

ANLEITUNG ACME

ALLGEMEINES

Zur Verwendung von ACME brauchen Sie einen EAB (external account binding) Account. Diesen können Sie am besten per E-Mail an its-helpdesk@ruhr-uni-bochum.de beantragen.

Zur Erstellung benötigen wir folgende Informationen von Ihnen:

- Name
- E-Mail
- Domains
- Projekt/Servername

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 Accounts bei HARICA genutzt.

EAB HMAC Key: Der HMAC Key wird genutzt, um die Daten bei der Kommunikation mit HARICA zu verschlüsseln und authentifizieren.

HINWEIS: Diese Daten sollten unbedingt geheim gehalten und nicht mit anderen Personen geteilt werden!

Um nun Serverzertifikate zu beantragen und abzurufen, benötigen Sie einen ACME-Client der Ihren EAB Account nutzen kann. Der bekannteste Client ist certbot (<https://certbot.eff.org/>). Darüber hinaus können auch andere ACME-kompatible Client-Implementierungen genutzt werden: <https://acmeclients.com/>

BEISPIELE

1. CERTBOT

Für den Certbot kann eine Konfigurationsdatei mit allen nötigen Angaben erstellt werden. Diese liegt per default unter „/etc/letsencrypt/cli.ini“. Falls keine cli.ini Datei vorhanden sein sollte, können Sie einfach eine erstellen. Die Datei sollte dann folgende Informationen enthalten:

```
max-log-backups = 1000
email = <Ihre E-Mailadresse>
key-type = rsa
agree-tos = true
standalone = true
noninteractive = true
rsa-key-size = 4096
server = <API-Endpunkt URL>
eab-kid = <EAB Key Identifier>
eab-hmac-key = <EAB HMAC Key>
```

Der Aufruf über Certbot sieht dann wie folgt aus:

```
certbot certonly --standalone -d <FQDN>,<SAN1>,<SAN2> --cert-name <certbot_inventory_Name>
```

2. WINC-ACME

Für win-acme kann man folgenden Aufruf verwenden:

```
.\wacs.exe --target manual --host <FQDN> --emailaddress <Emailadresse> --eab-key-identifier <EAB Key Identifier> --eab-key <EAB HMAC Key> --baseuri <API-Endpunkt URL> --store pemfiles --pemfilespath <Path>
```

Sie können auch den interaktiven Modus mit EAB nutzen:

```
.\wacs.exe --eab-key-identifier <EAB Key Identifier> --eab-key <EAB HMAC Key> --baseuri <API-Endpunkt URL>
```

KONTAKT & HILFE:

Bei Fragen und Problemen wenden Sie sich an unseren Helpdesk unter: its-helpdesk@ruhr-uni-bochum.de