SECARDEO

certLife Certificate Management

Certificate Lifecycle Management

- Connects with many public & private CAs
- Extended Management for Microsoft CA
- Central SQL certificate database
- Intuitive web GUI
- Role-based operations
- Active Directory integration
- Windows certificate templates
- User & Administrator self services

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

Certificates for users, servers, devices, ...

Convenient - Automated - Secure

Certificate lifecycle

Organizations today are using a huge number of X.509 certificates for S/MIME, SSL, VPN etc. These certificates have to be managed centrally from their creation to their usage to their expiration.

Management operations

The management of certificates with Secardeo certLife is carried out conveniently via a web browser. It provides an intuitive and powerful search and filter option. Furthermore it offers, for example, generating, approving or denying certificate requests and finding and displaying issued certificates and failed certificate requests. certLife supports different roles with distinct permissions on these management operations. This includes the option for recovering private keys using key recovery agents.
certLife helps you to get track with used TLS certificates and SSH keys by automated or manual discovery in your network.
For monitoring and analysis certLife provides services for statistics and notifications. By this, users or managers can be informed by customizable e-mail notifications about events like certificate expiration or revocation.

Self-service

certLife offers a comfortable certificate self-service for users and server administrators. After login with their aD credentials they can request, renew or revoke certificates and or recover archived keys.

Key pair generation

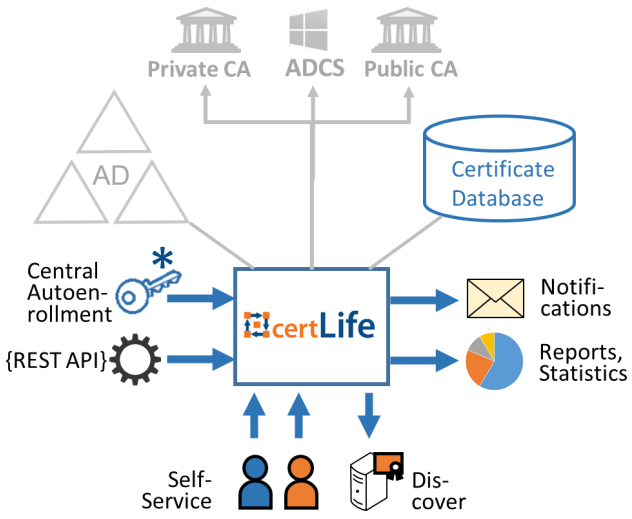
Key pairs and certificate requests (CSR) can be generated on an external machine or inside certLife for administrator self service or for central autoenrollment of user certificates.

Backend CAs

certLife provides connectors for public and private CAs and for Microsoft ADCS.

Integration

certLife integrates seamlessly with Active Directory to read or write data. Full certificate synchronization with a Microsoft CA is possible.
The certLife REST API offers a flexible way to integrate with existing enterprise applications.

