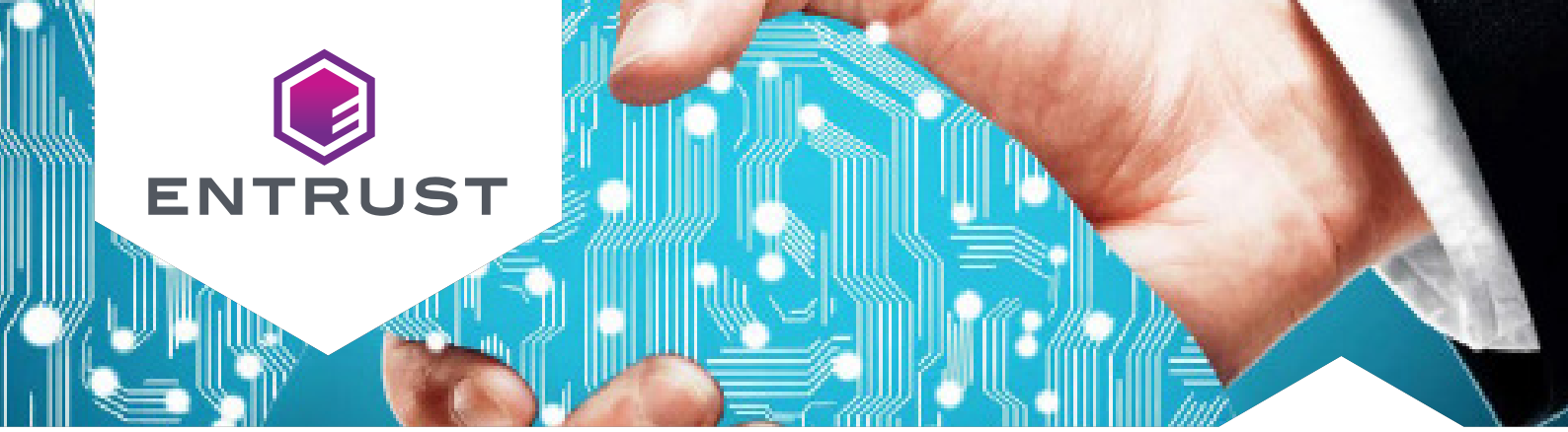

Entrust contribuisce a proteggere l'infrastruttura digitale della Tunisia

LA SFIDA: AIUTARE LA TUNISIA A ESPANDERE L'ECONOMIA DIGITALE GARANTENDO LA SICUREZZA PER I CITTADINI

Nel 2015 il governo tunisino ha lanciato Digital Tunisia 2020, un piano volto a incentivare l'economia digitale del Paese attraverso la valorizzazione dei servizi governativi online e del commercio elettronico. Ottenere la fiducia dei cittadini nei confronti dei servizi online pubblici e privati e delle transazioni elettroniche è stato individuato come il passaggio fondamentale per la riuscita dell'iniziativa. La National Digital Certification Agency (NDCA), l'entità fiduciaria di livello più elevato nel Paese, ha intrapreso questo piano strategico con l'obiettivo di riprogettare l'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) nazionale, il pilastro su cui si fonda la sicurezza delle transazioni digitali.

Per raggiungere gli obiettivi del progetto, era necessario prevedere non solo una transizione rapida dall'attuale PKI, ma anche il potenziamento dei servizi fiduciari. La PKI doveva inoltre essere conforme alle nuove e severe normative per la certificazione digitale.

LA SOLUZIONE: UNA NUOVA PKI PROTETTA DAGLI HSM NSHIELD DI ENTRUST

La modernizzazione della PKI del governo tunisino ha richiesto l'installazione dei migliori e più recenti hardware e software sul mercato, per migliorare la disponibilità, l'affidabilità e la qualità dei servizi. Per proteggere le chiavi di root utilizzate nella PKI, la NDCA sapeva che la soluzione ideale doveva essere basata su hardware, considerati i rischi derivanti dall'elaborazione delle informazioni sensibili in software.

Repubblica Tunisina

La NDCA seleziona PrimeKey + Entrust

Per un funzionamento e una sicurezza ottimali, la NDCA ha scelto una soluzione che unisce due componenti strategici: una nuova PKI di PrimeKey e gli hardware security module (HSM) di Entrust. Gli HSM nShield® di Entrust garantiscono la sicurezza della PKI, offrendo l'hosting e la protezione delle chiavi private delle autorità di certificazione (CA) durante le transazioni altamente sensibili.

