



Globale und sichere Zertifikatsverteilung für alle Umgebungen



DER KUNDE

Ein führender Energiekonzern

Der DXC Technology Endkunde ist eines der weltweit größten privaten Energiekonzerne und konsequent auf die neue Energiewelt mit erneuerbarer und dezentraler Energieerzeugung, Energieeffizienz und digitalen Lösungen ausgerichtet. Der Anspruch ist dabei hoch: Überall dort, wo das Unternehmen aktiv ist, soll die Welt der Energie sauberer und besser werden. Ebenso hoch ist der eigene Anspruch bei der IT-Sicherheit, nicht zuletzt auch durch regulatorische Anforderungen wie das IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen (KRITIS).

DIE AUSGANGSSITUATION

Migration & Kostensenkung

Im Rahmen eines Migrationsprojekts wurden die Weichen für ein neues System für die Ausstellung von digitalen Zertifikaten, einer sogenannten Public Key Infrastruktur (PKI), gestellt. Dabei sollte DXC Technology das bisherige System mit ca. 70.000 Zertifikaten und Smartcards in eine neue, zukunftssichere und flexiblere PKI überführt werden. Fokus war die Flexibilisierung, Standardisierung und Kostensenkung des PKI Betriebs. Kostenintensive zentrale PKI Registrierungsstellen, die zudem räumlich und zeitlich limitiert zur Verfügung standen, sollten eingespart werden.

DIE HERAUSFORDERUNG

Flexible oder sichere Personalisierung?

Für die neuen Anforderungen einer mobilen Arbeitsweise in einem modernen, weltweit agierenden Unternehmen war die bisherige PKI nur begrenzt geeignet. Anstelle aufwändiger zentraler Prozesse sollten Smartcards zukünftig schnell und flexibel im User-Self-Service-Modus durch den Endanwender direkt an seinem Rechner personalisiert werden können. Dabei sind Endanwender-Rechner, auf denen die Personalisierung im User-Self-Service durchgeführt wird, als unsicher einzustufen – besonders ausserhalb des sicheren Unternehmensnetzwerks.

DIE LÖSUNG

cgTunnel

Gemeinsam mit DXC Technology wurde eine moderne PKI Infrastruktur implementiert. Die Endanwender-Zertifikate werden zentral generiert und dezentral ausgegeben. Dabei verwaltet ein zentrales Smartcard-Management-System alle Smartcard-Prozesse wie beispielsweise die Personalisierung, bei der die Zertifikate mit privatem Schlüssel auf die Smartcard gespeichert werden.

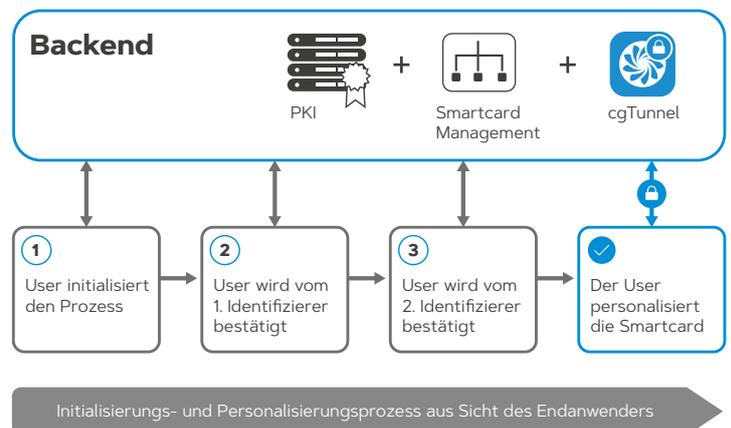
Die patentierte certgate Lösung cgTunnel schützt als zentraler Bestandteil die Verwaltung und Steuerung der Verbindungen zwischen dem Backend und dem Endanwender-Rechner. Ein sicherer Kommunikationstunnel sorgt für den Aufbau einer sicheren Ende-zu-Ende-Verschlüsselung zwischen dem zentralen Smartcard-Management-System über Netzwerke und dem Endanwender-Rechner bis zur Smartcard.

Die Mitarbeiter können nun weltweit, rund um die Uhr Ihre Smartcard innerhalb weniger Minuten selbst personalisieren; völlig unabhängig von Niederlassungen, Homeoffice oder Kundenstandorten. Zuvor war immer eine Reise zu Niederlassungen zu den Öffnungszeiten der jeweiligen PKI Registrierungsstelle erforderlich.

HIGHLIGHTS

- ✓ Initialisierung und Personalisierung von Smartcards im User-Self-Service
- ✓ 70.000 PKI Nutzer
- ✓ Kostensenkung
- ✓ Verbesserte Flexibilität
- ✓ Beschleunigung von Prozessen im Smartcard-Lebenszyklus
- ✓ Erhaltung des aktuellen Sicherheitsniveaus
- ✓ Weltweite Verfügbarkeit 24/7

Bei der Personalisierung werden sensible Informationen, wie das private Schlüsselmaterial elektronischer Zertifikate, vom Backend über Netzwerke und Endanwender-Rechner in die Smartcard des Endanwenders übertragen. Besondere Herausforderung war die sichere Ende-zu-Ende-Verschlüsselung vom Backend bis hin zur Smartcard, um die beiden Ziele Erhöhung der Flexibilität und Einhaltung der Sicherheit zu realisieren. Globale und sichere Zertifikatsverteilung für alle Umgebungen



Der Personalisierungsprozess Ablauf im User-Self-Service

DAS FAZIT

Personalisierung flexibel, sicher und kostengünstig!