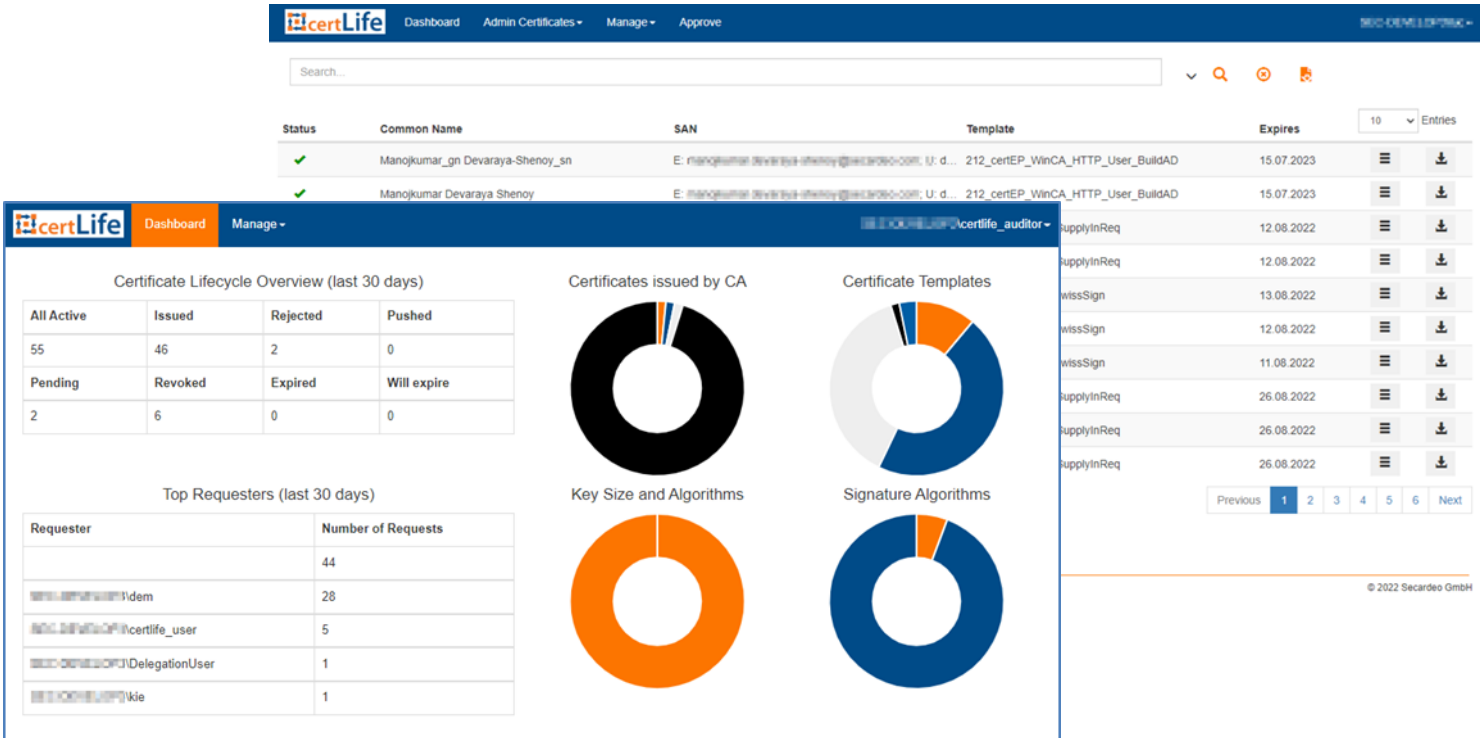


certLife provides an IIS web application and Windows services for managing the certificate lifecycle within the Secardeo TOPKI platform and it provides the following features:

- Convenient management of X.509 certificates and SSH keys via web browser
- Integration with Active Directory and use of Windows certificate templates
- Administration of additional metadata
- Role-based access using AD credentials
- Search, request, approve, revoke, delegate, renew, publish, upload certificates
- Archive and recover private keys
- Self-service for users and administrators
- Client or server based key pair generation and central autoenrollment
- Status notifications
- Reporting and statistics

certLife Enterprise Edition additionally provides

- Support for multiple CAs
- REST API
- Delegation of user and admin certificates
- Group-sharing of server certificates
- Discovery of TLS certificates and SSH keys



Operating Systems:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

SW Requirements:

- MS Internet Information Services v10.0
- .NET Framework 4.8

Machine Requirements:

- Disk Space: 450 MB
- Minimum Memory 4GB
- Minimum Cores 2

Standards:

- X.509 certificates RFC 5280
- PKCS#10 RFC 2986
- PKCS#12

Databases:

- Microsoft SQL Server 2016 or higher
- Azure SQL
- MySQL Server v8 or higher
- SQLite3 (local only)
- Data space 100 KB per certificate

Supported CA Backends:

- AWS ACM PCA
- D-Trust
- DigiCert CertCentral
- DigiCert SymAuth
- Dogtag CA
- EJBCA
- Globalsign Atlas
- Globaltrust
- MTG CARA
- OpenXPKI
- Red Hat Certificate Server
- Sectigo SCM
- SwissSign CMC
- Windows CA DCOM + HTTP

SECARDEO