EVIDEN

CASE STUDY

Virtualized smart cards and certificate lifecycle management at a global energy supplier

THE INITIAL SITUATION

A large company in the energy sector operates a public key infrastructure (PKI) that has grown over many years. The certificates from this PKI are used for authentication, encryption, and digital signatures. Accordingly, the PKI plays a central role in many security-critical processes within the company and is deeply integrated into the existing IT landscape.

USB tokens and smart cards are used as key storage devices for users and are integrated into all relevant applications via the Eviden SCinterface middleware.

The processes within the PKI, in particular the issuance, management, and blocking of cards and tokens, were originally run centrally via a card management system (CMS). These processes required a large number of manual interventions and meant that each employee had to pick up their card in person from the IT department.

Over time, the company adapted the processes to meet growing requirements, but did not automate them.

TOKENS AND CARDS:
cumbersome and expensive

Many stakeholders in the company were critical of USB tokens and cards. These had to be personalized, distributed, and later collected again, which administrators and users alike found cumbersome. These processes also hindered mobile working.

In addition, there were costs for the procurement and replacement of tokens and cards, partly due to wear and tear and loss. Processes such as temporary access to a colleague‘s encrypted emails, for example when covering for someone on vacation, could not be implemented. Similar problems arose with the use of group keys and key recovery.

MANUAL PROCESSES:
complex and not user-friendly

The manual processes involved in the certificate lifecycle also proved to be increasingly time-consuming and confusing. Users and administrators increasingly expressed their dissatisfaction with the cumbersome handling of keys and certificates, while support tickets piled up. This resulted in unnecessary operating costs for the company.

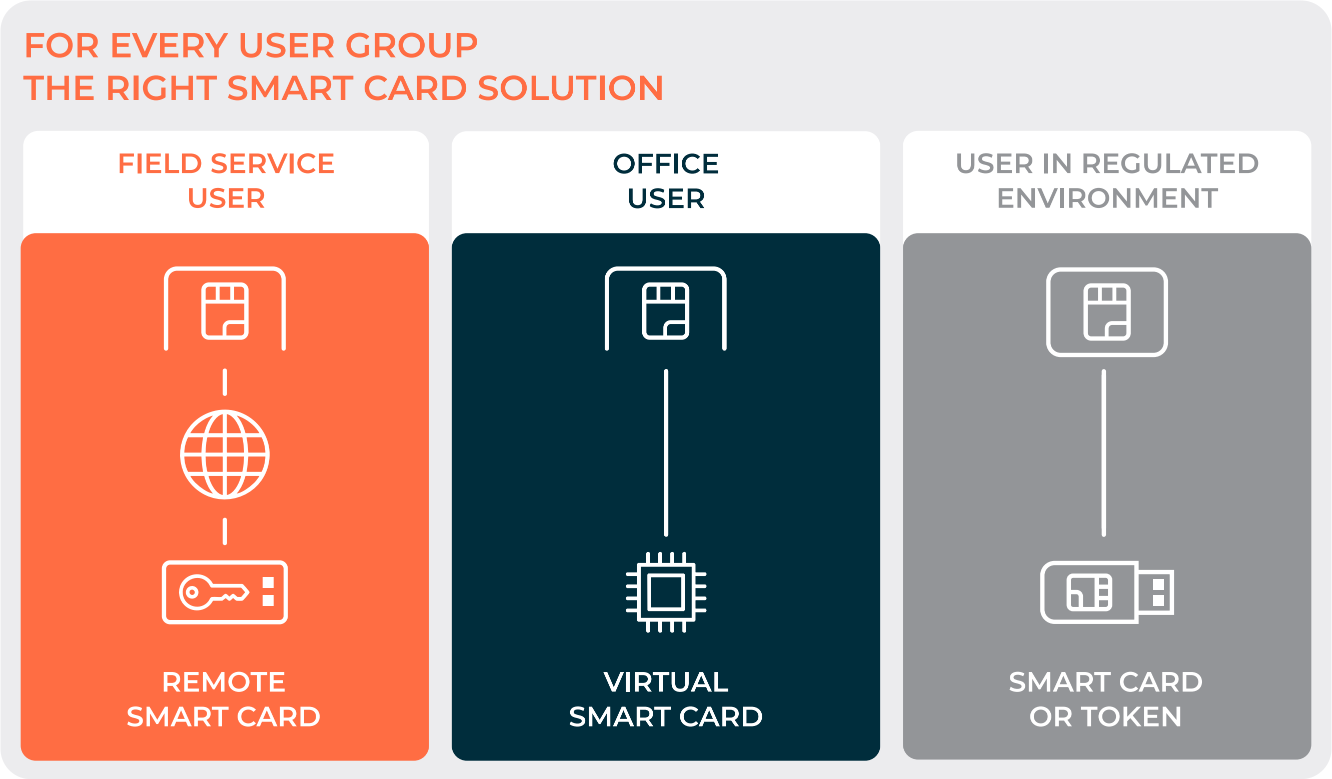
In addition, security risks arose because administrators were unable to keep track of validities and revocations, which led to errors. Auditing the often manual processes was difficult.

