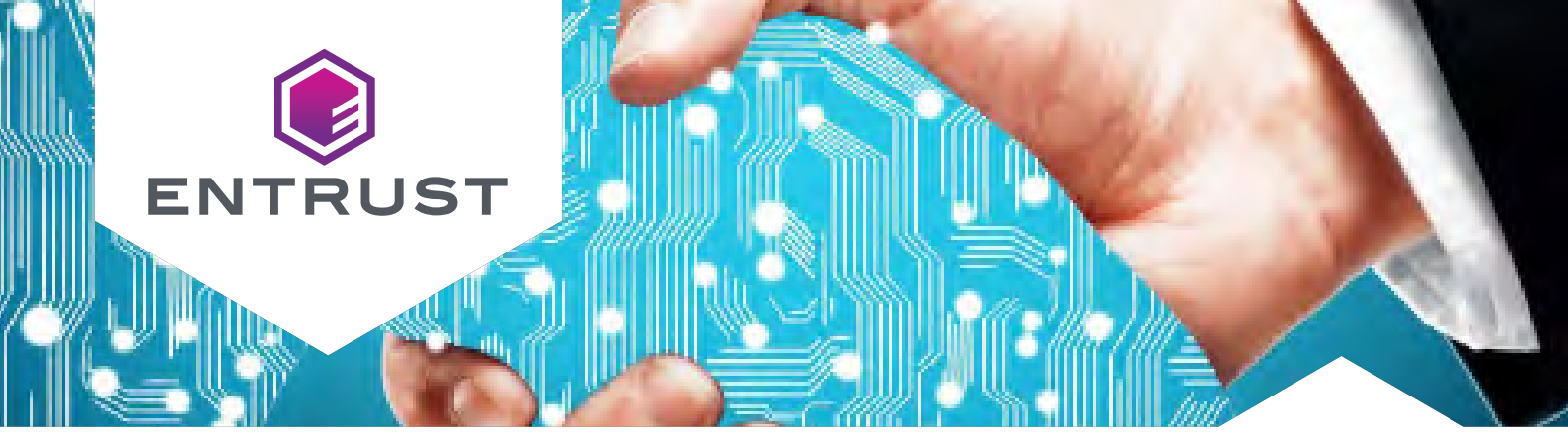

Entrust contribue à sécuriser l'infrastructure numérique de la Tunisie

LE DÉFI : AIDER LA TUNISIE À DÉVELOPPER SON ÉCONOMIE NUMÉRIQUE TOUT EN ASSURANT LA SÉCURITÉ DE SES CITOYENS

En 2015, le gouvernement tunisien a lancé le plan Digital Tunisia 2020, un plan destiné à stimuler l'économie numérique du pays en améliorant les services gouvernementaux en ligne et le commerce électronique. Le succès de l'initiative reposait sur le fait de gagner la confiance des citoyens tunisiens dans les services publics et privés en ligne et les transactions électroniques. L'Agence Nationale de Certification Électronique (ANCE), qui représente le plus haut niveau de sécurité du pays pour les transactions électroniques, s'est lancée dans le projet phare de Digital Tunisia 2020 afin de réorganiser l'infrastructure à clé publique (PKI) nationale, qui renforce la sécurité des transactions numériques.

Pour réussir, le projet nécessitait une transition rapide et en douceur des PKI existantes tout en offrant des services à la sécurité renforcée une fois mis en œuvre. En outre, les PKI devaient se conformer à de nouvelles réglementations strictes en matière de certification numérique.

LA SOLUTION : DE NOUVELLES PKI SÉCURISÉS PAR LES HSM NSHIELD DE ENTRUST

La modernisation des PKI du gouvernement tunisien nécessitait l'installation de matériel et de logiciels à jour, les meilleurs du marché, afin d'améliorer la disponibilité, la fiabilité et la qualité des services. Pour protéger les clés racines utilisées dans les PKI, l'ANCE savait qu'elle avait besoin d'une solution matérielle, car le traitement d'informations sensibles dans des solutions purement logicielles l'expose à des risques.

République tunisienne

L'ANCE a choisi PrimeKey et Entrust

Pour un fonctionnement et une sécurité optimaux, l'ANCE a choisi une solution qui combinait deux éléments essentiels : une nouvelle PKI de PrimeKey et des modules matériels de sécurité (HSM) de Entrust. Les HSM nShield® assureraient la sécurité de la PKI en hébergeant et en protégeant les clés privées des autorités de certification (CA) lors des transactions les plus sensibles.

