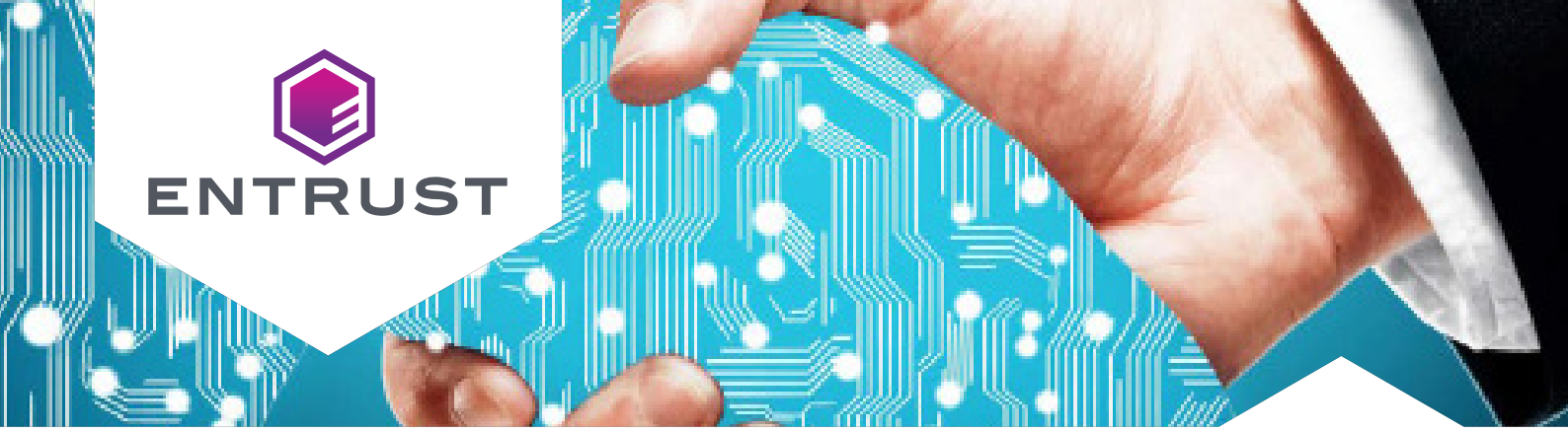

Entrust, 튀니지의 디지털 인프라 보안 강화

과제: 튀니지 디지털 경제 성장을 지원하고 시민에게 보안 제공

2015년, 튀니지 정부는 '디지털 튀니지 2020'이라는 사업에 착수했습니다. 이는 온라인 정부 서비스와 전자 상거래를 확대하여 튀니지의 디지털 경제를 활성화하고자 고안된 계획이었습니다. 디지털 튀니지 이니셔티브를 성공적으로 달성하는 데 필요한 근간은 공공·민간 온라인 서비스와 전자 거래에 대한 튀니지 국민의 신뢰와 확신을 얻는 것이었습니다. 튀니지에서 가장 신뢰받는 전자 거래를 대표하는 국립 디지털 인증 기관, NDCA(National Digital Certification Agency)는 디지털 튀니지 2020의 초석으로 디지털 거래 보안의 토대인 국립 공개 키 인프라(PKI)를 재편하는 프로젝트를 시작했습니다.

프로젝트에서 성공하려면 기존 PKI에서 신속하고 원활하게 전환하는 것이 필요했을 뿐만 아니라, 완성 후에도 신뢰도 높은 서비스를 제공해야 했습니다. 또한, 새로운 PKI는 엄격한 디지털 인증 관련 최신 규정을 준수해야 했습니다.

솔루션: 새로운 PKI에 ENTRUST NSHIELD HSM으로 보안 제공

튀니지 정부의 PKI를 현대화하려면 가장 우수한 최신 하드웨어와 소프트웨어를 설치하여 가용성과 안정성, 서비스 품질을 개선해야 합니다. NDCA는 PKI에 사용하는 루트 키를 보호하려면 하드웨어 기반 솔루션이 필요하다고 판단했습니다. 소프트웨어에 한정된 솔루션으로 민감한 정보를 처리하면 위험에 노출될 수 있기 때문입니다.

튀니지 공화국

NDCA이 선택한 솔루션, PrimeKey + Entrust

최적의 기능과 보안을 위해 NDCA는 두 가지 핵심 요소를 통합한 솔루션을 택했습니다. 바로, PrimeKey의 신규 PKI와 Entrust의 HSM(하드웨어 보안 모듈)입니다. Entrust nShield® HSM는 매우 민감한 거래 처리 과정에서 인증 기관(CA)의 개인 키를 호스팅하고 보호하는 방식으로 PKI에 보안을 제공합니다.

NDCA는 Entrust nShield HSM이 제공하는 두 가지 모델을 사용하여 PKI 보안을 유지하고 다음과 같은 유형의 거래를 보호했습니다.