THE CHALLENGE

The company recognized the disadvantages mentioned above and, in consultation with Eviden, developed a migration plan for a future-proof, convenient PKI solution. The aim here was to reduce costs and manual effort, achieve a smooth transition from the current to the target state, and increase user satisfaction.

MILESTONE 1
Hardware-free solutions instead
of smart cards and USB tokens

The existing cards and tokens were to be replaced for the majority of users by a solution that did not require any additional hardware on the user‘s part.



FOR EVERY USER GROUP
THE RIGHT SMART CARD SOLUTION

FIELD SERVICE USER

REMOTE SMART CARD

OFFICE USER

VIRTUAL SMART CARD

USER IN REGULATED ENVIRONMENT

SMART CARD OR TOKEN

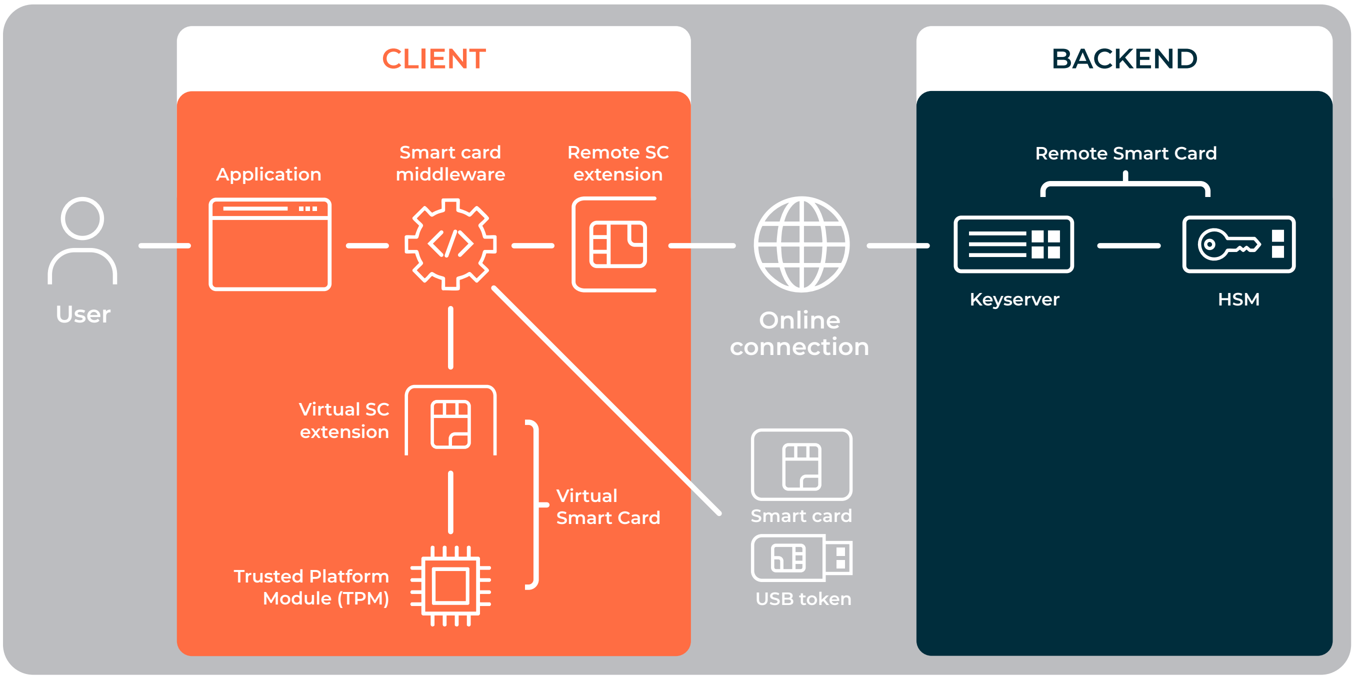
Three user groups were distinguished.

