

SwissSign CA

SwissSign AG

Quick Start Guide

Beantragung von ACME-Tokens mit Certbot

Revision

| Rev | Date | Who | Comment |
|------------|-------------|--------------|---|
| 1.0 | 21.06.2022 | SwissSign AG | Initiales Dokument |
| 1.1 | 11.12.2023 | SwissSign AG | Fehlerhafte Referenz bezüglich Wildcard-Zertifikaten und DNS entfernen |
| 1.2 | 04.10.2024 | SwissSign AG | Verweis auf unterstützten Schlüsseltyp zur Ausstellung der Zertifikate hinzufügen |

Inhalte

| | | |
|---|-------------------------------------|---|
| 1 | Einleitung..... | 4 |
| 2 | Setup | 4 |
| 3 | Beantragung eines Zertifikates..... | 4 |
| 4 | Revokation von Zertifikaten | 5 |
| 5 | Konto Verwaltung..... | 5 |

Einleitung

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

Setup

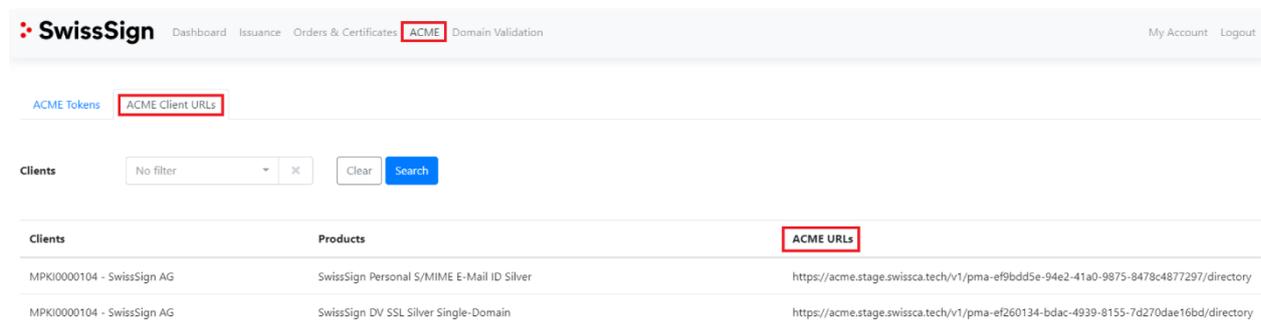
Client Server: Certbot

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 \(https://certbot.eff.org/\)](https://certbot.eff.org/) die Anleitung zur Installation von Certbot

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.swissign.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.swissign.ch/acme/client/urls>)
5. Wählen Sie "Client", um die ACME-URLs zu sehen



The screenshot shows the SwissSign user interface. At the top, there is a navigation bar with 'SwissSign' and several menu items: 'Dashboard', 'Issuance', 'Orders & Certificates', 'ACME', and 'Domain Validation'. The 'ACME' menu item is highlighted with a red box. Below the navigation bar, there are two sub-menus: 'ACME Tokens' and 'ACME Client URLs', with the latter also highlighted by a red box. Under 'ACME Client URLs', there is a search bar with a dropdown menu set to 'No filter', a 'Clear' button, and a 'Search' button. Below the search bar is a table with three columns: 'Clients', 'Products', and 'ACME URLs'. The 'ACME URLs' column is highlighted with a red box. The table contains two rows of data:

| Clients | Products | ACME URLs |
|----------------------------|--|---|
| MPKI0000104 - SwissSign AG | SwissSign Personal S/MIME E-Mail ID Silver | https://acme.stage.swissca.tech/v1/pma-ef9bdd5e-94e2-41a0-9875-8478c4877297/directory |
| MPKI0000104 - SwissSign AG | SwissSign DV SSL Silver Single-Domain | https://acme.stage.swissca.tech/v1/pma-ef260134-bdac-4939-8155-7d270dae16bd/directory |

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.swissign.ch/v1/ACME-URL/directory --domain dnstesting.xyz --key-type rsa --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 URL der SwissSign CA ACME
- **domain:** Domainname des Servers
- **preferred-challenges:** die Authentifizierungsmethode des Besitzes von domain
- **manual:** der Registrierungsprozess wird durchgeführt
- **key-type:** nur rsa unterstützt

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.

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.swissign.ch/v1/ACME-URL/directory
```

Konto Verwaltung

ACME verwendet eine und nur eine E-Mail als Kontaktkontaktinformation. Das Konto kann aktualisiert und deaktiviert werden (Achtung, Konto deaktivieren ist einseitig).

Konto-E-Mail-Update, nur eine E-Mail wird auf dem Konto aktualisiert.

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

Konto deaktivieren: <https://certbot.eff.org/docs/using.html>