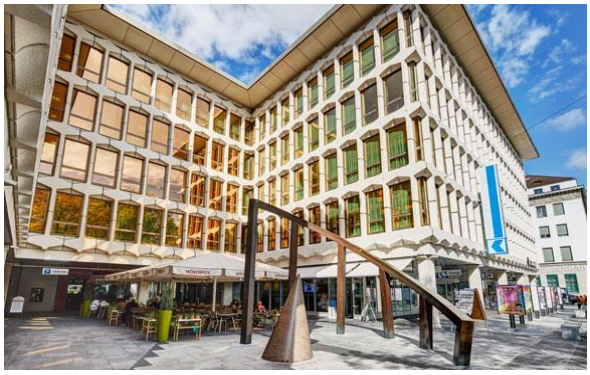
Certificate Management in a Swiss Bank

The Luzerner Kantonalbank relies on the TOPKI solution from SECARDEO for SSL/TLS certificate management.

Luzerner Kantonalbank AG



Founded in 1850, Luzerner Kantonalbank AG (LUKB) has around 1,300 employees and is the leading bank in the canton of Lucerne. As a classic universal bank, LUKB offers all the services of a modern bank. It operates a total of 23 branches and is one of the largest Swiss cantonal banks.

Challenges and goals

LUKB was looking for a solution for the efficient and convenient administration of X.509 certificates. The solution sought should support several public CAS such as SwissSign, QuoVadis/DigiCert and internal CAs such as ADCS.

The focus is on the management of SSL/TLS server certificates.

Requirements

Access control for certificate management is to take place via authorization groups with SSO and Kerberos. Several roles such as owner/requester or examiner/auditor should be supported.

The keys should be generated according to specifications with the option of archiving. Furthermore, the administration of pure RSA keys without certificates for SSH should be supported. The CSR generation should either take place centrally in the manual self-service or by uploading a CSR with subsequent checking option.

The certificate export should be possible in various formats with or without a certificate chain. It should also be possible to import your own certificates or third-party certificates from customers and partners.

The web-based user interface should enable detailed searches for certificate information and display the relevant attributes in a list. It should also be possible to manage additional attributes.

Reminder messages should be sent by e-mail based on configurable parameters, for example before a certificate expires. The solution should offer the possibility of generating reports and displaying log files so that processes can be traced. Furthermore, policies for the 4-eyes principle should be possible for certain certificate types.

The solution

The solution is based on product components from the SECARDEO TOPKI platform. With this several Microsoft CAs (ADCS) as well as public CAs can be connected. The following enrollment scenarios are covered:

- Windows Auto-Enrollment with certEP
- ACME Enrollment via certACME
- Manual Enrollment via Self-Service

> *„With the Secardeo components used, our requirements could be met to our satisfaction. We now have the management of the certificates centrally and thus a complete overview.“*
>
> *Michel Engler*
> *ICT Employee Identity- & Accessmanagement, Luzerner Kantonalbank AG, Luzern*

The certificates are centrally managed via certLife and the recovery of archived keys is done with certPush.

Customer Benefits

With the SECARDEO TOPKI solution, the customer's requirements for a uniform management of the certificates within the certificate life cycle could be fully met. The management of the certificates from a public CA as well as from the internal CA has been significantly simplified using a web-based tool. Many other features, such as automatic notifications, helped to significantly increase the reliability of PKI operation.

All in all, the introduction of the SECARDEO TOPKI solution for the customer resulted in a considerable simplification of the PKI processes through self-services and automation and the associated savings in time and costs.