EVIDEN

CASE STUDY

Virtualisierte Smartcards und Certificate-Lifecycle-Management bei einem globalen Energieversorger

DIE AUSGANGSSITUATION

Ein Großunternehmen aus der Energiebranche betreibt eine über viele Jahre gewachsene Public-Key-Infrastruktur (PKI). Die Zertifikate aus dieser PKI werden zur Authentifizierung, Verschlüsselung und digitalen Signatur eingesetzt. Dementsprechend spielt die PKI eine zentrale Rolle für viele sicherheitskritische Vorgänge im Unternehmen und ist tief in die bestehende IT-Landschaft integriert.

Als Schlüsselspeicher für die Nutzer kommen USB-Token und Smartcards zum Einsatz, welche über die Middleware Eviden SCinterface in alle relevanten Anwendungen integriert werden.

Die Prozesse innerhalb der PKI, insbesondere die Ausgabe, Verwaltung und Sperrung der Karten und Token, liefen ursprünglich zentral über ein Card Management System (CMS). Diese Vorgänge bedurften einer Vielzahl manueller Eingriffe und erforderten, dass jeder Mitarbeiter seine Karte persönlich in der IT-Abteilung abholen musste.

Das Unternehmen passte die Prozesse im Laufe der Zeit zwar an die wachsenden Anforderungen an, automatisierte sie jedoch nicht.

TOKEN UND KARTEN:
umständlich und teuer

Viele Stakeholder im Unternehmen sahen die USB-Token und Karten kritisch. Diese mussten personalisiert, verteilt und später wieder eingezogen werden, was Administratoren und Anwender gleichermaßen als umständlich empfanden. Diese Vorgänge behinderten zudem das mobile Arbeiten.

Zusätzlich entstanden Kosten für die Beschaffung und den Austausch der Token und Karten, auch bedingt durch deren Verschleiß und Verlust. Vorgänge wie der temporäre Zugriff auf die verschlüsselten E-Mails eines Kollegen, beispielsweise im Rahmen einer Urlaubsvertretung, ließen sich nicht abbilden. Ähnliche Probleme stellten sich bei der Verwendung von Gruppenschlüsseln und Key Recovery.

MANUELLE PROZESSE:
aufwendig und nicht benutzerfreundlich

Auch die manuellen Prozesse rund um den Zertifikats-Lebenszyklus erwiesen sich zunehmend als aufwendig und unübersichtlich. Anwender und Administratoren äußerten vermehrt ihren Unmut über den umständlichen Umgang mit Schlüsseln und Zertifikaten, während sich die Support-Tickets häuften. Für das Unternehmen entstanden unnötige Betriebskosten.

Zusätzlich ergaben sich Sicherheitsrisiken, da die Administratoren kaum noch den Überblick über Gültigkeiten und Sperrungen behalten konnten und dadurch Fehler passierten. Die Auditierung der oft manuell ablaufenden Vorgänge war schwierig.