- 전자 상거래를 진행하는 국민의 전자 신원 인증 및 기업의 B2B, B2G 거래 보호
- 온라인 세금 납부 및 신고, 세관 및 대외 무역 신고서 전자 제출, 전자 송장, 전자 금융 서비스를 포함한 온라인 거래 보안
- 튀니지의 온라인 전자 조달 시스템(TunEPS)으로 정부 입찰 요청에 응하는 기업 검증
- 각종 서류(전자 여권과 전자 신분증 등)의 칩에 저장된 생체 인식 정보와 기타 개인 식별 정보(PII)를 비롯한 서명 및 인증 정보 생성

USB 연결 Entrust nShield Edge HSM은 오프라인 루트 CA의 키를 생성하고 관리하는 데 사용할 수 있습니다. 네트워크에 연결된 Entrust nShield Connect HSM은 다음과 같이 다양한 서비스를 제공합니다.

- OCSP(온라인 인증서 상태 프로토콜) 트랜잭션을 지원하여 인증서 폐기 여부 확인
- 여권과 전자 신분증 칩에 저장된 생체 인식 정보와 전자 정보에 대한 인증서를 발급·서명하는 정부 서명 서버의 키를 사용하여 키와 거래 보안

NDCA는 데이터센터 두 곳에 Entrust nShield HSM을 설치했습니다. 한 곳은 생산 목적, 다른 한 곳은 백업 및 재해 복구 목적이었습니다.

HSM과 통합 지원을 제공하는 것 외에도 Entrust는 NDCA 기술부서에 교육을 제공하여 Entrust nShield HSM 활용 방법을 전수했습니다.

협력 주도

Entrust는 PrimeKey와의 직접적인 협업을 주도하여 PrimeKey사가 솔루션을 설계하고 테스트하는 데 필요한 자산과 지원을 제공했습니다. 직접적이고 적극적인 협업으로 프로젝트를 원활하게 실행할 수 있었을 뿐만 아니라 그 결과, 최적의 통합 솔루션을 제공할 수 있었습니다.

튀니지 공화국

솔루션 소개

Entrust nShield HSM

Entrust nShield HSM은 변조 방지 환경을 제공하여 안전한 암호화 처리와 키 관리가 가능합니다. nShield HSM은 FIPS 140-2 레벨 2 및 레벨 3, CC(공통 평가 기준) 인증, eIDAS 기준을 충족하며, 높은 효율성을 유지하는 동시에 암호화 시스템 관련 기존 보안 표준과 신규 보안 표준 모두를 충족합니다.

Entrust nShield HSM은 기업 핵심 애플리케이션의 암호화 작업과 키를 분리·보호하고 PKI, SSL/TLS, 코드 서명을 포함하는 다양한 애플리케이션의 암호화와 디지털 서명, 키 관리를 수행합니다. Entrust nShield HSM은 소프트웨어에 한정된 암호화보다 뛰어난 보안 기능과 엄격하게 보증하는 솔루션을 제공합니다. Entrust nShield HSM은 모든 주요 알고리즘을 지원하며 세계적인 수준의 처리 속도를 자랑합니다.

Entrust nShield HSM과 nShield 시큐리티 월드의 고유 아키텍처를 이용하면, 필요 용량만 구매해도 추후 요건 변화에 따라 솔루션을 쉽게 확장할 수 있습니다.

Entrust 키 솔루션의 장점

- 변조 방지 하드웨어 내에서 암호키 및 암호화 작업에 보안을 제공하여 소프트웨어 한정 솔루션에 한층 강화된 안전성 제공
- 인증받은 솔루션으로 신뢰 가능 – FIPS, CC 인증을 포함한 엄격한 표준에서 인증받았으며 eIDAS 표준 또한 준수하는 Entrust nShield HSM
- Entrust nShield 시큐리티 월드만의 아키텍처를 이용하여 키에 대한 주도권을 유지하고 변화하는 요건에 따라 확장 가능한 HSM 자산 구축

ENTRUST.COM/HSM에서 자세히 보기

튀니지 공화국

Entrust를 선택해야 하는 이유

FIPS 140-2 레벨 2 및 레벨 3, CC(공통 평가 기준) 인증 및 eIDAS 기준을 충족하는 Entrust HSM

Entrust nShield HSM은 프로젝트에 필요한 FIPS, CC 인증 및 eIDAS 표준 등 엄격한 지침을 충족합니다. Entrust 의 nShield Solo와 Connect HSM은 이탈리아 인증 기관인 OCSI를 통해 공통 평가 기준 EAL4+ 인증을 획득했습니다. 이는 유럽연합 지침 1999/93에 따라, Entrust nShield HSM에 SSCD(보안 서명 생성 장치, Secure Signature Creation Devices) 자격을 부여하는 인증입니다. 이 인증은 eIDAS 2014 규정 또한 준수합니다.

Entrust nShield HSM, NCDA에서 입증한 솔루션

Entrust nShield HSM은 기존 NDCA 프로젝트를 통해 성공적으로 배포되었습니다. 경쟁이 치열한 신규 PKI 입찰에서 NDCA는 양질의 솔루션을 제공하고 기관의 요구에 부응해온 Entrust를 주저 없이 선택했습니다.

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com