



**ENTRUST**

# Entrust ajuda a proteger a infraestrutura digital da Tunísia



## **DESAFIO: AJUDAR A TUNÍSIA A CRESCER SUA ECONOMIA DIGITAL E OFERECER SEGURANÇA PARA SEUS CIDADÃOS**

Em 2015, o governo da Tunísia lançou o Digital Tunisia 2020, um plano destinado a impulsionar a economia digital do país através da melhora dos serviços governamentais online e do comércio eletrônico. Para o sucesso da iniciativa, foi fundamental estabelecer a confiança dos cidadãos tunisinos nos serviços online públicos e privados e nas transações eletrônicas. A National Digital Certification Agency (NDCA), representando o mais alto nível de confiança do país para transações eletrônicas, embarcou no projeto do plano Digital Tunísia 2020 de reestruturação da infraestrutura nacional de chaves públicas (PKI), que sustenta a segurança das transações digitais.

Para ter sucesso, o projeto precisaria de uma transição fácil e rápida da PKI existente, ao mesmo tempo em que forneceria serviços de maior confiança quando implementados. Além disso, a PKI precisaria cumprir as novas e rigorosas leis de certificação digital.

## **SOLUÇÃO: PKI NOVA PROTEGIDA PELOS HSM NSHIELD DA ENTRUST**

A modernização da PKI do governo da Tunísia exigiria a instalação dos melhores e mais modernos hardwares e softwares disponíveis para melhorar a disponibilidade, a confiabilidade e a qualidade dos serviços. Para proteger as chaves básicas utilizadas na PKI, a NDCA sabia que precisava de uma solução baseada em hardware, já que o processamento de informações confidenciais em soluções apenas de software as expõe a riscos.



# República da Tunísia

## NDCA seleciona PrimeKey e Entrust

Para uma função e segurança ideais, a NDCA escolheu uma solução que combinava dois componentes cruciais: uma PKI nova da PrimeKey, e módulos de segurança de hardware (HSM) da Entrust. Os HSM nShield® da Entrust proporcionariam segurança para a PKI hospedando e protegendo as chaves privadas das Autoridades de Certificação (CA) durante transações altamente confidenciais.

A NDCA usou dois modelos de HSM nShield da Entrust para proteger a PKI e as transações, incluindo o seguinte:

- Autenticação das identidades eletrônicas dos cidadãos que realizam transações e transações B2G e B2G
- Proteção das transações online, incluindo pagamentos e declarações de imposto de renda online, apresentação eletrônica de declarações alfandegárias e de comércio exterior, faturas eletrônicas e serviços bancários eletrônicos
- Validação de empresas que respondem a pedidos de propostas do governo usando o sistema de contrato eletrônico online da Tunísia, TunEPS
- Criação de assinaturas e autenticação de informações, como dados biométricos e outras informações de identificação pessoal, armazenadas em chips em documentos, incluindo passaportes e cartões de identidade eletrônicos

O HSM Edge nShield da Entrust conectado por USB, é usado para gerar e gerenciar chaves para autoridades certificadoras offline. O HSM Connect nShield da Entrust ligado à rede realiza diversos serviços, como:

- Suporte para as transações com protocolo de status de certificado online para obter o status de revogação do certificado
- Proteção de chaves e transações usando essas chaves no servidor de assinatura do governo, que emite e assina certificados para informações biométricas e eletrônicas armazenadas em chips de passaporte e identidade eletrônicos.

A NDCA instalou seus HSM nShield Entrust em dois centros de dados, um para produção e o segundo para backup e recuperação de desastres.

Além de fornecer HSM e suporte de integração, a Entrust também fez o treinamento da equipe técnica da NDCA sobre como aproveitar ao máximo seus HSM nShield da Entrust.

## Colaboração proativa

A Entrust tomou a iniciativa de trabalhar diretamente com PrimeKey e oferecer os recursos e o suporte necessários para projetar e testar sua solução. Esta colaboração direta e proativa ajudou o projeto a funcionar sem problemas e resultou em uma solução perfeita e integrada.

# República da Tunísia

## SOBRE A SOLUÇÃO

### HSM nShield da Entrust

Os HSM nShield da Entrust oferecem um ambiente à prova de adulterações para processamento criptográfico seguro e gerenciamento de chaves. Os HSM nShield têm certificados FIPS 140-2 de nível 2 e nível 3 e Common Criteria, estão em conformidades com as normas eIDAS, e atendem aos padrões de segurança estabelecidos e emergentes para sistemas criptográficos, mantendo-se altamente eficientes.

Os HSM nShield da Entrust isolam e protegem operações criptográficas e chaves para as aplicações mais críticas das organizações, e realizam criptografia, assinatura digital e gerenciamento de chaves para uma ampla gama de aplicações incluindo PKIs, SSL/TLS e assinatura de código. Os HSM nShield da Entrust fornecem soluções de alta segurança e proteção superior em relação à criptografia apenas de software.

Os HSM nShield suportam todos os principais algoritmos e apresentam um desempenho de taxa de transação de nível superior.

Com os HSM nShield e a arquitetura exclusiva nShield da Entrust, você adquire apenas a capacidade de que precisa e pode dimensionar sua solução facilmente conforme suas necessidades mudam.

### Principais vantagens da solução da Entrust

- Protege chaves criptográficas e operações em hardware resistente a adulteração para aumentar significativamente a segurança de soluções para apenas software.
- Confiança em sua solução certificada - os HSM nShield da Entrust, são certificados com padrões rigorosos, incluindo FIPS e Common Criteria, e estão em conformidade com as normas eIDAS.
- Para manter o controle de suas chaves e criar conjuntos de HSM de acordo com suas necessidades com a arquitetura Security World nShield da Entrust.





# República da Tunísia

## POR QUE A ENTRUST?

Os HSM da Entrust têm certificados FIPS 140-2 de nível 2 e 3 e Common Criteria e estão em conformidade com as normas eIDAS

Os HSM nShield da Entrust seguem as rigorosas normas FIPS, Common Criteria e eIDAS exigidas para o projeto. A Entrust obteve a certificação Common Criteria EAL4+ para os HSM nShield Solo e HSM Connect através da agência de certificação italiana, OCSI. Sob a Diretiva 1999/93 da UE, esta certificação concede status SSCD (Secure Signature Creation Devices) para os HSM nShield da Entrust. Esta certificação também garante conformidade com as normas eIDAS de 2014.

**HSM nShield da Entrust uma solução de sucesso comprovado pela NDCA**

Os HSM nShield da Entrust já haviam sido instalados com sucesso em projetos anteriores da NDCA. Como a Entrust havia fornecido soluções de qualidade e respondido às necessidades da agência, a NDCA não hesitou em selecionar a empresa na licitação altamente competitiva para garantir uma nova PKI para o país.

## SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.



Saiba mais em

[entrust.com/HSM](https://entrust.com/HSM)



**ENTRUST**