# S/MIME and SSL certificate distribution for a kitchen manufacturer

Our customer relies on Secardeo's TOPKI solution for the distribution of keys and certificates for the end-to-end encryption of e-mails.

## Our customer

Our customer is a German manufacturer of combi steamers and ovens, cooking appliances suitable for large and commercial kitchens.

## Challenges and goals

At our customer, like in many medium and large sized companies, communication with internal users but also with external partners is massively done by e-mail based on Microsoft Outlook and Exchange and increasingly also with mobile devices. From a perspective of the IT security management at our customer it was not acceptable that internal e-mails could not be kept confidential. For example, a secretary had insight into management documents that are strictly confidential. Furthermore there was an urgent request to send only e-mails that are protected by a digital Signature to external recipients. By this, the external partner can be sure, that the e-mail stems from our customers employee and that the content was not modified.

## Requirements

The Information Security Manager, who is responsible for the project soon understood, that the security requirements can not be fulfilled by a Secure E-Mail Gateway. Especially you cannot achieve a seamless end-to-end encryption by it. Even worse, an automatically generated signature does not assure, that the originator in the e-mail's sender address really has approved its content.

On the other hand the Information Security Manager was aware, that for using S/MIME on the client the key distribution problem has to be solved. Especially for the external communication publicly accepted digital X.509 certificates have to be used so that the recipient may validate the signed e-mails without trouble.

Another important requirement was added: The issuance and renewal of the increasing number of SSL/TLS server certificates should be automated in order to save time and money and to ensure the availability of the servers.

In order to manage the large number of different certificates efficiently and reliably, a solution for Certificate Lifecycle Management should also be introduced.

## The solution

The Information Security Manager soon found the TOPKI solution from Secardeo that provides a fully automated distribution of private keys and accepted certificates from a public Certification Authority (CA).

> *"The challenge of distributing keys is being solved excellently by Secardeo's TOPKI solution"*
>
> *Information Security Manager*

Besides the outstanding functional and security-relevant features he was surprised by the price of the solution that is significantly lower than the price of common Secure E-Mail Gateways – accompanied with a clear added value of functionality.The initial concerns about the complexity of the key management could be overcome during a pilot project that took only a couple of weeks. The solution was then put into operation immediately without any delay.

At our customer the Secardeo certEP, which is integrated with Active Directory, meanwhile provides up to several thousand

# S/MIME and SSL certificate distribution for a kitchen manufacturer

Our customer relies on Secardeo's TOPKI solution for the distribution of keys and certificates for the end-to-end encryption of e-mails.

Windows users with accepted S/MIME certificates from SwissSign by autoenrollment. Private keys of a user are distributed to further (mobile) devices by Secardeo certPush.

In a subsequent step, the Secardeo certACME software for SSL/TLS autoenrollment was introduced. The component has a connection to a public CA from SwissSign as well as to an internal Microsoft CA (ADCS).

The Secardeo certLife component is used for the comprehensive management of S/MIME and SSL certificates.

The Secardeo TOPKI solution has excellently proven for the distribution of keys and it enormously reduces the management efforts by a high-grade reliable automation of the processes.