Field service with varying areas of responsibility

Remote Smart Cards were the ideal solution for this user group. These behave like the familiar, classic smart cards/tokens for the user. However, the secret key material is stored centrally on a server to which there is a secure online connection. Users are only authorized to use the key material – the rollout of keys and certificates to individual end devices and their deletion is therefore completely eliminated. This solution allows for the implementation of ad hoc access.

Office users with offline requirements

Virtual Smart Cards proved to be the best solution for users in this group. These are also accessed like a traditional smart card or USB token, but the cryptographic operations take place on the Trusted Platform Module (TPM) of the respective end device. A TPM is a sealed hardware module that stores secret keys and protects them from unauthorized access. TPMs are now built into almost every commercially available PC.



Remote Smart Cards and Virtual Smart Cards do not require a physical card, but instead access a central key server or a TPM.

Users in regulated environments

In addition to the two groups described above, there was a third group for which the smart cards could not be replaced by a hardware-free solution due to legal requirements regarding a second hardware factor.

MILESTONE 2

Automated certificate lifecycle instead of manual processes

The introduction of automated certificate lifecycle management (CLM) offered the greatest leverage in reducing effort and manual errors. The processes that had previously been carried out manually – in particular, enrollment, renewal, revocation, and management of certificates – were to be largely automated. End users would have virtually no involvement in the administration of certificates.

The implementation of these measures was not to result in any restrictions for users in their day-to-day work. Standardized and modular solutions were to be used in order to be able to respond flexibly to future requirements. This included, in particular, the option of converting the PKI to post-quantum cryptography.

The greatest leverage in reducing effort and manual errors came from the introduction of automated certificate lifecycle management (CLM).

THE SOLUTION

The switch to hardware-free smart card alternatives (milestone 1) was implemented first, as the automation of the certificate lifecycle (milestone 2) depends on it.

SWITCH TO HARDWARE-FREE SMART CARD ALTERNATIVES

The existing Eviden SCinterface smart card middleware has been expanded to include a module that enables the use of a central server or a TPM as key storage. This allows existing physical cards and the new Remote and Virtual Smart Cards to be used in parallel without users having to learn how to use new software. Users in high-security areas who still need a physical smart card for regulatory reasons also do not need to make any changes.

The keys are accessed via the Remote and Virtual Smart Card function of SCinterface via PKCS#11 interface or smart card minidriver. Nearly all applications, such as email programs, web browsers, or VPN clients, support one of these two interfaces.

The company decided to use Eviden Keymaster as the key server for the Remote Smart Cards. This server stores the users' private cryptographic keys on a hardware security module (HSM). Mutual authentication between Eviden SCinterface on the end device and the key server is performed using the OAuth protocol. The user authenticates themselves using a PIN or fingerprint, for example. Access to Eviden Keymaster is fully auditable.

The user keys that the Remote Smart Cards access are stored securely on a hardware security module (HSM).

AUTOMATION OF CERTIFICATE LIFECYCLE MANAGEMENT

When introducing certificate lifecycle management, the existing certification authority was retained and expanded to include a PKI management component implemented with the Eviden PKI Workflow Engine. With the Eviden PKI Workflow Engine, the company completely redesigned the enrollment process for users and groups, certificate renewal, and PIN reset, and automated these processes to a large extent. For example, a new certificate is now automatically generated before a certificate expires, ensuring a seamless transition. The user is not involved in this process and simply receives notification that the renewal was successful.

The architecture of the solution is designed to support future cryptographic requirements. Migration to post-quantum cryptography is planned and is scheduled to begin in 2026.

THE RESULT

The previous manual certificate management system resulted in a high volume of support requests, averaging **20,000 support tickets per year**.

