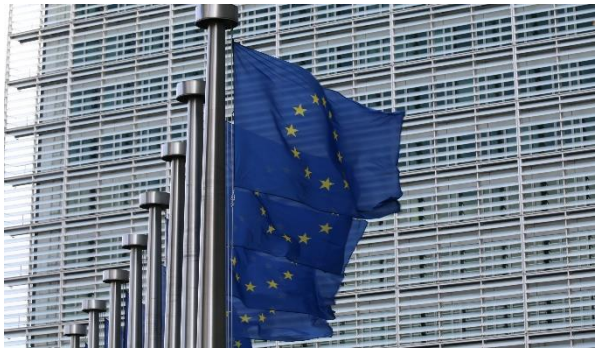
Certificate Management in an EU-Body

An EU Body relies on the TOPKI solution from SECARDEO to automate X.509 certificate management.

Body of the European Union



Our client is one of the bodies serving the administration of the European Union.

Challenges and objectives

The customer operated an internal PKI based on a Microsoft CA. This managed several hundred SSL certificates and over 1,000 S/MIME certificates. The primary need was to streamline operations related to the internal PKI. This means streamlining the management of the certificate lifecycle and automating the issuance and deployment of certificates on both Windows endpoints and mobile devices. Previously, all of these operations relied to a large extent on manual procedures and self-made scripts. Therefore, the customer would like a professional tool that could help to carry out all these activities more efficiently and reliably.

In addition, consideration was given to replacing the internal S/MIME certificates with certificates from a public CA.

Requirements

The main requirement for the certificate management solution is the automation of the entire certificate lifecycle for various certificate types for SSL, S/MIME and device authentication.

Furthermore, in this sense, the ability of such a solution to work with the internal Microsoft CA as well as with an external CA would be an additional added value.

In order to check whether all of these requirements are basically met by the TOPKI solution from SECARDEO, the customer wanted to implement a proof of concept as soon as possible.

The solution

For the proof-of-concept, the required software components were installed at the customer's site by the experts from SECARDEO. At the same time, with the support of SECARDEO, an MPKI agreement was concluded with one of the public CA that are interoperable with TOPKI and an MPKI account of that public CA was set up.

The solution consists of the components certEP for the auto-enrollment of certificates for users and computers in the Active Directory domain, certLife for the central management of all certificates using a web browser, certRevoke for the auto-revocation of orphaned certificates and certPush MDM for the distribution of S/MIME certificates to mobile devices. The certificate database was installed on a Microsoft SQL Server.

> *„TOPKI has been a game changer in the way we managed our PKI and S/MIME certificates. It has allowed us to streamline the operations related to certificate's management, by automating tasks that formerly required human intervention."*
>
> *IT Security Officer*

The PoC was successfully completed after a few weeks with a few adjustments and software updates. The productive system was now set up. Here the TOPKI components were connected with two CA backends, the public CA and the internal Microsoft CA. The configuration of the solution and the AD Certificate Templates, Group Policies as well as the connection to the Mobile Device Management system MobileIron Core was carried out

with competent support from the SECARDEO team.

Customer advantages

On the one hand, the SECARDEO TOPKI solution provided the customer with end-to-end automation of the processes within the certificate lifecycle.

On the other hand, the administration of the certificates from both a public CA and the internal CA has been significantly simplified by a web-based tool. Many other features, such as automatic notifications, helped to significantly increase the reliability of PKI operation.

For the individual user, the use of secure e-mails has become extremely convenient thanks to the automated distribution of certificates and private keys to all devices and is therefore standard.

Overall, the introduction of the SECARDEO TOPKI solution for the customer resulted in a considerable simplification of the PKI processes through automation and the associated time and cost savings.