Serverzertifikat beantragen

Ein Serverzertifikat bestelt aus einem privaten und einem öffentlichen Schlüssel, die mittels asymmetrischer Kryptographie *zueinander passen*. Der öffentliche Schlüssel, zusammen mit Metainformationen - wie dem Domainnamen für den das Schlüsselpaar gültig ist - werden in einem *Certificate Signing Request (CSR)* verpackt und durch eine *Certificate Authority (CA)* signiert. Das Resultat ist ein *öffentliches Serverzertifikat*, das ausschließlich mit dem *geheimen/privaten Schlüssel* verwendet werden kann.

Der Vertrag mit Sectigo wurde zum 10.01.2025 durch Sectigo gekündigt. Zur Überbrückung steht der Anbieter HARICA zur Verfügung. Die Ausstellung von Zertifikaten wird vorrübergehend manuell durch das RZ durchgeführt.

Speichern Sie den privaten Schlüssel nur auf Ihrem Server und erzeugen Sie ein Backup an einem sicheren Ort. Geben Sie den privaten Schlüssel niemals weiter und informieren Sie umgehend das Rechenzentrum, falls Sie den Schlüssel verlieren oder Grund zu der Annahme haben, dass dieser entwendet wurde!

Schlüsselpaar und Certificate Signing Request erstellen

Zur 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 nur einen Namen. 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