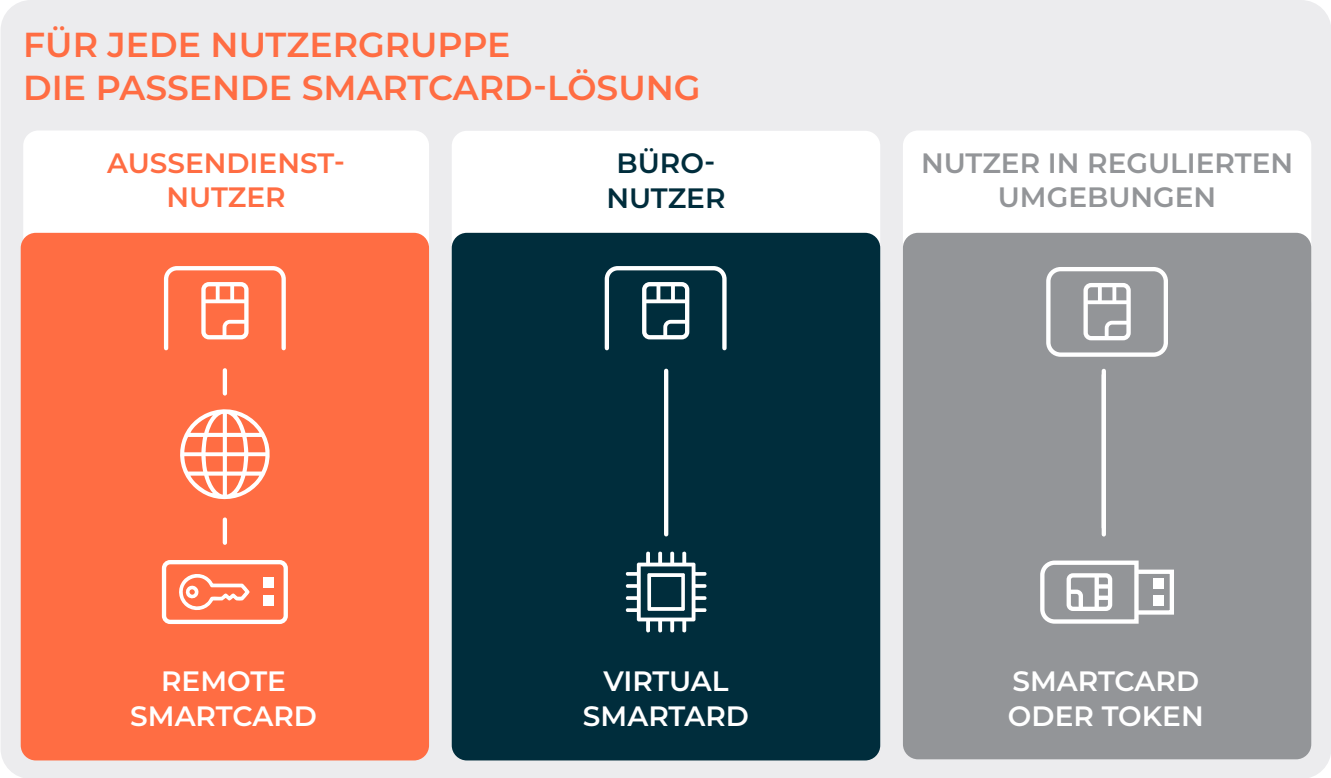
DIE HERAUSFORDERUNG

Das Unternehmen erkannte die genannten Nachteile und erarbeitete in Abstimmung mit Eviden einen Migrationsplan hin zu einer zukunftssicheren, komfortablen PKI-Lösung. Ziel hierbei war es, neben der Reduktion von Kosten und manuellen Aufwänden, einen reibungslosen Übergang vom Ist- zum Soll-Zustand zu erreichen und die Nutzerzufriedenheit zu erhöhen.

MEILENSTEIN 1

Hardwarefreie Lösungen statt Smartcards und USB-Token

Die vorhandenen Karten und Token sollten für einen Großteil der Nutzer durch eine Lösung ersetzt werden, welche völlig ohne zusätzliche Hardware beim Anwender auskam.



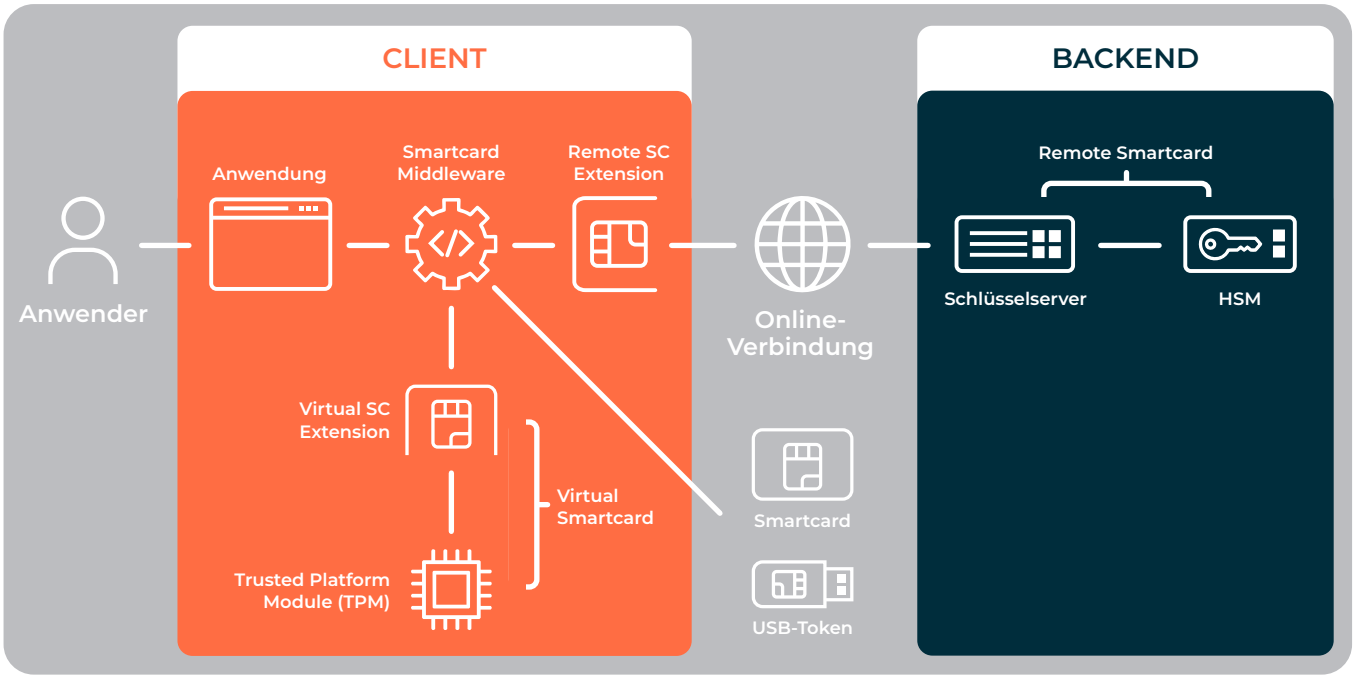
Drei Nutzergruppen wurden unterschieden.

