ecos

Case Study | R. STAHL AG

Case Study

ECOS TrustManagementAppliance

# R. STAHL AG operates PKI

ECOS TrustManagementAppliance is the central public key infrastructure (PKI) at R. Stahl AG

- **Operator:** R.STAHL AG
- **Sector:** Systems & Services
- **Objective:** New PKI for enterprise device management
- **Solution:** Virtually clustered PKI appliance | ECOS TrustManagementAppliance

STAHL

# Security is a top priority for **R. STAHL AG**'s IT network

The globally operating specialist for explosion protection uses a range of certificates to ensure that only known and authorized devices have access to the system.

**Thomas Merkel | Vice President Global IT | R. STAHL AG**
»Compared with the previous solution, the ECOS PKI provides more security and functionality with less effort.«

Security is of utmost priority for the IT network at R. STAHL AG. The global operating specialist for explosion protection ensures through a range of distinct certificates that only known and authorized devices have access.

The migration to the ECOS TrustManagementAppliance led to a central platform for PKI (public key infrastructure) and OTP (one-time password), which is tied to Active Directory. The result: greater security and better functionality, but less effort in maintenance and administration.

### About R. STAHL AG

Explosion protection at the highest level: STAHL's electric and electronic specialty products are worldwide in operation wherever the industry works with flammable substances and the smallest spark could have fatal consequences. From switches and distributors through to lighting or operating and signaling systems, the company provides explosion-proof components and system solutions for the oil and gas industry, the food industry, the chemical and pharmaceutical industry and the shipbuilding industry.

> »A key requirement for the new PKI was the Active Directory synchronization.«
>
> *Thomas Merkel, Vice President Global IT | R. STAHL*

The market-listed company, based in Waldenburg, Baden-Wuerttemberg, holds an internationally leading market position. R. STAHL employs about 1,700 people who work on productions sites in Germany, Norway, India, the USA and the Netherlands. However, R. STAHL's safety focus does not end with their own products. The company also sets highest standards for internal structures and processes to protect employees, systems, data, knowhow and production facilities. This includes issuing certificates to handle the devices operating in the company network. Previously, R. STAHL relied on a standard PKI solution for the issuance, validation and administration of these certificates.

The main problem: Although PCs and notebooks were properly detected, the growing number of various network devices beyond the traditional Windows world, for example phones or mobile end devices, got left out.

### BSI recommendations not achievable with previous solution

Besides this constraint, the previous solution also left a lot to be desired in other areas. For example, the reporting options were insufficient and certificate expiries thus frequently noted very late. The system, set by the manufacturer to be discontinued anyway, did also not allow the shift to the hash algorithm SHA-2.

Since the German Federal Office for Information Security (BSI), whose IT security guidelines R. STAHL follows very closely, strongly recommends this shift, the company finally decided to look for a suitable PKI and implement it. R. STAHL not only wanted a state-of-the-art solution concerning security aspects, but also a solution with the capability to manage certificates for all devices operated within the company.

»An important premise of the new PKI was the synchronization with Active Directory«, explains Thomas Merkel, Vice President Global IT at R.

# Securing the future with PKI and key management – ECOS **TrustManagementAppliance**

An initial market analysis revealed that only a few vendors were qualified to meet the very specific requirements of R. STAHL AG.

STAHL. »Besides, we also wanted this platform to cover the OTP area and thereover manage PKI and OTP combined in one solution with a single, central interface.«

**R. STAHL opts for Trust Management Appliance**

Due to the very specific prerequisites, a first market analysis showed that only few suppliers were qualified to meet all requirements. ECOS Technology's Trust Management Appliance (TMA) proved its worth to the R. STAHL representatives as it allows for the creation, storage, validation and management of all certificates and, if required, symmetric keys and OTP tokens from a single appliance.

As the ECOS TMA connects directly to Active Directory (or any other directory service, if desired), all user and client information can be synchronized, opening the door to extensive automation. After a successful trial, R. STAHL now employs the ECOS PKI solution as virtually clustered appliance, which also grants redundancy. The main application areas are the authentication of devices within the network, the Windows login procedure for users, the two-factor authentication for remote access and the data encryption on data carriers.

**High number of validations per hour**

Every client within the company provided with a certificate: Phones, access point servers, mobile end devices and partly (recent) facilities and machines operating in production. In the whole, R. STAHL manages by now about 8.000 certificates through the ECOS TMA. The traditional computer segment with PCs, notebooks and thin clients alone includes about 2.000 certificates validated for re-authentication at brief and frequent intervals. The PKI appliance thus performs a high, five-digit number of validations per hour.

To grant the greatest possible security level, R.STAHL uses daily updated certificate revocation lists (CRL) to verify the validity of the certificates. The company additionally operates an application-independent OCSP service (online certificate status protocol) to query the ECOS TMA in real-time and thus check whether the respective certificate is valid or not.

Certificates are also used in connection with hard drive and file encryption, as the login to the standards-based encryption of all computers with a local storage is managed by the PKI too. Furthermore, the ECOS TMA provides a unique digital file signature for encrypting single files or folders and thus grant absolute manipulation security. The PKI appliance synchronizes the public keys in the Active Directory for standards-based e-mail encryption (Outlook and S/MIME).

For access security and employee login to the network, R. STAHL employs multicards. The previous access control cards were replaced with smartcards and are now managed by the PKI too. These multicards additionally serve as employee identity card and for time tracking. To meet the individual user preferences, the specialist for explosion protection offers his employees the choice between solutions with card or USB token.

**More security and functionality, less effort**
An integrated reporting feature ensures that e-mail notifications are sent on time before certificates expires. To keep the processes regulating the annual certificate expiry and renewal as lean as possible, R. STAHL plans to launch a self-service portal. This web portal enables staff to reconfigure expired smartcards or synchronize tokens – an important aspect in helping employees avoid unnecessary steps.

»Compared with the previous solution, the ECOS PKI provides more security and functionality with less effort. The system meets all our requirements, is very reliable and failure-free. It also meets our need for a single platform for PKI and OTP, including integration with Active Directory. We are very satisfied with the ECOS solution«, concludes Merkel.

### Case Study – Scenario

**Operator**
R.Stahl AG

**Sector**
Systems and services for explosion protection

**Challenge**
New PKI managing all devices in the company

**Solution**
Virtually clustered PKI appliance for the authentication of devices in the network, Windows user logon process, two-factor authentication for remote access and encryption of data on data carriers.

**About R. STAHL AG**
Explosion protection at the highest level: From switches and distributors through to lighting or operating and signaling systems, the company provides explosion-proof components and system solutions for the oil and gas industry, the food industry, the chemical and pharmaceutical industry and the shipbuilding industry.

ECOS Technology GmbH
Sant' Ambrogio-Ring 13 a-b
55276 Oppenheim Germany

+49 6133 939 200
info@ecos.de

ecos.de