Sicurezza dei servizi cloud riconosciuta a livello federale con ORC ed Entrust

PIVotal ID™ di ORC, una soluzione per le identità federate adottata dagli enti pubblici statunitensi, mostra come le soluzioni "Identity as a Service" (IDaaS) basate sul cloud e supportate dalla crittografia avanzata offrano protezione e interoperabilità superiori.

I problemi relativi alla sicurezza sono ancora una fonte significativa di preoccupazione per molte aziende che stanno valutando se trasferire i propri dati sensibili nel cloud. L'esperienza di Operational Research Consultants Inc. (ORC), tuttavia, dimostra che il cloud può raggiungere un livello di sicurezza analogo, se non addirittura superiore, ai deployment on-premise, anche per le organizzazioni con requisiti rigorosi, come la pubblica amministrazione degli Stati Uniti.

ORC, UN'AZIENDA PIONIERISTICA NELLA GESTIONE DELLE IDENTITÀ A LIVELLO FEDERALE

ORC si è affermata come partner di fiducia degli enti pubblici statunitensi con il lancio, verso la metà degli anni '90, della Navy Acquisition Public Key Infrastructure, un'iniziativa mirata a proteggere le interazioni con appaltatori e fornitori. Nei vent'anni successivi, la pubblica amministrazione ha posto un'enfasi crescente sulla tutela delle informazioni e ORC è diventata l'azienda di riferimento per le soluzioni di sicurezza, nonché una delle prime società autorizzate a fornire prodotti e servizi per la gestione delle identità conformi ai requisiti governativi.

Oggi ORC gestisce più di tre milioni di identità e, negli anni, ha emesso oltre 10 milioni di certificati digitali conformi alle norme federali, per consentire l'accesso di dipendenti, appaltatori, collaboratori, veterani e cittadini ai servizi degli enti pubblici statunitensi.

ORC

SICUREZZA E INTEROPERABILITÀ PER L'IDENTIFICAZIONE E L'AUTENTICAZIONE

Nell'agosto 2004, l'amministrazione Bush ha emesso una direttiva presidenziale in materia di sicurezza interna (Homeland Security Presidential Directive, HSPD-12), mirata a introdurre uno standard che indicasse forme di identificazione sicure e affidabili per proteggere le strutture e le risorse federali. L'iniziativa non si è limitata al rilascio di badge identificativi ai dipendenti della pubblica amministrazione, ma si è concentrata invece sui processi necessari per l'emissione di credenziali personali sicure, sui metodi di verifica e sulla gestione del rischio e della qualità lungo l'intero ciclo di vita delle credenziali.

Questi processi sono stati introdotti dal programma Personal Identity Verification (PIV), mentre lo standard FIPS-201 (Federal Information Processing Standard) specifica gli elementi dell'interfaccia e dei dati della smart card PIV. Tra gli elementi dei dati presenti su una scheda PIV rientrano una o più chiavi crittografiche private asimmetriche. Per poter emettere certificati digitali agli utenti, i dipartimenti e le agenzie federali devono avvalersi di un'infrastruttura a chiave pubblica (PKI) conforme. L'iniziativa PIV ha dato origine anche ad altre credenziali a garanzia elevata per specifiche transazioni B2G (Business to Government), C2G (Citizen to Government) e C2B (Citizen to Business), supportando al tempo stesso l'interoperabilità federata tra quelle emesse. Tra le varianti PIV-Interoperable (PIV-I) e PIV sviluppate rientrano le credenziali Transportation Worker Identification Credential (TWIC®), First Responder Authentication Credentials (FRAC), Commercial Identity Verification (CIV) ed External Certificate Authority (ECA) PIV-I, che soddisfano vari requisiti normativi e sono progettate per garantire la scalabilità a livello globale. I processi e i criteri per l'emissione dei certificati, oltre alle protezioni garantite alle chiavi dell'autorità di certificazione root ed emittente della PKI, sono fattori essenziali per la sicurezza generale del sistema.

LE SFIDE: CERTIFICAZIONE, INTEROPERABILITÀ E FIDUCIA

In genere, i sistemi di gestione delle identità on-premise non si adattano con facilità a un ambiente cloud. ORC ha da subito riconosciuto la sicurezza come un criterio fondamentale affinché la gestione delle identità basata sul cloud venisse considerata affidabile da tutti gli enti pubblici federali. Ciò significa che l'unico modo per soddisfare i requisiti imposti dal NIST sarebbe stato garantire livelli elevati di protezione crittografica. Nel contesto della PKI, la creazione e la tutela delle chiavi dell'autorità di certificazione root ed emittente sarebbero dovute avvenire all'interno di un dispositivo hardware certificato secondo lo standard FIPS, dato che l'impatto operativo della compromissione di una di queste chiavi avrebbe comportato la revoca di tutti i certificati emessi nell'ambito della PKI nonché la riemissione delle credenziali.

