

ACME für Sectigo Zertifikate

Sinnvollerweise sollte die Nutzung von Zertifikaten für den Serverbetrieb automatisiert werden, um den Administrationsaufwand zu reduzieren und Hinweise auf abgelaufene Zertifikate zu vermeiden. Das RZ empfiehlt dies für alle Systeme, die länger als nur temporär betrieben werden. Hierzu kommt das inzwischen gut erprobte und stabile "Automated Certificate Management Environment (ACME)" zum Einsatz.

Vorgehen:

Es wird in den einzelnen Gliederungen bzw. Zuständigkeitsbereichen ein Admin bestimmt, der für eine oder mehrere Subdomain(s), z.B. physik.uni-freiburg.de zuständig ist. Dieser wendet sich an die PKI Stelle (pki@rz.uni-freiburg.de) des RZs und lässt sich einen ACME-Account einrichten.



Hinweis: Der Admin sollte auf jeden Fall einen regulären Mitarbeiter*in Status an der Universität Freiburg besitzen und bereits in der Vergangenheit über das DFN Serverzertifikate beantragt haben. War dies bisher nicht der Fall, wird ein formloses Bestätigungsschreiben vom Dekanat bzw. Leiter*in der Einrichtung benötigt.

Die beantragte Host-Domäne wird dann vom Rechenzentrum im Sectigo-Portal unterhalb der Domäne "uni-freiburg.de" hinzugefügt.

Es gibt eine ganze Reihe von Tools, die mit dem ACME-Server von Sectigo kommunizieren können und dabei für viele Standarddienste bereits Module enthalten, um diese zu konfigurieren (z.B. Apache, Nginx, ...). Eine Übersicht über diverse ACME Clients findet sich unter <http://acmeclients.com>. Ein weiterer, guter Einstiegspunkt hierfür ist zudem <https://certbot.eff.org> oder auch <https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-20-04>. Der Client ist für viele Betriebssysteme verfügbar, zudem können auf der Website Konfigurationsdateien erstellt werden.



Für Windows-Systeme kann dieser ACME Client jedoch für Apache / Nginx Server die Zertifikate nur beziehen, diese jedoch nicht automatisiert installieren. Ein ACME-Client mit GUI für Windows findet sich hier: <https://www.win-acme.com> - eine Anleitung wird momentan erstellt.

Diese Tools können einerseits direkt auf dem Server laufen, der mit dem Zertifikat arbeitet. Zudem können sie aber auch für eine ganze Serverlandschaft mit unterschiedlichen Administratoren auf einer dedizierten Maschine installiert werden, um die Zertifikate auf diese Weise dort zu beziehen und dann automatisiert zu verteilen.



Achtung: Der Account sollte auf jeden Fall nur auf sicheren Systemen eingesetzt werden, wo Nutzende nicht durch booten mit einem anderen Betriebssystem oder das Ausbauen des Datenträgers direkt Zugriff zum Filesystem erlangen können (Pool-PCs, Workstations in gemeinsam genutzten Laboren, Büros, ... o.ä.).

Auf dem System wird dann das jeweilige ACME-Tool konfiguriert, wofür die folgenden Informationen benötigt werden (Username, Passwort, ACME-Server)

Beispiel für certbot (Linux):

/etc/letsencrypt/cli.ini

```
max-log-backups = 0  
  
email = <userid>@rz.uni-freiburg.de  
  
agree-tos = true  
  
server = https://acme.sectigo.com/v2/GEANTOV  
  
eab-kid = <eab-kid>  
  
eab-hmac-key = <hmac>
```

[Zertifikate - Artikelübersicht](#), [Sicherheit - Artikelübersicht](#)



Hinweis: Das Setzen von <https://acme.sectigo.com/v2/GEANTOV> bietet den Vorteil, dass im Zertifikat als Stammorganisation GEANT und *nicht* SECTIGO steht. Das ist quasi der Ersatz für „DFN Forschungsverein...“. Hierfür muss jedoch ein ACME-Account in dem oben genannten Realm erstellt werden (Kontakt: pki@rz.uni-freiburg.de)



Für das Renewal der Zertifikate kann man entsprechende Automatismen setzen (hier das Beispiel für einen Systemd Timer):

/etc/systemd/system/certbot-renewal.timer

```
[Unit]  
  
Description=Timer for Certbot Renewal  
  
[Timer]  
  
OnBootSec=300  
  
OnUnitActiveSec=1d  
  
[Install]
```

```
WantedBy=multi-user.target
```

```
/etc/systemd/system/certbot-renewal.service
```

```
[Unit]
```

```
Description=Certbot Renewal
```

```
[Service]
```

```
ExecStart=/usr/bin/certbot renew --post-hook „systemctl  
restart nginx“
```

From:

<https://www.wiki.uni-freiburg.de/rz/> - RZ

Permanent link:

https://www.wiki.uni-freiburg.de/rz/doku.php?id=zertifikate_installieren_mit_acme-clients

Last update: **2023/01/13 12:45**

