Serverzertifikate (ACME)

Serverzertifikate werden auf Servern (z.B. Webserver, Mailserver) eingesetzt, um eine sichere Verbindung (z.B. HTTPS) zu ermöglichen. Zugrunde liegt ein asymmetrisches Kryptosystem, bei dem ein Schlüsselpaar (bestehend aus privatem und öffentlichen Schlüssel) genutzt wird. Der öffentliche Schlüssel wird zusammen mit Metainformationen (Domainname und Organisation) durch eine *Certificate Authority (CA)* signiert und dadurch von gängigen Betriebssystemen und Webbrowsern vertraut.

Die Ausstellung von Zertifikaten im Rahmen unserer Teilnehme an Geant TCS findet durch den Anbieter HARICA – der Teil des griechischen Universitätsnetzes GUnet ist – voll automatisiert mittels Automatic Certificate Management Environment (ACME) statt.

Geben Sie *Dritten* niemals Zugriff auf den *privaten Schlüssel* und informieren Sie umgehend das Rechenzentrum, falls Sie den Schlüssel verlieren oder Grund zu der Annahme haben, dass dieser entwendet wurde!

Verkürzte Laufzeiten von Server-Zertifikaten

Da die Sperrung von Zertifikaten aufwändig ist oder häufig überhaupt nicht vorgenommen wird, ist eine Verkürzung des Gültigkeitszeitraums eine schon lange diskutierte Lösung. Mit Letsencrypt entstand der erste Anbieter, der von Browsern vertraute Zertifikate kostenlos anbietet und der gleichzeitig relativ kurze Laufzeiten von nur noch 90 Tagen für diese Zertifikate wählte. Möglich ist dies nur durch Automatisierung, die mittels *Automatic Certificate Management Environment (ACME)* erreicht wird.

Das *CA/Browser Forum* hat nun im April 2025 die Anpassung der TLS Baseline Requirements und damit die schrittweise Verkürzung der Laufzeiten von Serverzertifikaten – von zunächst 200 Tagen im Jahr 2026 bis auf nur noch 47 Tage im Jahr 2029 – beschlossen. Aus diesem Grund bieten wir ab sofort den Bezug von OV-Zertifikaten mittels ACME an.

Die Gültigkeit von Serverzertifikaten sinkt schrittweise auf nur noch 47 Tage. Nutzen Sie ACME für die automatisierte Beantragung von Zertifikaten

Ab 15.06.2026 enthalten Serverzertifikate den Verwendungszweck *clientAuth* nicht mehr. Sollten Sie ein Zertifikat für die Authjentifizierung von Clients benötigen, sprechen Sie uns bitte an.

1. Beantragung mittels ACME
2. Manuell

Funktionsweise

Der Bezug von Zertifikaten geschieht mittels *External Account Binding (EAB)* und nicht – wie häufig gewohnt – mittels ACME-Challenge (z.B. mittels HTTP-01 oder DNS-01). Bei dieser Methode erhalten

Sie eine Art API-Schlüssel, der Ihnen die Ausstellung von Serverzertifikaten für die Ihnen freigeschalteten Domainnamen erlaubt. Da der API-Schlüssel auf den jeweiligen Servern auf denen die Zertifikate genutzt werden hinterlegt wird, bietet es sich an, je Server einen eigenen API-Schlüssel zu nutzen. Bei den ausgestellten Zertifikaten handelt sich um OV-Zertifikate, die neben dem Domainnamen auch den Organisationsnamen *Hochschule Fulda* enthalten.

Beantragung eines API-Key für ACME

Für jedes System, auf dem Sie ACME nutzen möchten, muss einmalig ein entsprechender Zugang durch das RZ erstellt werden.

Bitte teilen Sie uns dazu die folgenden Daten mit: Ihren **Namen** und Ihre **Hochschul-E-Mail Adresse**, einen **Projekt- oder Servernamen** zur Unterscheidung der verschiedenen API-Keys, sowie die **Liste der Domains** für die Sie in diesem Projekt oder auf diesem Server Zertifikate beziehen möchten.

Sie können gerne die folgende Vorlage nutzen.

```
Ich bitte um Ausstellung eines ACME-Zugangs.

Name:
E-Mail:
Projekt:
Domains:
```

Sie erhalten von uns:

API-Endpunkt URL	Die URL, über die Sie die ACME-Schnittstelle von HARICA erreichen. Achtung, diese ist für jeden Account unterschiedlich.
EAB Key Identifier	Der Key identifier (KID) wird zur Identifikation ihres Account bei HARICA genutzt.
EAB HMAC Key	Der HMAC Key wird genutzt um die Daten bei der Kommunikation mit HARICA zu verschlüsseln und authentifizieren.