Außendienst mit wechselnden Einsatzbereichen

Für diese Nutzergruppe boten sich **Remote Smartcards** an. Diese verhalten sich beim Anwender wie die bekannten, klassischen Smartcards/Token. Das geheime Schlüsselmaterial wird jedoch zentral auf einem Server verwahrt, zu dem eine sichere Online-Verbindung besteht. Die Anwender werden lediglich berechtigt, das Schlüsselmaterial zu nutzen – der Rollout von Schlüsseln und Zertifikaten an einzelne Endgeräte sowie deren Löschung entfällt somit komplett. Mit dieser Lösung lässt sich ad-hoc Zugriff umsetzen.

Büro-Nutzer mit Offline-Bedarf

Für Anwender aus dieser Gruppe erwiesen sich **Virtual Smartcards** als die beste Lösung. Diese werden ebenfalls wie eine klassische Smartcard oder ein USB-Token angesprochen, die kryptografischen Operationen finden jedoch auf dem Trusted Platform Module (TPM) des jeweiligen Endgeräts statt. Ein TPM ist ein abgeschottetes Hardware-Modul, das geheime Schlüssel speichert und diese vor unbefugtem Zugriff schützt. TPMs sind heutzutage in nahezu jedem handelsüblichen PC fest eingebaut.



Remote Smartcards und Virtual Smartcards benötigen keine physikalische Karte, sondern greifen auf einen zentralen Schlüsselserver oder ein TPM zu.

Nutzer in regulierten Umgebungen

Neben den beiden beschriebenen Gruppen gab es eine dritte, für die die Smartcards aufgrund von gesetzlichen Anforderungen bezüglich eines zweiten Hardware-Faktors nicht durch eine hardwarefreie Lösung ersetzt werden konnten.

MEILENSTEIN 2

Automatisierter Certificate Lifecycle statt manueller Prozesse

Den größten Hebel bei der Reduktion von Aufwänden und manuellen Fehlern bot die Einführung eines automatisierten Certificate-Lifecycle-Managements (CLM). Die bislang manuell durchgeführten Abläufe – insbesondere Enrollment, Erneuerung, Sperrung und Verwaltung von Zertifikaten – sollten dadurch weitgehend automatisiert werden. Die Endnutzenden sollten zur Administration der Zertifikate nahezu keine Berührungspunkte mehr haben.

Für die Nutzer durfte es bei der Umsetzung der genannten Maßnahmen keine Einschränkungen im Arbeitsalltag geben. Es sollten standardisierte und modulare Lösungen zum Einsatz kommen, um auf zukünftige Anforderungen flexibel reagieren zu können. Dies schloss insbesondere die Möglichkeit ein, die PKI auf Post-Quanten-Kryptografie umzustellen.

Den größten Hebel bei der Reduktion von Aufwänden und manuellen Fehlern bot die Einführung eines automatisierten Certificate-Lifecycle-Managements (CLM).

DIE LÖSUNG

Die Umstellung auf hardwarefreie Smartcard-Alternativen (MEILENSTEIN 1) wurde zuerst realisiert, da die Automatisierung des Certificate Lifecycle (MEILENSTEIN 2) davon abhängt.

