



ACME Proxy

- Automated web server certificates
- Connect with private or public CAs
- Central Certificate Database
- Full, auditable control over all certificates
- Interoperable with standard ACME client

Certificates for Web Servers

Interoperable - Automated - Centralized

Web server certificates

The communication between a web browser and a web server is protected by the TLS protocol (former SSL). X.509 certificates are used for the negotiation of session keys. For public web servers, these certificates must be issued by a trusted public CA. For internal servers, certificates from an internal private CA may be used. The lifetime of public TLS certificates, currently one year, decreases more and more and therefore an automated certificate management is required urgently.

ACME

The Automatic Certificate Management Environment (ACME) protocol serves for automating interactions be-

tween certification authorities and web servers. It was designed for the free Let's Encrypt CA service.

A lot of ACME clients exist, that can automatically enroll certificates from Let's Encrypt for standard web servers like Apache, NGINX, TomCat or IIS.

Let's Encrypt or Not?

There are a couple of reasons for an organization to use certificates from a commercial CA under a well defined contract.

Many organizations prefer to use an internal CA, where they have full control over internal server certificates.

On the other hand, when an administrator simply requests certificates directly from Let's Encrypt,

then the organization will loose control over all these certificates

Need for an ACME Proxy

With Secardeo certACME, all server certificates will be requested through this proxy. All certificates will be stored in the central TOPKI certificate database. From here they can be efficiently managed with other tools like Secardeo certLife. This ensures full control over the certificates and auditable certificate management processes.

The certACME proxy connects with public CAs like SwissSign or QuoVadis or an internal Microsoft CA (ADCS). By this, an organization can easily switch from one CA to a different one.



Webserver + ACME Module



SSL Certificate

ACME Proxy



Certification Authority



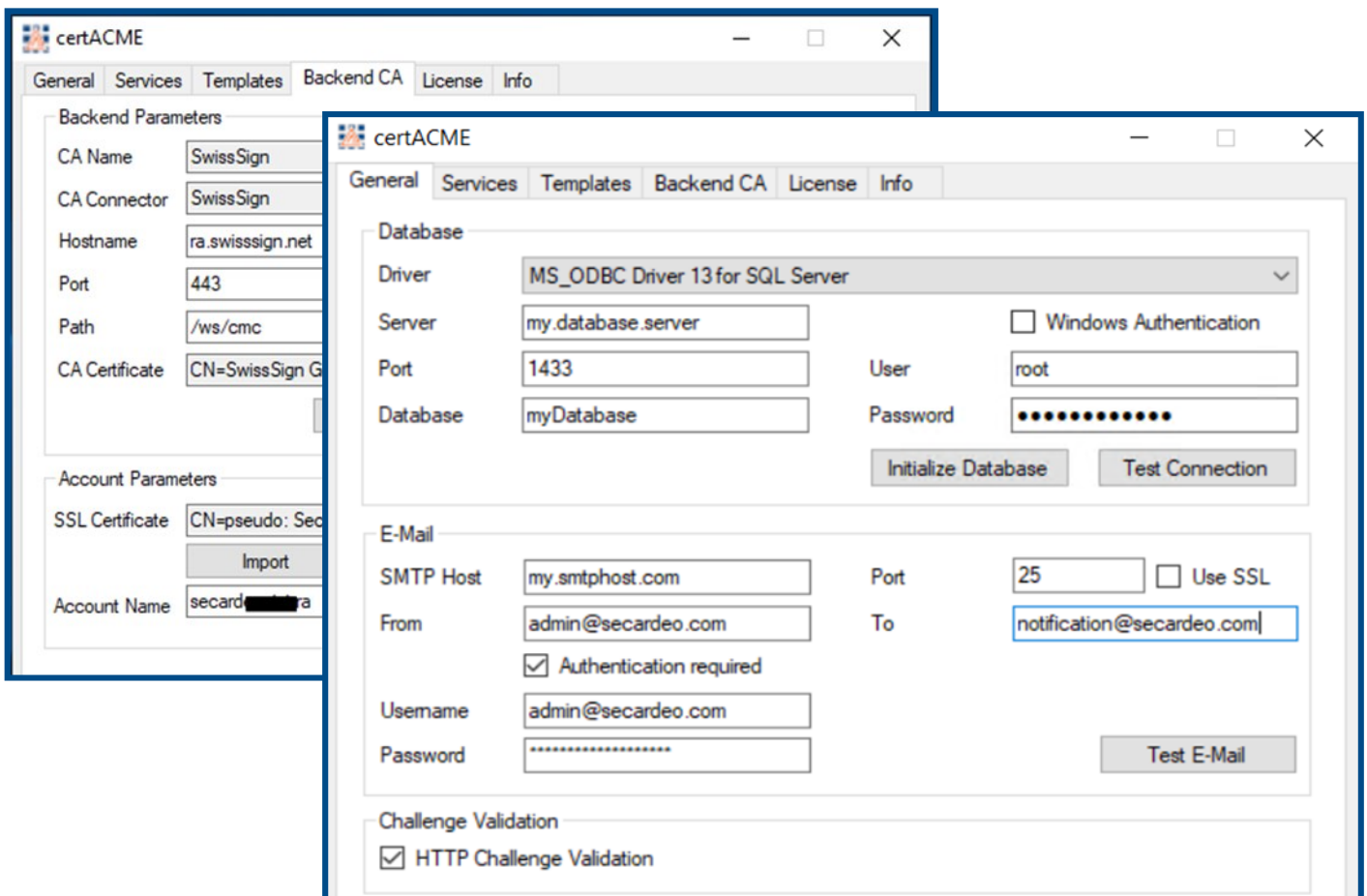
Secardeo GmbH
 Hohenadlstr. 4
 D-85737 Ismaning
 Tel. +49 89 18 93 58 90
 Fax +49 89 18 93 58 99
 info@secardeo.com
 www.secardeo.com

certACME integrates easily as a Microsoft IIS web application and provides the following features:

- Acts as an ACME server for standard ACME clients
- Validates a web server using a HTTP or DNS challenge
- Forwards CSR to a public or private CA
- Optionally enhances CSR with corporate attributes like Organization, Country, OU
- Stores certificates in a local or central SQL database
- Automatically sends configurable notifications to certificate managers and administrators

The certACME Enterprise Edition additionally provides

- Multiple Backend CAs
- Multiple AD Certificate Templates with individual challenge configuration
- Whitelist based domain name authorization
- ACME account management



Operating Systems:

- Windows Server 2016
- Windows Server 2019

SW Requirements:

- MS Internet Information Services v10.0
- .NET Framework 4.7 or higher
- .NET Core 3.1 or higher

Standards:

- X.509 certificates RFC 5280
- PKCS#10 RFC 2986
- ACME v2 RFC 8555

Databases:

- MySQL Server v5.7.14 or higher
- Microsoft SQL Server 2016 or higher
- SQLite3 (local only)

Supported CA-Backends

- SwissSign
- QuoVadis
- MS-CA Web Enrollment
- MS-CA DCOM

Supported ACME Clients:

- Certbot
- Lego
- Acme.sh
- Win-ACME

For further clients please ask us.