Halten Sie diese Daten unbedingt geheim und teilen Sie uns mit, falls Sie diese nicht mehr benötigen

Ausstellung

Die Beantragung, Ausstellung und Inbetriebnahme der Serverzertifikate kann voll automatisiert stattfinden. Dazu stehen Tools wie certbot (aber auch viele weitere) zur Verfügung. Die Präsentation einer ACME-Challenge (z.B. mittels HTTP-01 oder DNS-01) ist nicht notwendig. Stattdessen wird das Verfahren *External Account Binding (EAB)* genutzt, das Ihnen erlaubt mittels eines speziellen API-Schlüssel bestimmte Zertifikate zu beziehen.

Unter UNIXoiden Betriebssystemen mittels certbot

```
certbot certonly --standalone --non-interactive --agree-tos --email <eigene
Mailadresse> --eab-kid <Key ID> --eab-hmac-key <HMAC Key> --server <Server
```

```
URL> --domain <FQDN des Zertifikats>
```

Unter Micosoft Windows mittels "win-acme"

```
.\wacs.exe --source manual --acceptto s --eab-key-identifier <Key ID> --eab-key <HMAC Key> --baseuri <Server URL> --emailaddress <Mail> --host <FQDN>
```

Sowohl die Konfiguration als auch die ausgestellten Zertifikate finden Sie - falls nicht anders angegeben - im Verzeichnis `/etc/letsencrypt`.

Verzeichnis	Beschreibung
/etc/letsencrypt/accounts/acme-v02.harica.gr/	Enthält die Konfiguration Ihres ACME-Accounts. Hier befinden sich auch die privaten Schlüssel für Ihren den Zugang.
/etc/letsencrypt/live/	Enthält für jeden Domainnamen für den Sie ein Zertifikat ausgestellt haben ein Verzeichnis, in dem sich der *private Schlüssel* (privkey.pem), das *Serverzertifikat* (cert.pem), die *Zertifikatkette* (chain.pem) und die *vollständige Zertifikatkette inkl. dem Serverzertifikat* (fullchain.pem) befinden.

In der Regel benötigen Sie nur die Dateien privkey.pem und fullchain.pem

Manuelle Beantragung

Falls Sie ein Zertifikat benötigen, das spezielle Attribute enthält oder für die Authentifizierung von Clients eingesetzt werden kann, wenden Sie sich bitte an das Rechenzentrum.

Die manuelle Beantragung regulärer Serverzertifikate ist nur noch übergangsweise möglich. Bitte nutzen Sie ACME!

Schlüsselpaar und Certificate Signing Request erstellen

Für die manuelle Beantragung eines Serverzertifikats sind zunächst dessen Bestandteile (Schlüsselpaar und Metainformationen) zu generieren. Dies kann mit OpenSSL, das praktisch für alle aktuellen Betriebssystem verfügbar ist, geschehen. Wenn Sie GNU/Linux verwenden, steht Ihnen OpenSSL in aller Regel über den Paketmanager zur Verfügung. Unter Windows können Sie WinOpenSSL verwenden.

Konfigurationsdatei

Um das Schlüsselpaar und den Certificate Signing Request zu erstellen, verwenden Sie bitte die **Konfigurationsdatei der Hochschule Fulda**. An dieser Konfigurationsdatei müssen Sie keine Änderungen vornehmen - es seidenn, Sie möchten das Zertifikat mit mehr als einem Domainnamen ausstatten. In diesem Fall geschieht eine Änderung ausschließlich in den Zeilen 46-50!

Dateien erstellen

Geben Sie nun auf der Kommandozeile folgendes Kommando ein, um das Schlüsselpaar zu erzeugen.

```
  openssl req -new -nodes -out server.csr -keyout server.key -config
openssl.cnf
```

Nun werden alle notwendigen Metainformationen abgefragt. Die meisten Informationen dürfen nicht verändert werden. Die Angabe der Abteilung (Organizational Unit Name) ist optional. Unter *Common name* geben Sie bitte den primären Servernamen ein.

Die Bestandteile, die in diesem Schritt generiert werden sind:

- Certificate Signing Request (Datei server.csr, zum Hochladen auf die Antrags-Webseite)
- Privater Schlüssel des Server-Zertifikats (Datei server.key)

Zertifikatantrag stellen

Senden Sie ihren Zertifikatantrag (csr-Datei) an das Rechenzentrum. Öffnen Sie dazu zum Beispiel ein Ticket. Wir stellen das Zertifikat für Sie aus und lassen Ihnen die entsprechenden Dateien zukommen.

Senden Sie uns auf keinen Fall ihren privaten Schlüssel

Hinweise

- Für die Domain hs-fulda.de werden ausschließlich Zertifikate der Certificate Authorities (CS) HARICA und Letsencrypt akzeptiert
- Falls nicht anders beantragt stellt HARICA Zertifikate mit RSA-Schlüsseln und 2048 Bit Schlüssellänge aus
- HARICA erlaubt maximal 100 Domainnamen (SANs) in einem Zertifikat
- Es können keine Zertifikate für IP-Adressen ausgestellt werden
- HARICA unterstützt Schlüssellängen