With the introduction of the new solution, the ticket volume has been reduced by **80%** to **4,000 tickets per year**.

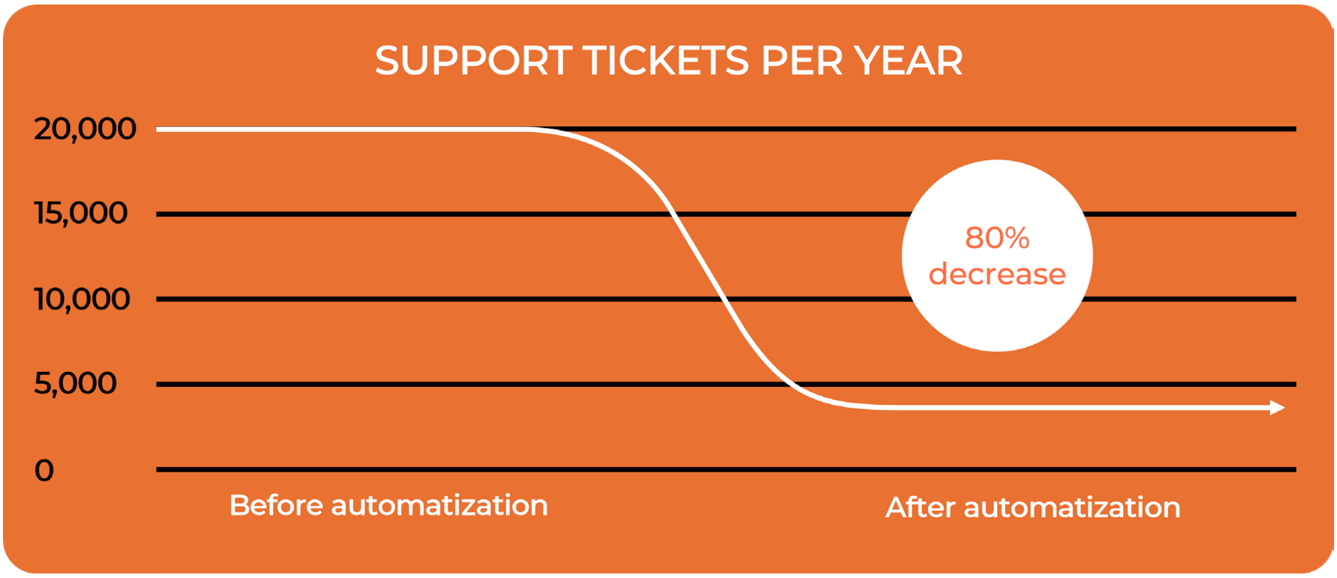
The remaining support requests mainly concern **simple transition or comprehension questions** and do not require in-depth technical effort.

At the same time, initial observations show a **significant improvement in user-friendliness**.

In particular, the newly designed processes for **enrollment** and **certificate renewal** are rated positively by users.

In addition, the **security of the administrative processes** has also been increased.

The **centralization of key management on an HSM-protected key server**, the **standardization of workflows**, and **improved auditability** have contributed significantly to this.



ADDED VALUE
FOR THE ENTERPRISE

✓ USER-FRIENDLY

Users receive their certificates automatically and can use them immediately. There is no longer any need to deal with lost, defective, or forgotten cards.

✓ SECURE

Private keys are managed centrally on an HSM-protected key server and never leave the protected environment. Automated, standardized processes ensure that every user always has a valid certificate that is suitable for the respective application and that cryptographic specifications are consistently enforced.

✓ EASY TO ADMINISTER

Certificates and keys can be generated, renewed, and blocked centrally. There is no need to operate and manage physical cards or USB tokens, which significantly reduces administrative overhead.