UMSTELLUNG AUF HARDWAREFREIE SMARTCARD-ALTERNATIVEN

Die vorhandene Smartcard-Middleware Eviden SCinterface wurde um ein Modul erweitert, welches die Nutzung eines zentralen Servers oder eines TPM als Schlüsselspeicher ermöglicht. Dadurch können vorhandene physikalische Karten sowie die neuen Remote und Virtual Smartcards parallel verwendet werden, ohne dass die Anwender den Umgang mit einer neuen Software lernen müssen. Nutzer aus Hochsicherheitsbereichen, die aus regulatorischen Gründen weiterhin parallel eine physikalische Smartcard benötigen, müssen sich ebenfalls nicht umstellen.

Der Zugriff auf die Schlüssel erfolgt über die Remote- und Virtual-Smartcard-Funktion von SCinterface per PKCS#11-Schnittstelle oder Smartcard Minidriver. Nahezu alle Anwendungen wie E-Mail-Programme, Web-Browser oder VPN-Clients unterstützen eine dieser beiden Schnittstellen.

Das Unternehmen entschied sich, Eviden Keymaster als Schlüsselserver für die Remote Smartcards zu nutzen. Die privaten kryptografischen Schlüssel der Anwender werden auf diesem Server gespeichert und sind durch ein Hardware Security Module (HSM) geschützt. Die gegenseitige Authentifizierung zwischen Eviden SCinterface auf dem Endgerät und dem Schlüsselserver erfolgt über das OAuth-Protokoll. Der Anwender authentifiziert sich dabei beispielsweise mittels PIN oder Fingerabdruck. Die Zugriffe auf den Eviden Keymaster sind vollständig auditierbar.

Die Anwenderschlüssel, auf die die Remote Smartcards zugreifen, werden auf einem Hardware Security Module (HSM) sicher gespeichert.

AUTOMATISIERUNG DES CERTIFICATE-LIFECYCLE-MANAGEMENTS

Bei der Einführung des Certificate-Lifecycle-Managements wurde die bestehende Zertifizierungsstelle beibehalten und um eine PKI-Management-Komponente erweitert, die mit dem Produkt Eviden PKI Workflow Engine realisiert ist. Mit der Eviden PKI Workflow Engine gestaltete das Unternehmen das Enrollment für Benutzer und Gruppen, die Zertifikats-Erneuerung sowie den PIN-Reset komplett neu und automatisierte diese Vorgänge weitgehend. Beispielsweise wird jetzt vor Ablauf eines Zertifikats automatisch ein neues generiert, was einen nahtlosen Übergang sicherstellt. Der Anwender wird dabei nicht involviert und erhält lediglich die Information, dass die Erneuerung erfolgreich war.

Die Architektur der Lösung ist darauf ausgelegt, auch zukünftige kryptografische Anforderungen zu unterstützen. Die Migration zur Post-Quanten-Kryptografie ist vorgesehen und soll noch im Jahr 2026 beginnen.

DAS ERGEBNIS

Das zuvor manuelle Zertifikatsmanagement führte zu einem hohen Supportaufkommen von durchschnittlich **20.000 Support-Tickets pro Jahr**.

Mit der Einführung der neuen Lösung konnte das Ticketvolumen um **80 % reduziert** werden – auf **4.000 Tickets jährlich**.

