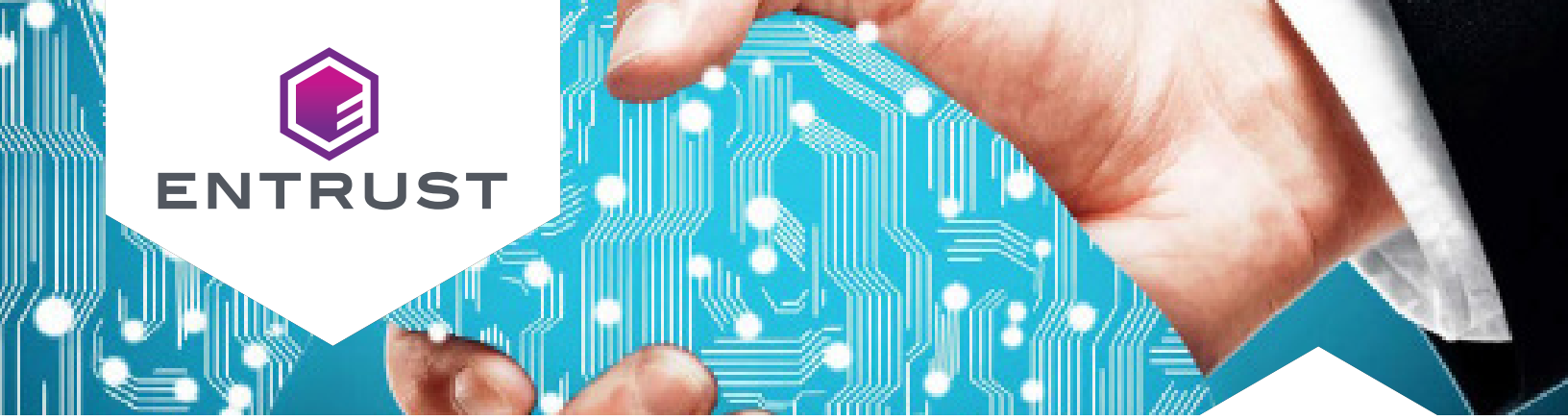

Entrust ayuda a proteger la infraestructura digital de Túnez

EL DESAFÍO: AYUDAR A TÚNEZ EN EL CRECIMIENTO DE SU ECONOMÍA DIGITAL AL BRINDAR SEGURIDAD PARA SUS CIUDADANOS

En 2015, el gobierno de Túnez lanzó Digital Tunisia 2020, un plan diseñado para impulsar la economía digital de la nación al enriquecer los servicios gubernamentales en línea y el comercio electrónico. Para el éxito de la iniciativa fue fundamental el establecimiento de la confianza de los ciudadanos de Túnez en los servicios públicos y privados en línea y en las transacciones electrónicas. La Agencia Nacional de Certificación Digital (NDCA), que representa el nivel más alto de confianza del país para las transacciones electrónicas, se embarcó en el proyecto fundamental de Túnez Digital 2020 para rediseñar la infraestructura de clave pública nacional (PKI), que sustenta la seguridad de las transacciones digitales.

Para tener éxito, el proyecto necesitaría una transición rápida y sin problemas desde la PKI existente, al mismo tiempo que proporcionaría servicios de confianza mejorados una vez implementado. Además, la PKI debería cumplir con las nuevas y estrictas regulaciones para la certificación digital.

LA SOLUCIÓN: NUEVA PKI ASEGURADA POR HSMs NSHIELD DE ENTRUST

La modernización de la PKI del gobierno de Túnez requería instalar el mejor hardware y software actualizado y disponible para mejorar la disponibilidad, confiabilidad y calidad de los servicios. Para proteger las claves raíz utilizadas en la PKI, el NDCA sabía que necesitaba una solución basada en hardware, ya que el procesamiento de información confidencial en soluciones de solo software lo expone a riesgos.

República de Túnez

NDCA selecciona PrimeKey + Entrust

Para una función y seguridad óptimas, la NDCA eligió una solución que combinaba dos componentes cruciales: una nueva PKI de PrimeKey y módulos de seguridad de hardware (HSMs) de Entrust. Los HSMs nShield® de Entrust proporcionarían seguridad para la PKI al alojar y proteger las claves privadas de las Autoridades de Certificación (CA) durante las transacciones altamente confidenciales.

