SwissSign

SwissSign CA

SwissSign AG

Quick Start Guide

Requesting ACME Tokens with Certbot

Revision

Rev	Date	Who	Comment
1.0	21.06.2022	SwissSign AG	Initial document
1.1	11.12.2023	SwissSign AG	Remove erroneous reference regarding wildcard certificates and DNS
1.2	04.10.2024	SwissSign AG	Add reference to key type supported to issue the certificates

SwissSign

Contents

Introduction

Automated Certificate Management Environment (ACME) protocol automates the certificate issuance of web server certificates. This protocol uses the DNS challenge type to verify the ownership of webservers and domain names.

Setup

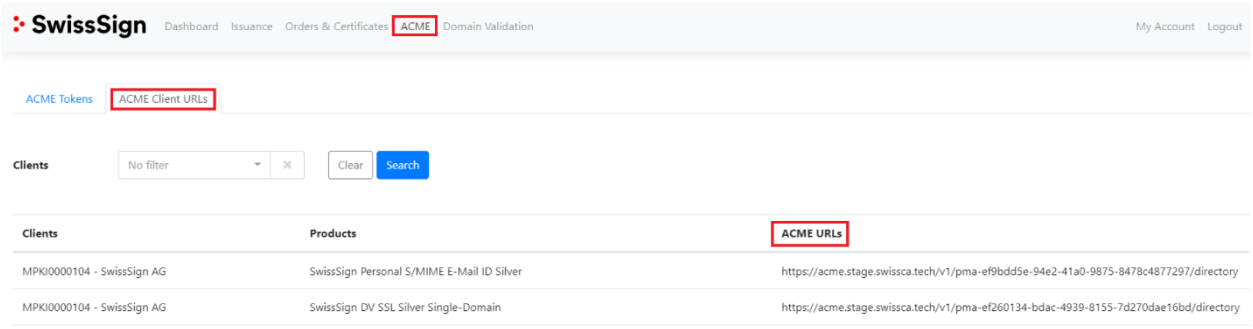
Client Server: Certbot

Certbot or any other ACME client can be used to apply for certificates. If Certbot is not yet setup on your computer, you can find the instructions to install it **here** (**https://certbot.eff.org/**)

For every certbot command, --server parameter MUST be specified to our SwissSign CA ACME mapping address.

SwissSign CA Server Setup step-by-step:

1. Log into https://ra.swisssign.ch
2. Log in with your RA Operator Login
3. Go to the ACME submenu in the top navigation
4. Click on" ACME Client URLs" (https://ra.swisssign.ch/acme/client/urls)
5. Choose "Client" to see the ACME URLs



Request Certificate

To request a new certificate manually, open command window and input the following command in the client:

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

The most basic way to apply for the certificate is used in the command.

Parameter list:

- **certonly**: only apply for the certificate
- **server**: the URL of SwissSign CA ACME
- **domain**: domain name of the server
- **preferred-challenges**: the authentication method of ownership of the domain
- **manual**: the enrollment process will be accomplished
- **key-type**: only rsa is supported

In the production environment, ideally, the ACME certificate enrollment and renewal should be fully automatic.

The automation including:

1. Automatic enrollment/renew
2. Automatic install of the certificate to the webserver
3. Automatic execution of the pre hooked script and post hooked script
4. Automatically upload the verification token to the DNS (dns verification) or http server (http verification)

Certbot provides automatic ways to simplify the certificate issuing and updating process.

Please refer to **Certbot Help** to get more information and get help to better leverage the advantage of automatic setup.

Revocation of Certificates

List all the enrolled certificates on the computer:

```
sudo certbot certificates
```

Generic

Revoke certificate:

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

Account management

ACME uses one and only one email as account contact information. The account can be updated and disabled (warning, account disable is one-way).
Account email update, only one email will be updated to the account.

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

Account disable: https://certbot.eff.org/docs/using.html