cryptas

we protect identities.

CUSTOMER STORY

ENHANCED SECURITY THROUGH PKI MODERNIZATION

HOW THE NATIONAL PARLIAMENT OF AN EU MEMBER STATE MODERNIZED ITS PKI FOR HIGHER SECURITY STANDARDS AND CERTIFICATE AUTOMATION

THE STARTING POINT

The national parliament of an EU member state decided to expand and modify its technical infrastructure. This meant that a renewal of the PKI was also due.

At the time of the PKI modernization, the parliament was already operating a PKI for issuing digital certificates for various computer network and device applications, including IEEE 802.1x based network authentication. However, the planned introduction of a new voice-over-IP system, in particular, required certificate automation protocols that the existing PKI deployment could not handle.

To solve this issue, both an upgrade of the existing PKI to a modern version and a fresh installation of brand-new PKI components were considered. This required not only an appropriate software but also the design and implementation of security-related processes and roles & responsibilities, as well as hardware security.

THE SOLUTION

For the initial roll-out of a suitable PKI solution at the parliament, CRYPTAS deployed a fresh certification authority (CA) based on the latest version of PrimeKey EJBCA as a software appliance protected with an Entrust nShield Connect Hardware Security Module.

Due to the elevated security standards of this newly deployed PKI architecture, it was a challenge to upgrade the existing PKI. Unlike the legacy system, the new PKI is set up with hardware-secured key management, documented CA policies, and strict role-based security management.

Thus, instead of importing the pre-existing keys with a less secure history of origin into the new PKI, a migration strategy was established that is aligned with the life cycle of the certificates: The old PKI's certificates are renewed by the new PKI upon their regular expiry or revocation.

In other words, the legacy PKI remains in operation for the administration of the installed base until all certificates of this PKI have expired and the new PKI system has taken over the chain of trust for all certificates in the organization in its entirety.

At the time of deployment of the modernized PKI system, "high availability" through fully redundant subsystems was not required to protect the computer networks and servers throughout the internal network. Therefore it was not implemented. However, the chosen setup was configured in such a way that it could be easily upgraded to a high-availability configuration for future extensions if required.

THE RESULTS

The new certification authority for the parliament was successfully implemented, at first to protect computer networks and devices, including voice-over-IP endpoints. The focus on standard protocols and automated certificate management resulted in a more robust and scalable system. Automation also enabled shorter certificate life cycles, which is inherently beneficial for enhanced security.

To further enhance security through the online validation of certificates and for future application needs, an expansion of the system to include a high-availability setup is planned. Two identical PKI nodes, each with a dedicated HSM, are to be set up in a distinct network zone, plus a third node for fail-over.