SwissSign

SwissSign CA

SwissSign AG

Quick Start Guide - Beantragung von ACME-Tokens mit Certbot

SwissSign

Revision

Rev	Date	Who	Comment
1.0	21.06.2022	SwissSign AG	Initiales Dokument

SwissSign

Inhalte

1 Einleitung

Das Protokoll Automated Certificate Management Environment (ACME) automatisiert die Ausstellung von Webserver-Zertifikaten. Dieses Protokoll verwendet DNS- oder HTTP-Challenge-Typen, um die Eigentümerschaft von Webservern und Domänennamen zu überprüfen..

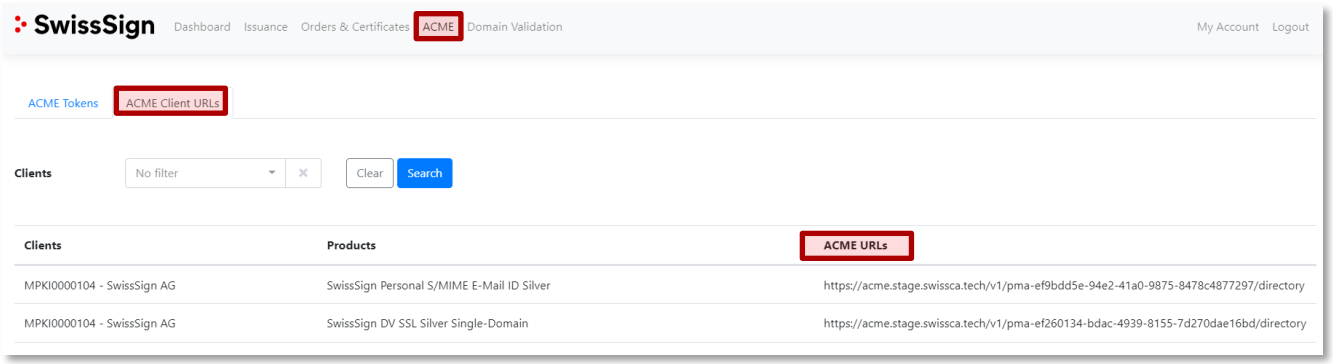
2 Setup

Certbot oder ein anderer ACME-Client kann für die Beantragung des Zertifikats verwendet werden. Wenn Certbot noch nicht auf Ihrem Computer installiert ist, finden Sie hier die Anleitung zur Installation von Certbot (**https://certbot.eff.org/**)

Bei jedem certbot-Befehl MUSS der Parameter --server auf die SwissSign CA ACME-Mapping-Adresse angegeben werden.

SwissSign CA Server Einrichtung Schritt für Schritt:

1. Melden Sie sich bei https://ra.swisssign.ch an.
2. Melden Sie sich mit Ihrem RA Operator Login an.
3. Gehen Sie zum Untermenü ACME in der Top Navigation
4. Klicken Sie auf "ACME Client URLs" (https://ra.swisssign.ch/acme/client/urls)
5. Wählen Sie "Client", um die ACME-URLs zu sehen



3 Beantragung eines Zertifikates

Um ein neues Zertifikat manuell anzufordern, öffnen Sie das Befehlsfenster und geben Sie den folgenden Befehl in den Client ein:

```
sudo certbot certonly -server https://acme.swisssign.ch/v1/ACME-URL/directory -domain
*.dnstesting.xyz -preferred-challenges=dns -manual
```

In diesem Befehl wird die einfachste Art der Beantragung des Zertifikats verwendet.

Parameter Liste:

- **certonly**: nur für das Zertifikat beantragen
- **server**: die SwissSign CA ACME url

- **domain**: Domainname des Servers (Wildcard-Format wird unterstützt)
- **preferred-challenges**: die Authentifizierungsmethode des Besitzes von DNS. Es werden sowohl http als auch dns unterstützt
- **manual**: der Registrierungsprozess wird durchgeführt

In der Produktionsumgebung sollte die Registrierung und Erneuerung von ACME-Zertifikaten idealerweise vollautomatisch erfolgen.

Die Automatisierung umfasst:

1. Automatische Registrierung/Erneuerung
2. Automatische Installation des Zertifikats auf dem Webserver
3. Automatische Ausführung des Pre-Hooked-Skripts und des Post-Hooked-Skripts
4. Automatischer Upload des Verifizierungs-Tokens auf den DNS- (dns-Verifizierung) oder http-Server (http-Verifizierung)

Certbot bietet automatische Möglichkeiten zur Vereinfachung des Prozesses der Zertifikatsausstellung und -aktualisierung.

In der Certbot-Hilfe finden Sie weitere Informationen und Hilfe, um die Vorteile der automatischen Einrichtung besser nutzen zu können.

4 Revokation von Zertifikaten

Listen Sie alle registrierten Zertifikate auf dem Computer auf:

```
sudo certbot certificates
```

Generisch:

Revokation eines Zertifikates:

```
sudo certbot revoke --cert-name example.com --reason keycompromise --server
https://acme.swisssign.ch/v1/ACME-URL/directory
```

5 Konto Verwaltung

ACME verwendet eine und nur eine E-Mail als Kontokontaktinformation. Das Konto kann aktualisiert und deaktiviert werden (Achtung, Konto deaktivieren ist einseitig).
Konto-E-Mail-Update, nur 1 E-Mail wird auf dem Konto aktualisiert.

```
sudo certbot update_account --server https://acme.swisssign.ch/v1/ACME-URL/directory -
m demo@xyz.ch
```

Konto deaktivieren: (https://certbot.eff.org/docs/using.html)