SECARDEO

certLife Certificate Management

Certificate Lifecycle Management

- Central SQL certificate database
- Intuitive web GUI
- Role-based operations
- Active Directory integration
- Windows certificate templates
- Central or client-side key pair generation
- 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

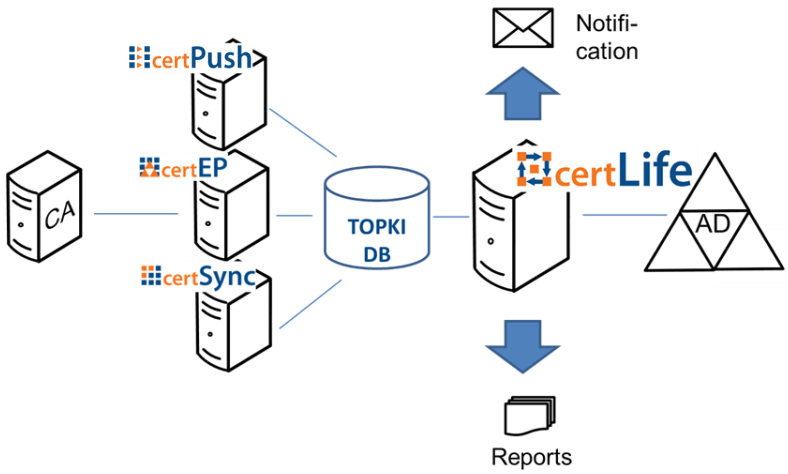
The administration of the certificates of the organization with Secardeo certLife is carried out conveniently and clearly via a web browser. It provides an intuitive and powerful search and filter option. Furthermore it offers, for example, generating, approving or denying certificate requests and finding and displaying issued certificates and failed certificate requests. certLife supports different roles with distinct permissions on these management operations. This includes the option for recovery of private keys using key recovery agent certificates.
For monitoring and evaluating events and certificate status, certLife provides services for Reporting/Statistics and Notifications. By this, certificate owners or managers can be informed by customizable e-mail notifications about events like certificate expiration or revocation.

Key pair generation

In a Windows domain, key pairs are generated on the clients and requests are submitted to certEP. In addition, certLife supports a server-side key-pair generation that can be used manually, e.g. for a user self service, or automatically, e.g. for automatic distribution to mobile devices via Secardeo certPush or certMode.

Integration

certLife is a IIS web application for certificate lifecycle management within the Secardeo TOPKI platform.
In order to fulfill all tasks, certLife interacts with Secardeo certEP and certPush KRS and other TOPKI components. All requests to a CA are sent via certEP by using Windows certificate templates. certLife integrates seamlessly with Active Directory to read or write data.
The certLife REST API offers a flexible way to integrate with existing enterprise applications.

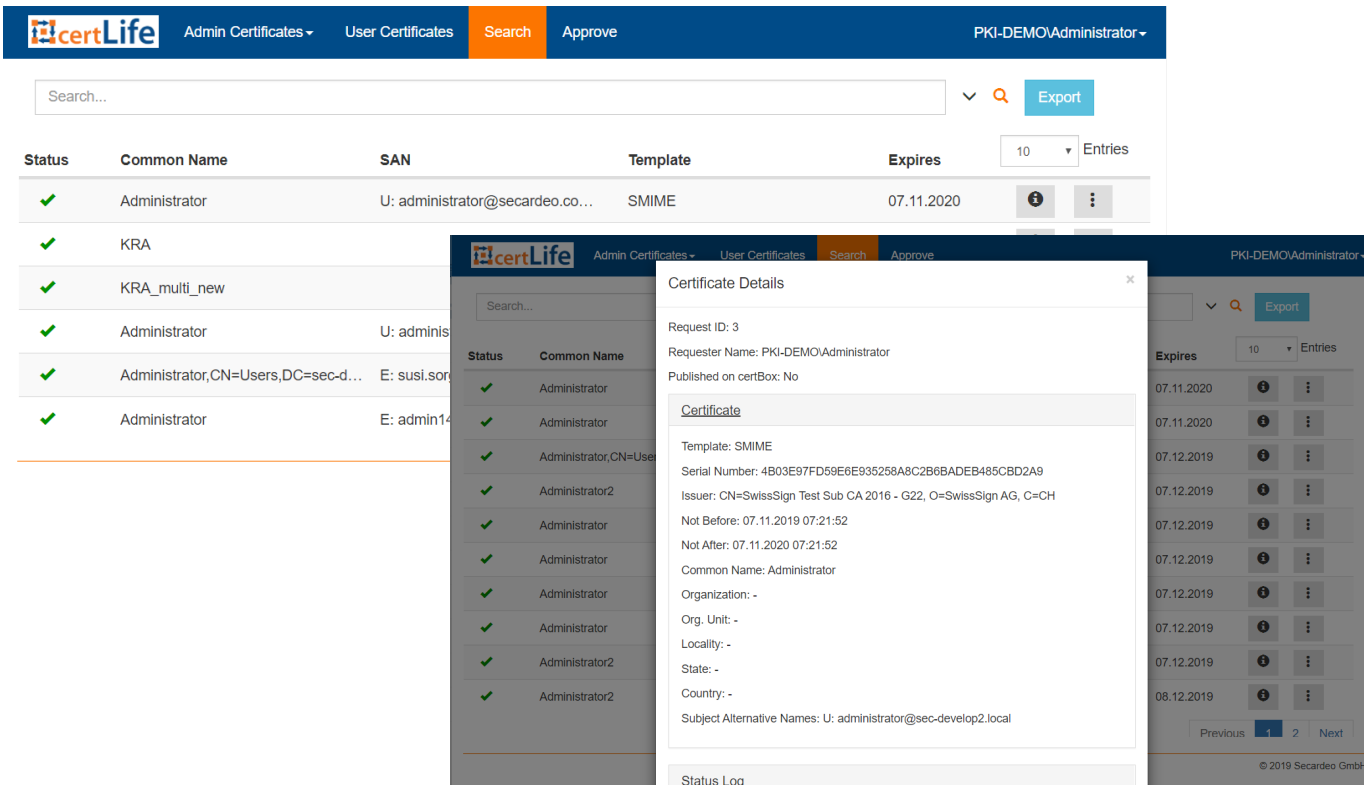


certLife provides an IIS web application and Windows services for managing the certificate lifecycle within the Secardeo TOPKI platform and provides the following features:

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

certLife Enterprise Edition additionally provides

- Support for multiple CAs
- REST API



Operating Systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

SW Requirements:

- MS Internet Information Services v8.5/v10.0
- Secardeo certEP v5 or higher
- Secardeo certPush KRS v3 or higher

Standards:

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

Databases:

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

Supported Web Browsers:

- Internet Explorer 9.0 (or higher)
- Microsoft Edge 40.0 (or higher)
- Mozilla Firefox 52.0 (or higher)
- Google Chrome 59.0 (or higher)

For questions regarding support off further browsers please contact us.