Durch den Einsatz von cgTunnel konnte der Endkunde die definierten Projektziele Flexibilisierung und substantielle Kostensenkung bei gleichzeitig hoher Sicherheit erreichen. Teure Reisen der Mitarbeiter zu den PKI Registrierungsstellen werden eingespart und durch einen 24/7 verfügbaren User-Self-Service ersetzt.

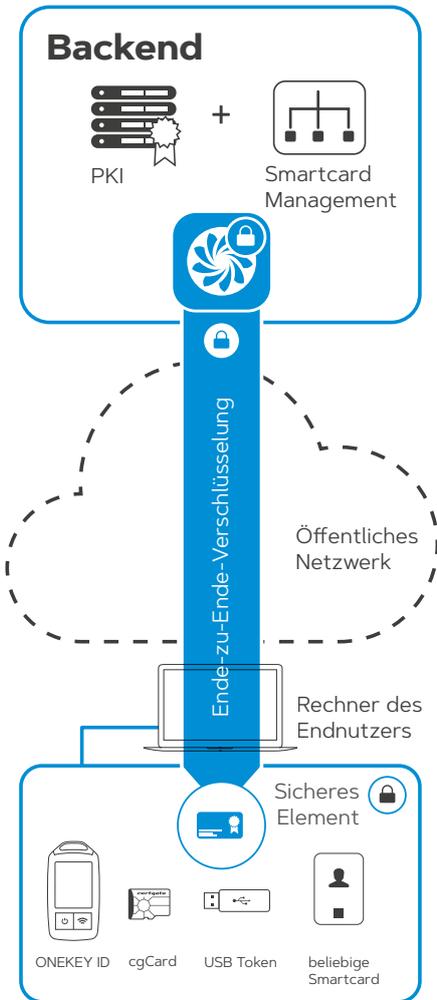
Die Entscheidung für cgTunnel für eine sichere, dezentrale Personalisierung wurde nach der Bewertung von Alternativen getroffen. Das proprietäre Remote Desktop Protocol (RDP) von Microsoft ist deutlich komplexer und verursacht substantiell höhere Lizenzkosten. Bei anderen Konzepten, wie Virtual Private Networks (VPN), oder die verschlüsselten Datenübertragung über Hypertext Transfer Protocol Secure (HTTPS) und Secure Sockets Layer (SSL) fehlen durchgängige Ende-zu-Ende-Verschlüsselungen bis auf die Smartcard.

Die standardisierten Schnittstellen von cgTunnel haben die Systemintegration für DXC Technology vereinfacht. Die hohe Skalierbarkeit von cgTunnel stellt auch die Verfügbarkeit der Gesamtlösung bei nicht planbaren Lastspitzen sicher. Die hohe Flexibilität gewährleistet zusätzlich, dass auch zukünftige Anforderungen wie beispielsweise die Personalisierung auf Smartphones effizient umgesetzt werden können.



cgTunnel

cgTunnel ist eine international patentierte Technologie zur sicheren Übertragung von Zertifikaten und privatem Schlüsselmaterial von einem zentralen System an weltweit verteilte Endgeräte, bzw. deren Smartcards. Alle Daten werden Ende-zu-Ende-verschlüsselt direkt auf die Smartcard des Endnutzers übertragen. cgTunnel ermöglicht sichere, kostengünstige und weltweit skalierbare dezentrale Personalisierung von Smartcards.



Sichere Zertifikatsverteilung mit cgTunnel



„cgTunnel erfüllt zuverlässig und kostengünstig die hohen Anforderungen unserer Kunden bei der sicheren globalen Verteilung von Zertifikaten. certgate betreut Projekte erfolgreich und fristgerecht. Genauso, wie man es erwartet.“

Über certgate

certgate ist einer der führenden IT Security Anbieter für sichere, mobile Kommunikationstechnologien und langjähriges Mitglied der Allianz „IT Security Made in Germany“.

International führende Unternehmen und Behörden, wie die Bundesagentur für Arbeit und staatliche Sicherheitsbehörden im Ausland sichern ihre mobile Kommunikation über certgates patentierte Technologie und Produkte. certgate's Lösungen werden weltweit auch über Partner vertrieben und ermöglichen wirklichen

Schutz vor Hackern, mobile data leakage und nicht autorisierten Zugriff – auch durch staatliche Behörden. Bereits heute schützt certgate nachhaltig weltweit für tausende von Anwendern täglich deren mobile Kommunikation und Daten.

Erfahren Sie noch heute, warum sichere Kommunikation von vielen führenden Experten unbedingt empfohlen wird unter: <https://www.certgate.com/why-encryption>



certgate GmbH
Merianstrasse 26
90409 Nürnberg
Germany

Phone + 49 (0) 911 93 523-0
E-Mail: info@certgate.com

Web: www.certgate.com