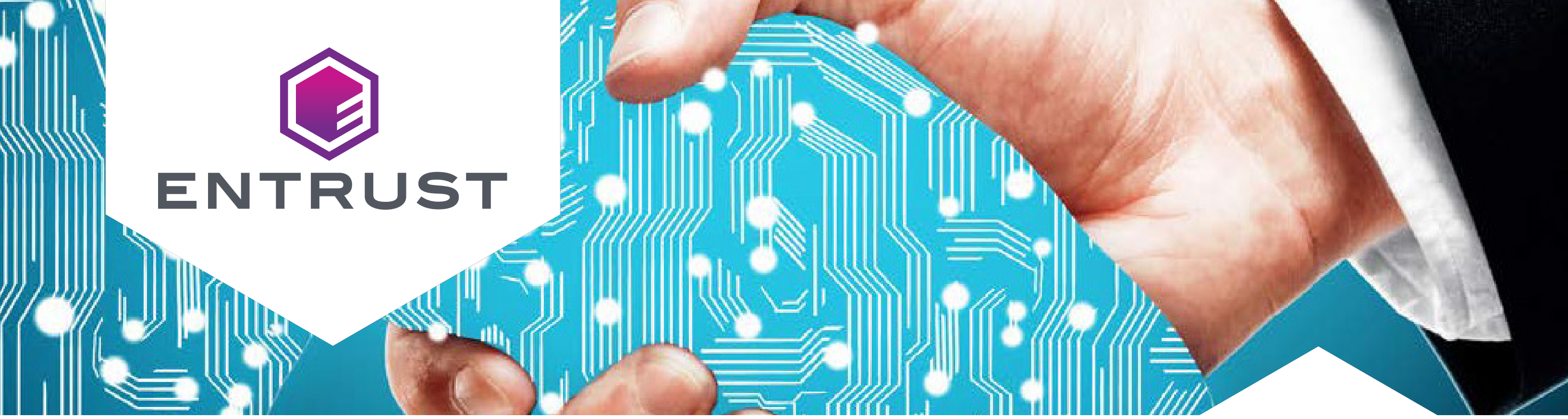

Entrust helps secure Tunisia's digital infrastructure

THE CHALLENGE: HELP TUNISIA GROW ITS DIGITAL ECONOMY WHILE DELIVERING SECURITY TO ITS CITIZENS

In 2015, the Tunisian government launched Digital Tunisia 2020, a plan designed to boost the nation's digital economy by enriching online government services and electronic commerce. Fundamental to the success of the initiative was establishing Tunisia's citizens' trust and confidence in the public and private online services and electronic transactions. The National Digital Certification Agency (NDCA), representing the nation's highest level of trust for electronic transactions, embarked on the cornerstone project of Digital Tunisia 2020 to re-engineer the national public key infrastructure (PKI), that underpins the security of digital transactions.

To succeed, the project would need a smooth and rapid transition from the existing PKI while also providing enhanced trust services once implemented. Additionally, the PKI would need to comply with new stringent regulations for digital certification.

THE SOLUTION: NEW PKI SECURED BY ENTRUST NSHIELD HSMs

Modernizing Tunisia's government PKI would require installing up-to-date, best available hardware and software to improve availability, reliability, and quality of services. To protect the root keys used in the PKI, the NDCA knew it needed a hardware-based solution, as processing sensitive information in software-only solutions exposes it to risk.

Republic of Tunisia

NDCA selects PrimeKey + Entrust

For optimum function and security, the NDCA chose a solution that combined two crucial components: A new PKI from PrimeKey, and hardware security modules (HSMs) from Entrust. Entrust nShield® HSMs would provide security for the PKI by hosting and protecting the private keys of the Certification Authorities (CAs) during the highly sensitive transactions.

The NDCA used two models of Entrust nShield HSMs to secure the PKI and protect transactions including the following:

- Authenticating electronic identities of citizens carrying out and B2G transactions and B2G transactions
- Securing online transactions including online tax payments and returns, electronic submission of customs and foreign trade declarations, electronic invoices, and e-banking services
- Validating companies responding to government Requests for Proposals using Tunisia's on-line e-procurement system, TunEPS
- Creating signatures and authenticating information, such as biometric data and other personal identifying information (PII), stored on chips in documents including e-passports and eID cards

The USB-connected Entrust nShield Edge HSM, is used to generate and manage keys for the offline root CAs. The network-attached Entrust nShield Connect HSM, performs a variety of services such as:

- Supporting Online Certificate Status Protocol (OCSP) transactions to obtain certificate revocation status
- Securing keys and transactions using those keys on the government signing server, which issues and signs certificates for biometric and electronic information stored in passport and eID chips.

The NDCA installed their Entrust nShield HSMs in two datacenters, one for production and the second for back- up and disaster recovery.

In addition to providing HSMs and integration support, Entrust also delivered training to NDCA's technical team on how to take full advantange of their Entrust nShield HSMs.

Proactive collaboration

Entrust took the initiative to work directly with PrimeKey and provided them the assets and support they needed to design and test their solution. This direct and proactive collaboration helped the project run smoothly and resulted in an optimally integrated solution.

Republic of Tunisia

ABOUT THE SOLUTION

Entrust nShield HSMs

Entrust nShield HSMs provide a tamper-resistant environment for secure cryptographic processing and key management. nShield HSMs are FIPS 140-2 Level 2 and Level 3, Common Criteria certified and eIDAS compliant, and meet established and emerging security standards for cryptographic systems while staying highly efficient.

Entrust nShield HSMs isolate and protect cryptographic operations and keys for organizations' most critical applications, and perform encryption, digital signing, and key management for an extensive range of applications including PKIs, SSL/TLS, and code signing. Entrust nShield HSMs provide high-assurance solutions, and superior protection over software-only cryptography.

Entrust nShield HSMs support all leading algorithms and feature world-class transaction rate performance.

With Entrust nShield HSMs and the unique nShield Security World architecture, you buy only the capacity you need and easily scale your solution as your needs evolve.

Entrust key solution benefits

- Protect cryptographic keys and operations within tamper-resistant hardware to significantly enhance security over software-only solutions.
- Trust your certified solution – Entrust nShield HSMs are certified to stringent standards including FIPS and Common Criteria, and are compliant with eIDAS standards.
- Maintain control over your keys and build HSM estates that scale with your evolving needs with the unique Entrust nShield Security World architecture.

LEARN MORE AT ENTRUST.COM/HSM

Republic of Tunisia

WHY ENTRUST?

Entrust HSMs are FIPS 140-2 tLevel 2 and 3 and Common Criteria certified and eIDAS compliant

Entrust nShield HSMs meets the stringent FIPS, Common Criteria, and eIDAS standards required for the project. Entrust has earned Common Criteria EAL4+ certification for nShield Solo and Connect HSMs through the Italian certification agency, OCSI. Under the 1999/93 EU Directive, this certification grants SSCD (Secure Signature Creation Devices) status to Entrust nShield HSMs. This certification also provides compliance with the eIDAS 2014 Regulation.

Entrust nShield HSMs, an NCDA-proven solution

Entrust nShield HSMs had been deployed successfully in previous NDCA projects. Because Entrust had delivered quality solutions and had been responsive to the agency's needs, the NDCA didn't hesitate to select Entrust in the highly competitive bid to secure the nation's new PKI.

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com