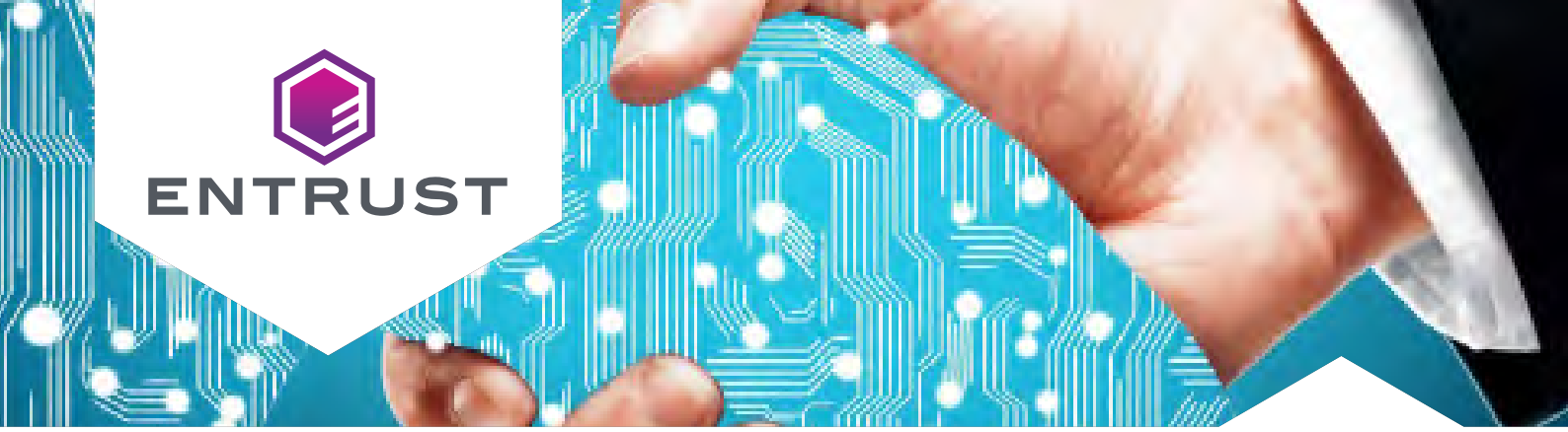

Entrust hilft bei der Sicherung der digitalen Infrastruktur Tunesiens

DIE HERAUSFORDERUNG: DAS WACHSTUM DER TUNESISCHEN DIGITALEN WIRTSCHAFT UNTERSTÜTZEN UND GLEICHZEITIG DEN BÜRGERN SICHERHEIT BIETEN

2015 startete die die tunesische Regierung mit der Umsetzung der „Digitales Tunesien 2020“ Strategie zur Förderung der digitalen Wirtschaft. Dazu gehörte die Erweiterung der elektronischen Behördendienste (E-Government) und der Ausbau von E-Commerce. Für den Erfolg der Initiative war es entscheidend, dass die tunesischen Bürger Vertrauen in öffentliche und private Onlinedienste sowie elektronischen Transaktionen haben. Die National Digital Certification Agency (NDCA), die als Root-Zertifizierungsbehörde in Tunesien agiert und für vertrauenswürdige elektronische Transaktionen steht, nahm als zentrales Projekt der „Digitales Tunesien 2020“ Initiative die Neugestaltung der nationalen Public-Key-Infrastruktur (PKI) als Basis für sichere digitale Transaktionen in Angriff.

Für die erfolgreiche Durchführung des Projekts war ein reibungsloser und schneller Übergang von der bestehenden PKI erforderlich, wobei nach der Implementierung gleichzeitig verbesserte Vertrauensdienste bereitgestellt werden sollten. Darüber hinaus musste die PKI neue strenge Vorschriften für die digitale Zertifizierung erfüllen.

DIE LÖSUNG: NEUE DURCH ENTRUST NSHIELD HSMs GESICHERTE PKI

Die Modernisierung der PKI der tunesischen Regierung erforderte die Installation der besten und aktuellsten Hardware und Software, um die Verfügbarkeit, Zuverlässigkeit und Qualität der Dienste zu verbessern. Um die in der PKI verwendeten Root-Schlüssel zu schützen, benötigte die NDCA eine hardwarebasierte Lösung, da die Verarbeitung sensibler Informationen in reinen Software-Lösungen Risiken birgt.

Tunesische Republik

NDCA entscheidet sich für PrimeKey + Entrust

Um eine optimale Funktion und Sicherheit zu gewährleisten, entschied sich die NDCA für eine Lösung, die zwei entscheidende Komponenten miteinander kombiniert: eine neue PKI von PrimeKey und Hardware-Sicherheitsmodule (HSMs) von Entrust. Hierbei sorgen die Entrust nShield® HSMs für die Sicherheit der PKI, indem sie die privaten Schlüssel der Zertifizierungsbehörde (Certification Authority/CA) während der hochsensiblen Transaktionen hosten und schützen.

