SECARDEO

certACME SSL/TLS Autoenrollment

ACME Proxy

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

Certificates for Servers, Clients, Devices

Interoperable - Automated - Centralized

TLS certificates

The communication between a web browser and a web server is protected by the TLS protocol. X.509 certificates are used for proving server authenticity and exchanging encryption keys. Public web servers need trusted certificates from a public CA and internal servers often use a Microsoft CA (ADCS).

ACME

The Automatic Certificate Management Environment (ACME) protocol has been specified for automating interactions between CAs and web servers. It was designed for the free Let's Encrypt CA service. The protocol can also be used to autoenroll certificates to client computers and mobile devices.

The ACME client functionality is either already integrated in systems like Apache or Apple devices or it can be easily added by using free ACME clients.

Internal servers

Many customers are using a Microsoft CA. However, there is no support for ACME from Microsoft. There is also an increasing demand to request certificates for internal servers from free ACME CAs like Let's Encrypt or from commercial PKIs.

Central management

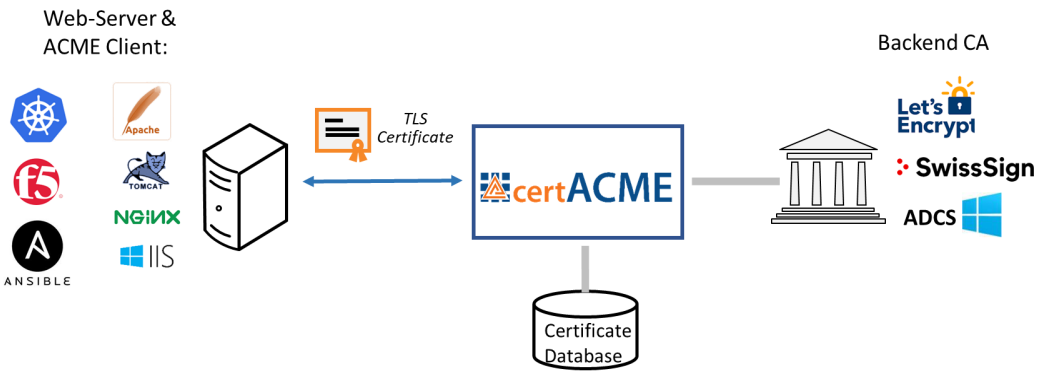
In any ACME scenario, the ability to govern and manage all certificates centrally is crucial!
certACME acts as a proxy between the ACME clients and the connected CAs. All certificates will be stored in the central TOPKI certificate database. Here they can be managed efficiently with tools like Secardeo certLife.

Increased security

In addition to standard ACME validations, certACME offers Whitelisting, EAB AD authorization, ACME acceptance and MDM device lookup.

Integration

certACME enrolls certificates for public or internal web servers like Apache, nginx, TomCat, IIS, Linux clients or even Apple devices. It also serves for Ansible, Kubernetes or F5 systems.
certACME connects with public or private managed CAs or an internal Microsoft CA. By this, you can easily switch from CA to CA.



