Das Feld External Requesters kann ausgefüllt werden, wenn ein weiterer Administrator über den Status des Zertifikates informiert werden soll.

CSR *

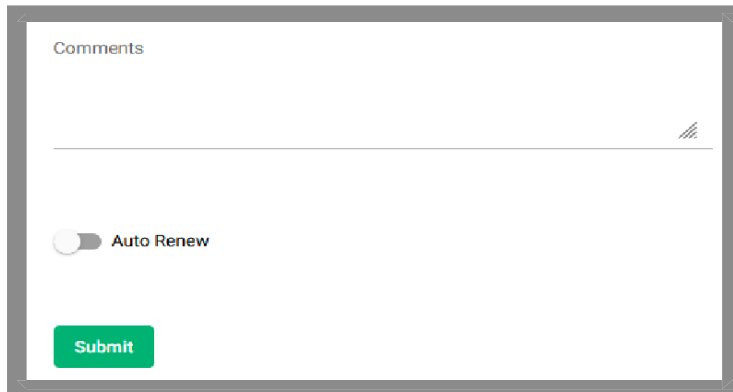
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDCCCA-FACAQAwcIx.CzAJBgNVBAYTAkRFHRcwFQYDVQQIDA5TYWNo2VuLUFu
aGFsdEUMBIGA1UEBwwLV2Vybm1nZXJvZGUxQzBBBgNVBAoMOKhVY2hzY2h1bGUG
SGFyeiIwSG9jaHNjaHVzZS8mdWVyIGFuZ2V3YW5kdGUgV21zc2Vuc2NoYWZ0ZW4x
HDAaBgNVBAMME3d3dy5rYXQtbmV0end1cm5uZGUxITAFBgkqhkiG9w0BCQEWEnR2
aXR1cmFAaHhtaGFyei15kZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMBWmSUXxMTcf0P3Io+e6a3cCz6VK14eVnCZHa0BSWkqocOGncsaUEOV7A0t73
G1y5n4/RajW4k/7npa8/vfnT7BggN5dj/Gdf3w6v2fE5VefDw4E6Q0u4G05iddat
AF0FwEpx0Nn042fEdodnTQ/04rYN5Hf9MF7+G55HhsLuUZHST51/cYts9Qg8u58a
Xmd3dQAu3L814Hwwx4ES/0zH/dzo9kAjFM1uDa1tpThjk11Qv5S/KfFkAh8CKV+y
DwRYNpSUao710Bo3KXKvQyQQjYtO+fAx7PofqXdgFvwqtIJLnjt9bXkr22csyrxg
TE7h...
```

Common Name
url.hs-harz.de

Subject Alternative Names
test.hs-harz.de

External Requesters

Auto Renew kann eingeschaltet werden. Wählen Sie die Tage aus, wann ein Renew erfolgen soll, z.B. 7 Tage. Dann wird 7 Tage vor Ablauf des Zertifikates automatisch ein neuer Antrag mit denselben Daten generiert. Diese kann dann von den Mitarbeiter der Zertifikatsstelle bearbeitet werden.



Comments

Auto Renew

Submit

Und absenden.

Ihr Antrag wird schnellstmöglich bearbeitet. Über den Status werden Sie per E-Mail informiert.

Hinweis:

Die Serverzertifikate, die per Antrag eingehen verlängern sich nicht automatisch neu, hierzu bitte nachfolgenden Punkt beachten.

Serverzertifikate automatisiert verwalten – ACME / Certbot

Mit der neuen CA von Sectigo ist es möglich Zertifikate automatisiert mittels ACME-Protokoll erstellen zu lassen.

Beispiele für unterstützte Clients: certbot, acme.sh oder win-acme

ACME- Account beantragen

Beim Rechenzentrum können die Zugangsdaten per E-Mail beantragt werden. Dazu schicken Sie einfach eine formlose E-Mail mit der FQDN des Servers an ca@hs-harz.de. Sie bekommen dann die notwendigen Werte für das externe Accountanbindung (eab-kid, eab-hmac-key und Sectigo Server) zugeschickt.

Lokale Installation z.B. certbot

Red Hat 8

```
yum install epel-release  
yum install certbot python2-certbot-apache
```

Debian

```
apt install certbot
```

Zertifikatsverwaltung mit certbot

Zertifikat erstellen

```
# certbot certonly --standalone --non-interactive --agree-tos --email <admin.mail@b-tu.de> --server <sectigo_server> --eab-kid <Wert von EAB-KID> --eab-hmac-key <Wert von EAB-HMAC-KEY> --domain <FQDN des Servers>,<alternativer FQDN>,<alternativer FQDN>,...
```

Mit den Werten von eab-kid und eab-hmac-key sind so umzugehen, wie mit dem privaten Schlüssel vom Zertifikat. Wenn certbot das erste Zertifikat heruntergeladen und sich beim Server registriert hat, werden beide Werte nicht mehr benötigt. certbot speichert sich die Anmeldedaten für das Zertifikat im dazugehörigen Account. Die Accountdaten sind deshalb zu schützen.

Die aktuellen Zertifikate sind dann unter `/etc/letsencrypt/live/<FQDN des Servers>/` zu finden und können direkt verlinkt werden.

Unter dem Verzeichnis `/etc/letsencrypt/live/FQDN des Serverzertifikats + Kette` abgelegt. Unter dem Verzeichnis `*/etc/letsencrypt/account/` wird ein entsprechender LetsEncrypt-Account angelegt.

Das Zertifikat in die WebServer-Config eintragen.

Zertifikat erneuern

```
# certbot renew --standalone --non-interactive --agree-tos --server <sectigo_server>
```

Renew kann regelmäßig, zum Beispiel per Cronjob, aufgerufen werden. Certbot prüft daraufhin alle installierten Zertifikate auf Ihre Laufzeit. Zertifikate mit einer verbleibenden Laufzeit von weniger als 30 Tagen werden aktualisiert.

Zertifikat sperren

```
# certbot revoke --cert-path <Pfad zum zu sperrenden Zertifikat> --server <sectigo_server>
```

Bei Fragen und Problemen stehen wir Ihnen gern zur Verfügung.

Ihr HS-Harz-CA Team