Die NDCA nutzt zwei Modelle von Entrust nShield HSMs, um die PKI und Transaktionen zu sichern. Zu letzteren gehören:

- Authentifizierung elektronischer Identitäten von Bürgern, die Business-to-Government-Transaktionen durchführen (B2G)
- Sicherung von Online-Transaktionen einschließlich Online-Steuerzahlungen und -erklärungen, elektronische Einreichung von Zoll- und Außenhandelserklärungen, elektronische Rechnungen und E-Banking-Dienste
- Validierung von Unternehmen, die für Ausschreibungen der Regierung Tunesiens elektronisches Beschaffungssystem TunEPS nutzen
- Erstellen von Unterschriften und Authentifizierungsinformationen, wie biometrische Daten und andere persönliche Identifikationsinformationen (PII), die auf Chips in Dokumenten wie elektronischen Reisepässen (ePass) und elektronischen Personalausweisen (eID-Karte) gespeichert sind.

Das über USB angeschlossene Entrust nShield Edge HSM wird genutzt, um Schlüssel für die Offline-Root-CA zu erzeugen und zu verwalten. Das an das Netzwerk angeschlossene Entrust nShield Connect HSM führt eine Vielzahl von Diensten aus, wie z. B:

- Unterstützung von OCSP-Transaktionen (Online Certificate Status Protocol) zur Erlangung des Zertifikatswiderrufsstatus
- Sicherung von Schlüsseln und Transaktionen unter Verwendung dieser Schlüssel auf dem Signierungsserver der Regierung, der Zertifikate für biometrische und elektronische Informationen ausstellt und signiert, die in Pass- und eID-Chips gespeichert sind.

Die NDCA installierte ihre Entrust nShield HSMs in zwei Rechenzentren, eines für die Produktion und das zweite für Backup und Disaster Recovery.

Neben der Bereitstellung von HSMs und Integrationsunterstützung schulte Entrust auch das technische Team der NDCA, damit die Vorteile der Entrust nShield HSMs voll ausgeschöpft werden können.

Proaktive Zusammenarbeit

Entrust arbeitete direkt mit PrimeKey zusammen und stellte dem Team die Mittel und die Unterstützung zur Verfügung, die es für den Entwurf und das Testen seiner Lösung benötigte. Diese direkte und proaktive Zusammenarbeit trug zum reibungslosen Ablauf des Projekts bei und führte zu einer optimal integrierten Lösung.

Tunesische Republik

ÜBER DIE LÖSUNG

nShield HSM von Entrust

Entrust nShield HSMs bieten eine manipulationssichere Umgebung für die sichere kryptographische Verarbeitung und Schlüsselverwaltung. nShield HSMs sind nach FIPS 140-2 Level 2 und Level 3 und Common Criteria zertifiziert sowie eIDAS-konform. Sie erfüllen etablierte und aufkommende Sicherheitsstandards für kryptographische Systeme und bleiben dabei höchst effizient.

Entrust nShield HSMs isolieren und schützen kryptographische Vorgänge und Schlüssel für die wichtigsten Anwendungen von Unternehmen und führen Verschlüsselung, digitale Signierung und Schlüsselverwaltung für eine breite Palette von Anwendungen durch, darunter PKIs, SSL/TLS und Code Signing. Entrust nShield HSMs bieten hochsichere Lösungen und überlegenen Schutz gegenüber reiner Software-Kryptographie. Entrust nShield HSMs unterstützen alle führenden Algorithmen und bieten eine erstklassige Leistung bei der Transaktionsrate.

Sie kaufen nur die Entrust nShield HSMs und die einzigartige nShield Security World Architektur, die Sie aktuell benötigen. Sollten Ihre Anforderungen zunehmen, können Sie die Kapazität Ihrer Lösung jederzeit anpassen.

Vorteile der Schlüssellösungen von Entrust

- Schutz für kryptographische Schlüssel und Operationen innerhalb manipulationssicherer Hardware, wodurch die Sicherheit gegenüber reinen Software-Lösungen deutlich erhöht wird
- Zertifizierte Lösung – Entrust nShield HSMs sind nach strengen Standards, einschließlich FIPS und Common Criteria, zertifiziert und entsprechen den eIDAS-Standards
- Kontrolle über Ihre Schlüssel und Aufbau von HSM-Systemen, die dank der einzigartigen Architektur der Entrust nShield Security World mit Ihren sich entwickelnden Bedürfnissen skalierbar sind

Tunesische Republik

WARUM ENTRUST?

Entrust HSMs sind FIPS 140-2 Level 2 and 3 und Common Criteria zertifiziert und eIDAS-konform

Entrust nShield HSMs erfüllen die strengen FIPS-, Common Criteria- und eIDAS-Standards, die für das Projekt erforderlich sind. Entrust hat die Common Criteria EAL4+ Zertifizierung für nShield Solo und Connect HSMs von der italienischen Zertifizierungsagentur OCSI erhalten. Gemäß der EU-Richtlinie 1999/93 gewährt diese Zertifizierung Entrust nShield HSMs den Status von SSCD (Secure Signature Creation Devices). Diese Zertifizierung gewährleistet auch die Einhaltung mit der eIDAS-Verordnung von 2014.

Entrust nShield HSMs, eine NCDA-erprobte Lösung

Entrust nShield HSMs wurden bereits in früheren NDCA-Projekten erfolgreich eingesetzt. Da Entrust qualitativ hochwertige Lösungen geliefert hatte und auf die Bedürfnisse der Behörde eingegangen war zögerte die NDCA nicht, Entrust in der hart umkämpften Ausschreibung zur Sicherung der neuen PKI des Landes zu wählen.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com