



ENTRUST

SECURITY
IDENTIFICATION

La Finlandia protegge l'integrità dei documenti di identità e dei passaporti elettronici EAC grazie a Entrust

Gli hardware security module (HSM) nShield® di Entrust garantiscono l'autenticità dei passaporti elettronici finlandesi grazie alla protezione delle impronte digitali mediante certificati.

La Finlandia conta una delle popolazioni che utilizzano più dispositivi elettronici al mondo e, da tempo, è leader nell'erogazione di servizi governativi online, basati su una gestione efficace delle identità e degli accessi. Tra questi, spicca il centro per i servizi anagrafici del Paese (Population Register Centre, PRC). L'ente gestisce le infrastrutture a chiave pubblica (PKI) e le autorità di certificazione (CA) nazionali, protette con gli HSM nShield di Entrust e responsabili del rilascio dei "Citizen Certificate" (certificati per i cittadini), ovvero identità digitali univoche e verificabili. I cittadini possono utilizzare questi certificati per accedere ai servizi online della pubblica amministrazione, la cui protezione è assicurata in modo efficiente ed economico. Quando la Finlandia ha avuto bisogno che il PRC adottasse una tecnologia simile per l'emissione di nuovi passaporti elettronici conformi alle più recenti direttive dell'Unione europea (UE) in materia, l'ente non ha avuto dubbi e si è rivolto a Entrust per garantire l'integrità del processo.

« Il PRC ha molta esperienza nella fornitura di servizi online della pubblica amministrazione attraverso un'implementazione PKI e l'emissione e l'uso di certificati digitali. Riteniamo che gli HSM nShield di Entrust siano un'ottima soluzione per la protezione delle chiavi private. »

- Jan Partanen, Population Register Centre della Finlandia



Population Register Centre della Finlandia

Secondo Jan Partanen, responsabile dello sviluppo del Population Register Centre della Finlandia, "I nuovi passaporti elettronici dell'UE sono i più sicuri al mondo, perché protetti da certificati digitali a prova di manomissione. Tuttavia, il sistema può funzionare soltanto se i Paesi sono in grado di proteggere le chiavi di firma che assicurano l'autenticità dei certificati digitali. Gli HSM nShield di Entrust garantiscono la sicurezza delle chiavi di firma da utilizzare nell'ambito delle CA, della PKI e dell'emissione di documenti di identità elettronici. Per questo motivo, abbiamo grande fiducia nella nostra capacità di garantire l'integrità dei passaporti elettronici e dei servizi online della pubblica amministrazione finlandese."

OBIETTIVO PRIVACY E SICUREZZA

Le impronte digitali sono caratteristiche e uniche per ciascun individuo e vengono impiegate dall'UE per garantire che solo l'effettivo titolare di un determinato passaporto possa utilizzarlo per viaggiare. In che modo? Basata sullo standard Extended Access Control (EAC), la seconda generazione di passaporti elettronici dell'UE consente agli enti pubblici di sfruttare dati biometrici più accurati, come un'impronta digitale o la scansione dell'iride. I passaporti elettronici EAC proteggono la privacy del titolare garantendo, al contempo, la validità del documento. Una volta che questi innovativi passaporti saranno implementati su scala più ampia, diventerà praticamente impossibile viaggiare con un passaporto UE falso assumendo l'identità di un'altra persona. Lo standard EAC richiede agli Stati membri dell'Unione europea di aggiungere i dati delle impronte digitali ai documenti di viaggio a lettura ottica.

I certificati digitali, che vengano utilizzati per proteggere PKI, passaporti o documenti di identità elettronici, sono sicuri, perché vengono emessi da una CA attendibile utilizzando una chiave di firma univoca. Tuttavia, se una chiave di firma venisse compromessa o rubata, un individuo potrebbe emettere un certificato

digitale apparentemente valido. Gli HSM offrono un ambiente a prova di manomissione significativamente più sicuro rispetto alle soluzioni software. L'UE ne impone, dunque, l'utilizzo per generare, archiviare e proteggere le chiavi di firma della CA per i passaporti elettronici.

UNA STORIA FATTA DI SUCCESSI

In passato, il governo finlandese si è affidato agli HSM per proteggere le CA e PKI nazionali. Sin dall'inizio, quindi, il PRC sapeva che sarebbero stati la scelta prioritaria per proteggere l'integrità dei passaporti elettronici. Sicuri e semplici da operare, gli HSM si sono integrati perfettamente con le CA di emissione dei certificati del Paese. Gli HSM sono certificati secondo lo standard FIPS (Federal Information Processing Standard) 140-2 di livello 3, il benchmark di sicurezza per le soluzioni crittografiche più diffuso tra gli enti governativi e le aziende, nonché un requisito imposto dallo standard EAC dell'UE in materia di passaporti elettronici. Il team di servizi professionali Entrust ha inoltre dimostrato la propria esperienza nell'ambito dei passaporti elettronici e della gestione delle chiavi, un altro aspetto rilevante per aiutare il PRC a stabilire un processo efficiente ed economico per il rilascio di questi documenti d'identità.