La NDCA utilizó dos modelos de HSMs nShield de Entrust para asegurar la PKI y proteger las transacciones, incluso los siguientes aspectos:

- Autenticar identidades electrónicas de ciudadanos que realizan y transacciones B2G y transacciones B2G
- Asegurar transacciones en línea, lo que incluye pagos y devoluciones de impuestos en línea, presentación electrónica de declaraciones de aduanas y comercio exterior, facturas electrónicas y servicios de banca electrónica
- Validación de empresas que responden a solicitudes de propuestas gubernamentales utilizando el sistema de contratación electrónica en línea de Túnez, TunEPS
- Crear firmas y autenticar información tales como datos biométricos y otra información de identificación personal (PII), almacenada en chips en documentos que incluyen pasaportes electrónicos y tarjetas de identificación electrónica

El HSM nShield Edge de Entrust, conectado por USB, se utiliza para generar y administración claves para las CA raíz fuera de línea. El HSM nShield Connect de Entrust, conectado a la red, realiza una variedad de servicios tales como:

- Admitir transacciones del Protocolo de estado de certificados en línea (OCSP) para obtener el estado de revocación de certificados
- Asegurar claves y transacciones usando esas claves en el servidor de firma del gobierno, que emite y firma certificados para información biométrica y electrónica almacenada en pasaportes y chips de identificación.

El NDCA instaló sus HSMs nShield de Entrust en dos centros de datos, uno para producción y el segundo para respaldo y recuperación ante desastres.

Además de proporcionar los HSMs y el apoyo de integración, Entrust también ofreció capacitación al equipo técnico de NDCA sobre cómo aprovechar al máximo sus HSMs nShield de Entrust.

Colaboración proactiva

Entrust tomó la iniciativa de trabajar directamente con PrimeKey y les proporcionó los activos y el apoyo que necesitaban para diseñar y poner a prueba su solución. Esta colaboración directa y proactiva ayudó a que el proyecto se desarrollara sin problemas y resultó en una solución integrada de forma óptima.

República de Túnez

ACERCA DE LA SOLUCIÓN

HSMs nShield de Entrust

Los HSMs nShield de Entrust proporcionan un entorno a prueba de manipulaciones indebidas para el procesamiento criptográfico seguro y la administración de claves. Los HSMs nShield cuentan con FIPS 140-2 Nivel 2 y Nivel 3, están certificados con Common Criteria y cumplen con eIDAS, además de los estándares de seguridad establecidos y emergentes para sistemas criptográficos, sin dejar de ser altamente eficientes.

Los HSM nShield de Entrust aíslan y protegen las operaciones criptográficas y las claves para las aplicaciones más críticas de las organizaciones. Llevan a cabo el cifrado, la firma digital y la administración de claves para una amplia gama de aplicaciones, incluidas la PKI, SSL/TLS y code signing. Los HSMs nShield de Entrust brindan soluciones de alta seguridad y una protección superior sobre la criptografía de solo software.

Los HSMs nShield de Entrust admiten todos los algoritmos líderes y cuentan con un rendimiento de índice de transacciones de clase mundial.

Con los HSMs nShield de Entrust y la arquitectura única nShield Security World, usted compra solo la capacidad que necesita y escala fácilmente su solución a medida que evolucionan sus necesidades.

Los beneficios clave de la solución Entrust

- Protección para claves criptográficas y operaciones en un hardware a prueba de manipulaciones indebidas para mejorar significativamente la seguridad sobre las soluciones de solo software.
- Confiar en su solución certificada: los HSMs nShield de Entrust están certificados según estrictos estándares, incluidos FIPS y Common Criteria, y cumplen con los estándares eIDAS.
- Mantenga el control sobre sus claves y cree propiedades HSM que se adapten a sus necesidades cambiantes con la arquitectura única nShield Security World de Entrust.

APRENDA MÁS EN ENTRUST.COM/HSM

República de Túnez

¿POR QUÉ ENTRUST?

Los HSMs de Entrust tienen la certificación FIPS 140-2 Nivel 2 y 3 y Common Criteria y cumplen con eIDAS

Los HSMs nShield de Entrust cumplen con los estrictos estándares FIPS, Common Criteria y eIDAS requeridos para el proyecto. Entrust ha obtenido la certificación Common Criteria EAL4+ para HSMs nShield Solo y Connect a través de la agencia de certificación italiana OCSI. Según la Directiva de la UE 1999/93, esta certificación otorga el estado SSCD (Dispositivos de creación de firmas seguras) a los HSMs nShield de Entrust. Esta certificación también proporciona el cumplimiento del Reglamento eIDAS 2014.

Los HSMs nShield de Entrust, una solución comprobada por NCDA

Los HSMs nShield de Entrust se habían implementado con éxito en proyectos anteriores de NDCA. Debido a que Entrust había brindado soluciones de calidad y había respondido a las necesidades de la agencia, la NDCA no dudó en seleccionar a Entrust de entre la oferta altamente competitiva, para asegurar la nueva PKI de la nación.

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com