✓ EFFICIENT COOPERATION

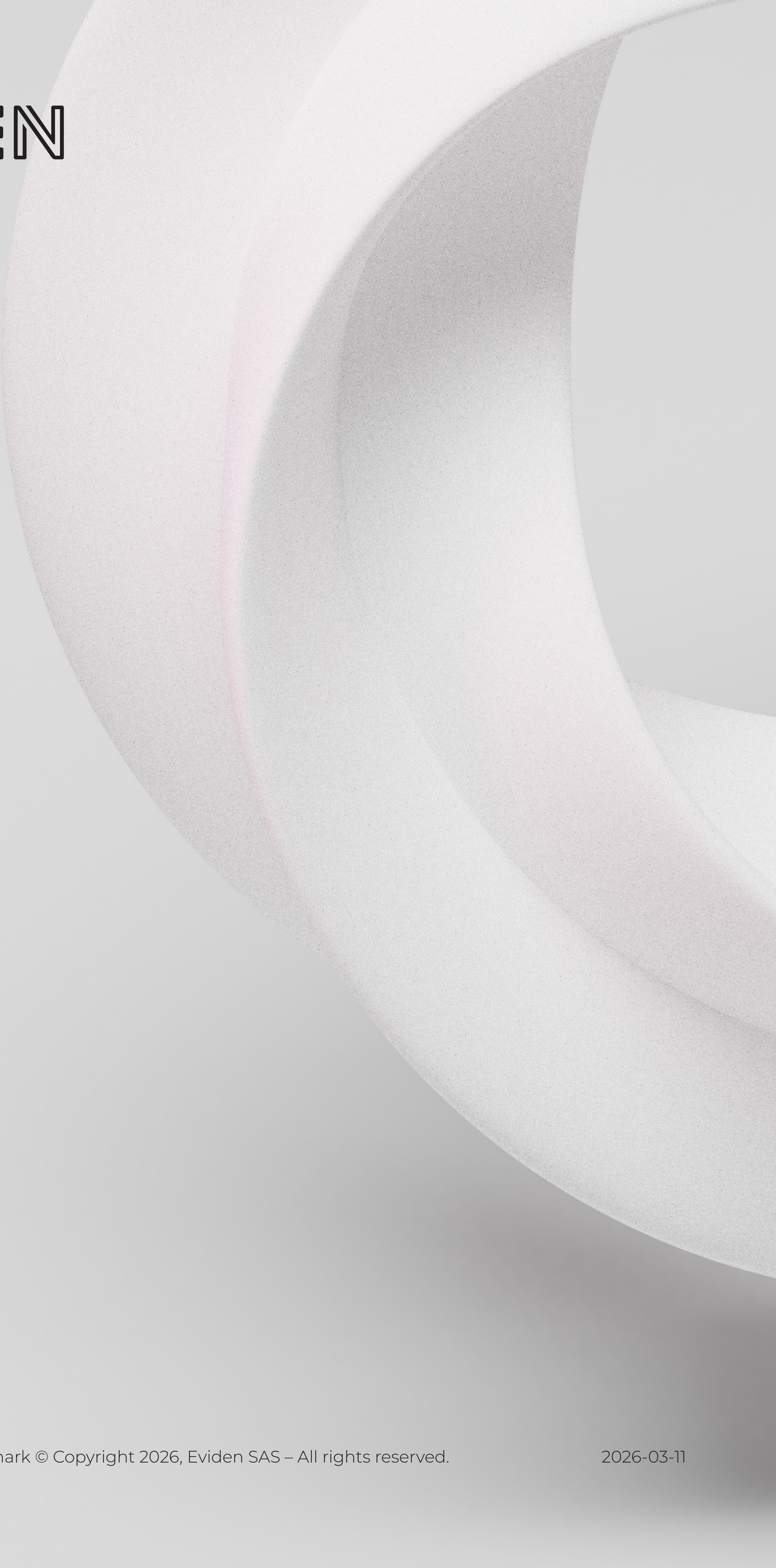
Proxy arrangements and group certificates can be implemented smoothly, as multiple authorized persons are granted access to the same remotely managed private keys. Absences and cross-team processes can be mapped without additional administrative effort.

✓ ECONOMICAL

Automating certificate management reduces operating and support costs in the long term. At the same time, there are no expenses for cards, USB tokens, or their lifecycle management.

✓ FLEXIBLY SCALABLE

Uniform middleware supports Virtual Smart Cards, Remote Smart Cards, classic smart cards, and USB tokens. This allows different usage scenarios to be operated in parallel without system disruption.



Eviden Digital Identity

Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724 - 50
F: +49 209 16724 - 61

Further information:

2026-03-11