ORC ha inoltre dovuto soddisfare vari requisiti di certificazione e accreditamento, tra cui Federal Bridge, PIV/PIV-I, DoD e FISMA, oltre a supportare la certificazione incrociata a più livelli. Questo aspetto, in particolare, richiedeva il supporto di una gamma flessibile di livelli e criteri di sicurezza. La soluzione doveva, inoltre, essere comprovata e basata su standard di sistemi aperti, per garantire un'ampia interoperabilità. Infine, ORC ha riconosciuto l'importanza di assicurare alti livelli di disponibilità e affidabilità per i servizi crittografici in un ambiente cloud.

ORC

LA SOLUZIONE: PIVOTAL ID™ DI ORC IN COLLABORAZIONE CON ENTRUST

La suite di soluzioni PIVotal ID™ di ORC offre sicurezza elevata per l'utilizzo del cloud a livello federale e include servizi gestiti certificati e accreditati per l'emissione di credenziali di identità affidabili, usate dagli enti pubblici statunitensi e applicabili in federazioni a livello globale. Un esempio è costituito dall'emissione di certificati digitali dalle PKI basate sugli hardware security module (HSM) nShield® di Entrust. ORC ha emesso e gestisce milioni di credenziali conformi che proteggono le transazioni tra le agenzie federali (civili e di difesa) e i dipendenti, gli appaltatori globali, i partner commerciali, i veterani e i cittadini che accedono ai servizi della pubblica amministrazione e dei settori regolamentati negli Stati Uniti. PIVotal ID™ supporta credenziali:

- Personal Identification Verification (PIV)
- Non-Federal Issuer PIV-Interoperable (NFI PIV-I)
- External Certificate Authority (ECA)
- Access Certificates for Electronic Services (ACES)
- TWIC Certificate Manufacturing Authority
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

ORC ha riconosciuto le capacità superiori di protezione e accelerazione crittografica della famiglia di hardware security module nShield di Entrust, che offre inoltre la flessibilità e la scalabilità necessarie a proteggere e gestire le chiavi root e tutte le chiavi subordinate all'interno di un'infrastruttura di servizi cloud sicura.

SOLUZIONI CONVENIENTI PER LA SICUREZZA DELLA CRITTOGRAFIA

Gli HSM nShield di Entrust sono progettati su una piattaforma temprata a prova di manomissione che protegge e gestisce le chiavi sensibili utilizzate per la crittografia e l'apposizione di firme digitali, supportando applicazioni di ogni tipo, dalla gestione delle identità ai servizi Web, passando per la crittografia dei database, la tokenizzazione, i servizi PKI e l'autenticazione avanzata. Gli HSM nShield sono la scelta più conveniente per stabilire controlli logici e fisici adeguati nei sistemi per cui la crittografia basata su software non è in grado di garantire livelli di sicurezza sufficienti.

ORC

GLI HSM NSHIELD DI ENTRUST CONSENTONO ALLE IMPRESE DI:

- Ottenere una flessibilità operativa ineguagliata e alti livelli di disponibilità e scalabilità negli ambienti cloud e virtualizzati.
- Ridurre i costi relativi alla conformità normativa e alle attività quotidiane di gestione delle chiavi, come il back-up e la gestione remota.
- Garantire la continuità aziendale grazie alla semplicità di implementazione degli HSM, al provisioning efficiente delle chiavi e a funzionalità hardware resilienti.
- Migliorare la sicurezza delle applicazioni critiche proteggendo le chiavi e le operazioni crittografiche all'interno di dispositivi hardware a prova di manomissione.
- Introdurre una netta separazione delle responsabilità e controlli duali attraverso criteri di amministrazione rigorosi, tra cui l'autenticazione a più fattori basata sui ruoli e l'autorizzazione basata sul quorum.

INFORMAZIONI SU ORC

ORC, una società del gruppo WidePoint e partner di fiducia dell'amministrazione pubblica statunitense, collabora con clienti governativi e aziendali offrendo soluzioni conformi e affidabili per lo scambio e la sicurezza delle informazioni. Fornitore d'élite di servizi di tutela e autenticazione dei dati per applicazioni B2G, G2G e C2G, ORC garantisce l'interoperabilità delle proprie soluzioni con i sistemi legacy e la loro perfetta integrazione con i principali software sul mercato. L'azienda si affida agli HSM nShield di Entrust per fornire servizi di gestione delle identità sul cloud altamente sicuri e riconosciuti a livello federale.

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