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

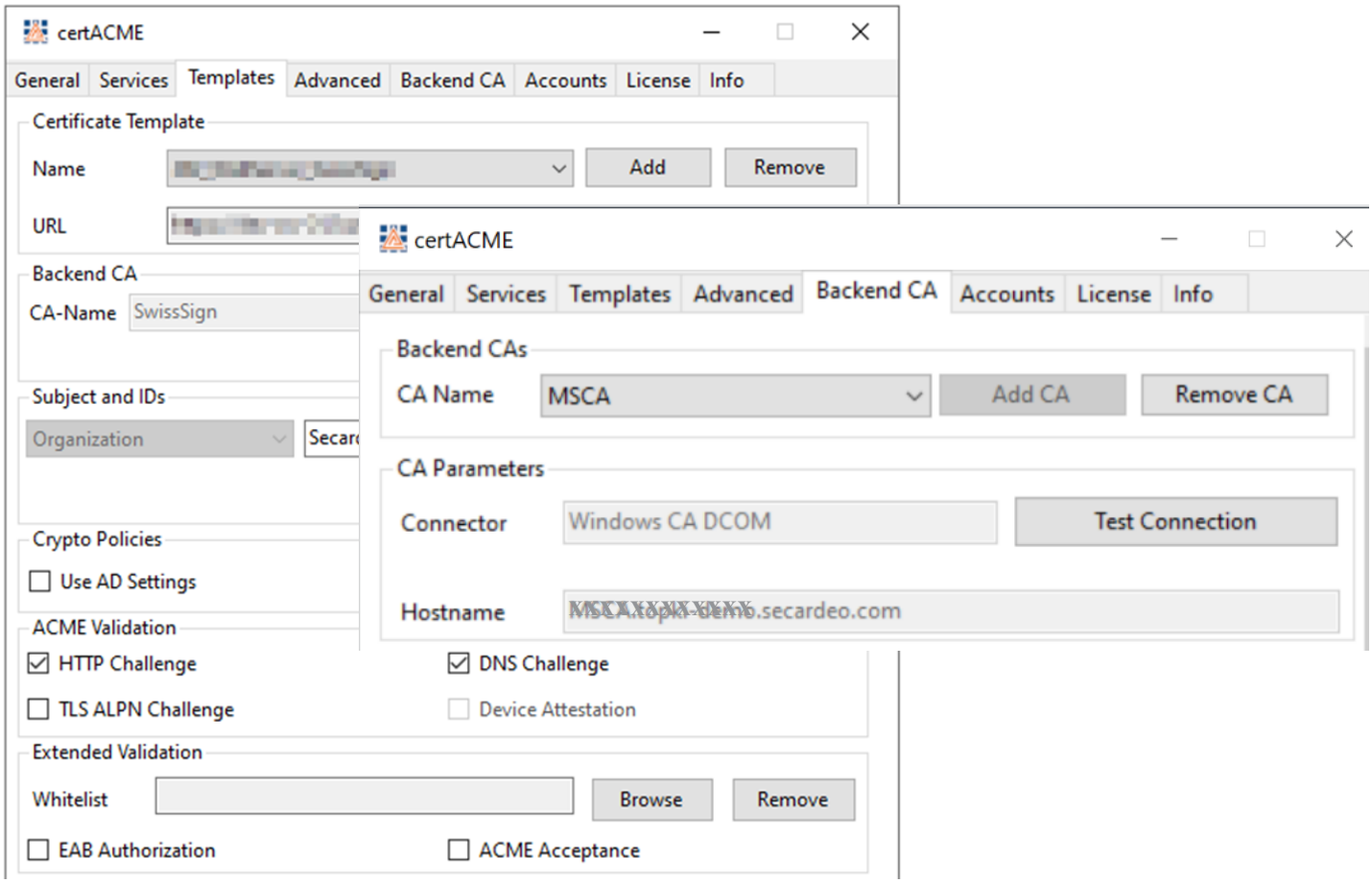
certACME

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

- Acts as an ACME server for standard ACME clients
- Auto-enrolls TLS certificates to internal or external servers from a private or public CA
- Supports common web servers, Kubernetes, Ansible and F5 Big-IP server pools
- Validates a server using ACME HTTP, DNS, TLS-ALPN challenge
- Optionally enhances CSR with corporate attributes like Organization, Country, OU
- Validates crypto policies and stores certificates in a local or central SQL database
- Automatically sends configurable notifications to certificate managers and administrators

certACME Enterprise Edition additionally provides

- Support of AD certificate templates and multiple backend CAs
- Enhanced security by DNS-Whitelisting, name validation + modification rules (RegEx), ACME acceptance or EAB authorization
- Enrollment of device certificates using Apple device attestation and MDM lookup



System Requirements:

- Windows Server 2016-2025
- MS IIS v10
- .NET 8
- Disk Space: 450 MB
- Minimum Memory 4GB
- Minimum Cores 2

Databases:

- MySQL Server v8.0.22 or higher
- Microsoft SQL Server 2016 or higher
- SQLite3 (local only)

Standards:

- X.509 certificates RFC 5280
- PKCS#10 RFC 2986
- ACME v2 RFC 8555
- TLS ALPN RFC 8737
- Device Attestation IETF Draft

Supported ACME Clients:

- acme.sh
- Ansible
- Apache mod_md
- Certbot
- cert-manager
- dehydrated
- lego
- Posh-ACME
- simple-acme
- win-acme

For further clients please ask us.

Supported CA Backends:

- ACME
- ADCS
- DogTag
- EJBCA
- Let's Encrypt
- OpenXPKI
- ZeroSSL
- AWS PCA
- DigiCert
- D-Trust
- GlobalSign
- Microsoft CA
- SwissSign

For further CAs, please ask us.

Supported MDM Systems:

- Microsoft Intune
- MobileIron Core API v2

SECARDEO