L'ANCE a utilisé deux modèles de HSM nShield de Entrust pour sécuriser la PKI et protéger les transactions, notamment les suivantes :

- Authentifier les identités électroniques des citoyens effectuant des transactions B2G
- Sécuriser les transactions en ligne, y compris les paiements et déclarations d'impôts en ligne, l'envoi électronique des déclarations de douane et de commerce extérieur, les factures électroniques et les services de banque en ligne
- Valider les entreprises répondant aux appels d'offres du gouvernement en utilisant le système électronique tunisien de passation des marchés publics, TunEPS
- Créer des signatures et authentifier des informations, telles que des données biométriques et d'autres informations à caractère personnel, stockées sur des puces dans les documents, notamment les passeports électroniques et les cartes d'identité électroniques

Le HSM nShield Edge de Entrust relié par USB est utilisé pour générer et gérer des clés pour les CA racines hors-ligne. Le HSM nShield Connect de Entrust connecté au réseau assure divers services, tels que :

- La prise en charge des transactions du protocole OCSP (Online Certificate Status Protocol) pour obtenir le statut de révocation des certificats
- La sécurisation des clés et des transactions à l'aide de ces clés sur le serveur de signature du gouvernement, qui émet et signe des certificats pour les informations biométriques et électroniques stockées dans les puces des passeports et des cartes d'identité électroniques.

L'ANCE a installé ses HSM nShield de Entrust dans deux centres de données, l'un pour la production et l'autre pour la sauvegarde et la récupération en cas de défaillance.

En plus de fournir des HSM et une assistance lors de la mise en œuvre, Entrust a également dispensé une formation à l'équipe technique de l'ANCE sur la manière de tirer pleinement parti de ses HSM nShield de Entrust.

Collaboration proactive

Entrust a pris l'initiative de travailler directement avec PrimeKey et leur a fourni les atouts et le soutien dont ils avaient besoin pour concevoir et tester leur solution. Cette collaboration directe et proactive a contribué au bon déroulement du projet et a abouti à une solution intégrée de manière optimale.

République tunisienne

À PROPOS DE LA SOLUTION

Les HSM nShield de Entrust

Les HSM nShield de Entrust fournissent un environnement inviolable pour les opérations de chiffrement sécurisé et la gestion de clés. Les HSM nShield sont certifiés FIPS 140-2 niveau 2 et niveau 3 et Critères communs, sont conformes à l'eIDAS, et répondent aux normes de sécurité établies et émergentes pour les systèmes de chiffrement tout en restant très efficaces.

Les HSM nShield de Entrust isolent et protègent les opérations de chiffrement et les clés pour les applications les plus sensibles des organisations, et réalisent le chiffrement, la signature numérique et la gestion de clés pour un large éventail d'applications, y compris les PKI, le SSL/TLS et la signature de code. Les HSM nShield de Entrust offrent des solutions strictement sécurisées et une protection supérieure au chiffrement purement logiciel.

Les HSM nShield de Entrust prennent en charge tous les principaux algorithmes et offrent des performances de classe mondiale en matière de taux de transaction.

Grâce aux HSM nShield de Entrust et à l'architecture unique de Security World nShield, vous n'achetez que la capacité dont vous avez besoin et pouvez facilement faire évoluer votre solution en fonction de vos besoins.

Principaux avantages de la solution de Entrust

- Protéger les clés et les opérations de chiffrement au sein d'un matériel inviolable afin de renforcer considérablement la sécurité de vos solutions purement logicielles.
- Une confiance absolue en votre solution certifiée – Les HSM nShield de Entrust sont certifiés selon des normes strictes, dont FIPS et Critères communs, et sont conformes aux normes eIDAS.
- Garder le contrôle de vos clés et créer des domaines HSM qui évoluent en fonction de vos besoins grâce à l'architecture unique de Security World nShield de Entrust.

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

République tunisienne

POURQUOI AVOIR CHOISI ENTRUST ?

Les HSM de Entrust sont certifiés FIPS 140-2 niveau 2 et 3 et conformes aux Critères communs et aux normes eIDAS

Les HSM nShield de Entrust répondent aux normes strictes FIPS, Critères communs et eIDAS requises pour le projet. Entrust a obtenu la certification Critères communs EAL4+ pour les HSM nShield Solo et Connect, par l'intermédiaire de l'organisme de certification italien, l'OCSI. En vertu de la directive européenne 1999/93, cette certification accorde le statut SSCD (Secure Signature Creation Devices) aux HSM nShield de Entrust. Cette certification assure également la conformité avec le règlement eIDAS 2014.

Les HSM nShield de Entrust, une solution approuvée par l'ANCE

Les HSM nShield de Entrust avaient été déployés avec succès dans le cadre de précédents projets de l'ANCE. Parce qu'Entrust avait fourni des solutions de qualité et avait répondu aux besoins de l'agence, l'ANCE n'a pas hésité à choisir à nouveau Entrust dans le cadre de l'appel d'offres très compétitif pour obtenir la nouvelle PKI du pays.

À PROPOS DE ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com