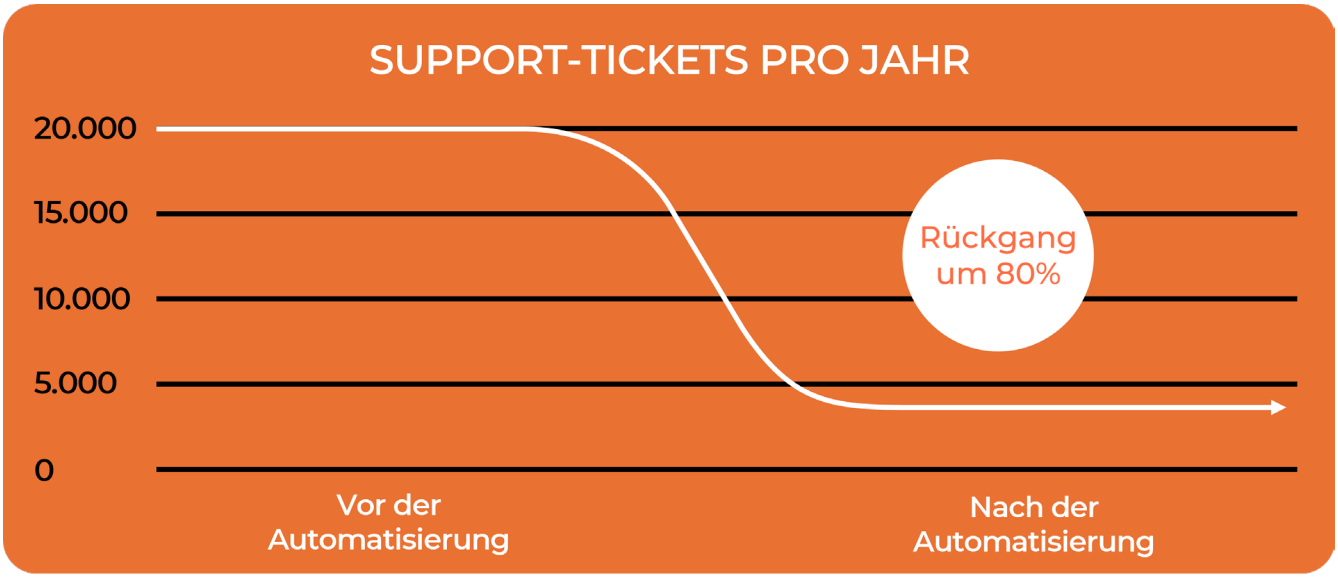
Die verbleibenden Supportanfragen betreffen überwiegend **einfache Umstellungs- oder Verständnisfragen** und erfordern keinen vertieften technischen Aufwand.

Parallel dazu zeigen erste Beobachtungen eine **deutlich verbesserte Benutzerfreundlichkeit.**

Insbesondere die neu gestalteten Prozesse für **Enrollment** und **Zertifikats-Erneuerung** werden von den Anwendern positiv bewertet.

Darüber hinaus konnte auch die **Sicherheit der administrativen Prozesse** erhöht werden.

Maßgeblich dazu beigetragen haben die **Zentralisierung der Schlüsselverwaltung auf einem HSM-geschützten Schlüsselserver,** die **Standardisierung der Workflows** sowie eine **verbesserte Auditierbarkeit.**



MEHRWERT FÜR DAS UNTERNEHMEN

BENUTZERFREUNDLICH

Anwender erhalten ihre Zertifikate automatisiert und sofort nutzbar. Der Umgang mit verlorenen, defekten oder vergessenen Karten entfällt vollständig.

SICHER

Private Schlüssel werden zentral auf einem HSM-geschützten Schlüsselserver verwaltet und verlassen zu keinem Zeitpunkt die geschützte Umgebung. Automatisierte, standardisierte Prozesse stellen sicher, dass jeder Anwender jederzeit über ein gültiges und zum jeweiligen Anwendungsfall passendes Zertifikat verfügt und kryptografische Vorgaben konsistent durchgesetzt werden.

EINFACH ZU ADMINISTRIEREN

Zertifikate und Schlüssel lassen sich zentral erzeugen, erneuern und sperren. Der Betrieb und die Verwaltung physischer Karten oder USB-Token entfallen, wodurch der administrative Aufwand deutlich sinkt.

EFFIZIENTE ZUSAMMENARBEIT

Vertreterregelungen und Gruppenzertifikate lassen sich reibungslos umsetzen, da mehreren berechtigten Personen der Zugriff auf dieselben, remote verwalteten privaten Schlüssel ermöglicht wird. Abwesenheiten und teamübergreifende Prozesse können ohne zusätzlichen administrativen Aufwand abgebildet werden.

WIRTSCHAFTLICH

Die Automatisierung des Zertifikatsmanagements reduziert nachhaltig Betriebs- und Supportkosten. Gleichzeitig entfallen Ausgaben für Karten, USB-Token sowie deren Lifecycle-Management

FLEXIBEL SKALIERBAR

Eine einheitliche Middleware unterstützt Virtual Smartcards, Remote Smartcards sowie klassische Smartcards und USB-Token. Unterschiedliche Nutzungsszenarien können dadurch parallel und ohne Systembruch betrieben werden.

EVIDEN

Eviden Digital Identity

Munscheidstr. 14
D 45886 Gelsenkirchen

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

Weitere Informationen:

2026-02-24