La NDCA ha adottato due modelli di HSM nShield per proteggere la PKI e le transazioni e assicurare:

- L'autenticazione delle identità elettroniche dei cittadini che effettuano transazioni B2G
- La protezione delle transazioni online, compresi i pagamenti e le dichiarazioni fiscali, l'invio digitale di dichiarazioni doganali e di commercio estero, le fatture elettroniche e i servizi di online banking
- La convalida delle aziende che rispondono agli inviti a presentare proposte da parte del governo attraverso il sistema tunisino di e-procurement TunEPS
- La creazione di firme e l'autenticazione di dati biometrici e altre informazioni di identificazione personale, archiviati su chip in passaporti e documenti d'identità elettronici

Dotati di collegamento USB, gli HSM nShield Edge di Entrust generano e gestiscono le chiavi per le CA root offline. Gli HSM nShield Connect, invece, sono collegati alla rete e offrono servizi come:

- Il supporto delle transazioni basate sul protocollo OCSP (Online Certificate Status Protocol) per ottenere lo stato di revoca del certificato
- La protezione delle chiavi e delle transazioni mediante le chiavi sul server di firma del governo, che emette e firma i certificati per le informazioni biometriche ed elettroniche archiviate nei chip dei passaporti e dei documenti d'identità elettronici

La NDCA ha installato gli HSM nShield di Entrust in due data center, uno per la produzione e l'altro per il back-up e i processi di disaster recovery.

Oltre a fornire gli HSM e il supporto all'integrazione, Entrust si è occupata anche della formazione del team tecnico della NDCA, per permettere all'agenzia di trarre il massimo dai dispositivi nShield.

Collaborazione proattiva

Entrust ha preso l'iniziativa di lavorare direttamente con PrimeKey, fornendo le risorse e il supporto necessari per progettare e testare la soluzione dell'azienda. Questa collaborazione ha contribuito allo svolgimento ottimale del progetto, portando a una soluzione perfettamente integrata.

Repubblica Tunisina

DETTAGLI DELLA SOLUZIONE

HSM nShield di Entrust

Gli HSM nShield di Entrust stabiliscono un ambiente a prova di manomissione per attività sicure di elaborazione crittografica e gestione delle chiavi. Certificati in base allo standard FIPS 140-2 di livello 2 e 3 e ai Common Criteria, sono inoltre conformi al Regolamento eIDAS e soddisfano gli standard di sicurezza consolidati ed emergenti per i sistemi crittografici, mantenendo comunque alti i livelli di efficienza.

Gli HSM nShield isolano e proteggono le operazioni crittografiche e le chiavi usate per le applicazioni più critiche di un'organizzazione. Eseguono inoltre funzioni come la cifratura, l'apposizione di firme digitali e la gestione delle chiavi per un'ampia gamma di scenari, tra cui PKI, SSL/TLS e firma del codice, fornendo soluzioni a elevata garanzia e una protezione superiore rispetto alla crittografia unicamente basata su software.

Infine, supportano tutti i principali algoritmi e tassi di transazioni ineguagliati all'interno del settore.

La combinazione degli HSM nShield e dell'esclusiva architettura Security World consente alle aziende di acquistare solo la capacità di cui hanno bisogno, ma offre la scalabilità necessaria a ridimensionare la soluzione in risposta all'evoluzione delle esigenze.

I vantaggi principali della soluzione di Entrust

- Sicurezza più elevata rispetto alle soluzioni basate su software grazie alla protezione delle chiavi e delle operazioni crittografiche all'interno di hardware a prova di manomissione
- Totale affidabilità: gli HSM nShield sono certificati secondo normative rigorose, tra cui lo standard FIPS e i Common Criteria, e sono conformi al Regolamento eIDAS
- Mantenimento del controllo delle proprie chiavi e scalabilità in risposta all'evoluzione delle esigenze aziendali grazie all'esclusiva architettura nShield Security World di Entrust

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Repubblica Tunisina

PERCHÉ ENTRUST?

Certificazione secondo i Common Criteria, lo standard FIPS 140-2 di livello 2 e 3 e conformità al Regolamento eIDAS

Gli HSM nShield di Entrust soddisfano le rigorose disposizioni dello standard FIPS, dei Common Criteria e del Regolamento eIDAS, requisiti essenziali per il progetto. Entrust ha ottenuto la certificazione Common Criteria EAL4+ per gli HSM nShield Solo e Connect dall'agenzia di certificazione italiana OCSI. Ai sensi della direttiva UE 1999/93, tale certificazione attribuisce agli HSM nShield di Entrust lo status di dispositivo di creazione di firme sicure (SSCD, Secure Signature Creation Device) e garantisce la conformità al Regolamento eIDAS del 2014.

HSM nShield di Entrust, una soluzione approvata dalla NCDA

In passato, gli HSM nShield di Entrust erano già stati selezionati per altri progetti della NDCA. Grazie alla qualità elevata delle soluzioni e alla grande disponibilità dimostrata da Entrust, la NDCA non ha esitato a selezionare l'azienda tra le proposte altamente competitive ricevute nell'ambito della gara d'appalto per la nuova PKI del Paese.

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com

Entrust è un marchio, un marchio registrato e/o un marchio di servizio di Entrust Corporation negli Stati Uniti e/o in altri Paesi. ©2020 Entrust Corporation.