

Certificate Management in Association of Health Insurance Physicians

KV Hessen relies on the TOPKI solution from Secardeo for the certificate management of SSL certificates.

KASSENÄRZTLICHE
VEREINIGUNG
HESSEN



KV Hessen



The Association of Statutory Health Insurance Physicians of Hesse (KVH) with its headquarters in Frankfurt and its more than 1700 employees ensures medical care by physicians and psychotherapists in private practice in the federal state of Hesse, organizes the medical on-call service (ÄBD) and represents the interests of its members.

Challenges and objectives

The KVH intended to use a certificate management system (CMS) to manage the X.509 certificates used by the KVH. This applies to certificates from an internal Microsoft CA as well as certificates from an external public CA. The focus is on SSL/TLS server certificates.

Requirements

The requirements were defined within the framework of the negotiated award with partial tender "Certificate Management Software" (CMS) of the Association of Statutory Health Insurance Physicians in Hesse.

The issuance of certificates via multiple interfaces based on configurable certificate templates is to be enabled. Authenticated access to the CMS should be possible and certificates should be issued for multiple operating systems. The CMS database is to be managed using MS-SQL. Management in the certificate lifecycle for the creation, revocation and central storage of private keys shall be possible.

The output of reports and the notification of certificate events via e-mail are also to be supported. The protection of confidentiality of the information stored in the CMS and protection against unauthorized modification of the data, including auditability and revision security, is also required.

Another requirement is that an initial connection setup from the perimeter domains into the KVH domain should not be established.

The solution

The solution is based on the certLife and certACME product components of the SECARDEO TOPKI platform. One or more Microsoft CAs (ADCS) and, if required, public CAs can be connected. The following enrollment scenarios are covered:

- Windows manual or autoenrollment
- SCEP Enrollment via NDES
- ACME Enrollment via certACME
- Central Autoenrollment
- Enrollment via REST API
- Manual Enrollment via Self-Service
- Remote Push

„The use of SECARDEO's certificate management products allows us to create certificates more conveniently than before and to have a complete overview of the existing certificates.“

Jan Herold, IT-Infrastructure KV-Hessen

In order to fully meet the requirements, SECARDEO made appropriate adjustments to the standard products.

Customer advantages

The SECARDEO TOPKI solution enables the customer to automate all processes within the certificate lifecycle. On the other hand, the management of certificates from both a public CA and the internal CA has been greatly simplified by a web-based tool.



Many other features such as automatic notifications helped to significantly increase the reliability of PKI operations.

Overall, the introduction of the SECARDEO TOPKI solution brought the customer a significant simplification of the PKI processes through automation and associated time and cost savings.