"Il PRC ha molta esperienza nell'erogazione di servizi online della pubblica amministrazione attraverso un'implementazione PKI e l'emissione e l'uso di certificati digitali," ha osservato Partanen. "Riteniamo che gli HSM siano un'ottima soluzione per la protezione delle chiavi di firma. Ovviamente, la gestione delle chiavi riveste un ruolo altrettanto importante. Il team di servizi professionali Entrust ha un'ottima conoscenza dei processi di gestione, oltre a una lunga esperienza nella fornitura di soluzioni affidabili. Per questo, non abbiamo avuto alcun dubbio: ci siamo affidati al team di Entrust e abbiamo implementato gli HSM nShield per proteggere i nostri passaporti elettronici."



Population Register Centre della Finlandia

« Grazie agli HSM nShield di Entrust, le nostre chiavi di firma rimangono sempre all'interno del perimetro di sicurezza dell'HSM, quindi non sono mai esposte a un rischio di uso improprio. Gli HSM e i certificati digitali possono sembrare complessi, ma il risultato del loro utilizzo è molto semplice: garantiscono l'integrità dei passaporti elettronici, delle CA, delle PKI e dei servizi online della pubblica amministrazione della Finlandia. »

- Jan Partanen, Population Register Centre della Finlandia

IL PROCESSO DI VERIFICA

In collaborazione con il team di servizi professionali Entrust, il PRC ha sviluppato e implementato un nuovo processo di rilascio dei passaporti elettronici, conforme agli standard UE e in grado di proteggere la privacy dei cittadini. Questi nuovi documenti integrano un chip contenente un certificato digitale e l'impronta digitale del titolare. La CA root del Paese emette i certificati utilizzando chiavi di firma generate e protette in modo sicuro in un HSM nShield di Entrust. Le chiavi di firma non sono mai esposte a un rischio di uso improprio, perché rimangono all'interno dei margini dell'HSM. Ai valichi di frontiera, l'identità del titolare del passaporto viene verificata da un dispositivo di lettura; solo i dispositivi autorizzati dai certificati digitali sono in grado di leggere i passaporti, proteggendo la privacy del titolare e garantendo la validità del documento.

CONVENIENZA E DISPONIBILITÀ ELEVATA

Invece di un HSM basato su un singolo server, il PRC ha preferito adottare un HSM della famiglia nShield Connect di Entrust, che supporta la connessione alla rete. Grazie a questa funzionalità, il PRC ha notato due importanti vantaggi. Da un lato, l'HSM comunica con più server, quindi non è stato necessario acquistare un dispositivo per ogni server della PKI

responsabile dei passaporti elettronici, con una conseguente riduzione dei costi relativi all'hardware. Dall'altro, l'HSM offre efficienza, disponibilità elevata e scalabilità, con failover automatico per agevolare il passaggio tra vari HSM.

"Gli HSM nShield di Entrust offrono un vantaggio notevole in termini di costi e disponibilità, perché un solo dispositivo può supportare più server e applicazioni contemporaneamente," ha spiegato Partanen. "Include inoltre tutte le funzionalità di sicurezza che ci si aspettano da un HSM, inclusa la separazione delle responsabilità per proteggere i dispositivi dalla manipolazione dall'interno."

PROTEZIONE DEI PROCESSI E DEI CITTADINI

Secondo Partanen, il valore degli HSM è ulteriormente confermato se si considerano le conseguenze di potenziali errori nell'emissione dei passaporti elettronici che includono impronte digitali protette da certificati. "Nel caso dei passaporti elettronici, la compromissione delle chiavi di firma consentirebbe a criminali e terroristi di emettere passaporti contraffatti. Se le chiavi venissero invece utilizzate per sbloccare il passaporto elettronico stesso, la privacy del titolare potrebbe risultare irrimediabilmente compromessa.



Population Register Centre della Finlandia

I VANTAGGI DI ENTRUST

- Verifica elettronica dell'identità
- Protezione dell'integrità dei passaporti elettronici e della privacy dei cittadini
- Prevenzione di frodi, contraffazioni e usi impropri dei passaporti
- Fornitura sicura di servizi online da parte della pubblica amministrazione

PROFILO DELL'ORGANIZZAZIONE

Fondato nel 1969, il Population Register Centre della Finlandia archivia le informazioni anagrafiche e relative all'identificazione di individui ed edifici del Paese, offrendo alla popolazione soluzioni di identificazione di alta qualità per servizi online e non solo.

Per maggiori informazioni sul PRC, visita: www.vrk.fi e www.fineid.fi.

Grazie all'implementazione degli HSM nShield di Entrust, le nostre chiavi di firma rimangono sempre all'interno del perimetro di sicurezza dell'HSM, quindi non sono mai esposte a un rischio di uso improprio. Gli HSM e i certificati digitali possono sembrare complessi, ma il risultato del loro utilizzo è molto semplice: garantiscono l'integrità dei passaporti elettronici, delle CA, delle PKI e dei servizi online della pubblica amministrazione della Finlandia."

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



ENTRUST