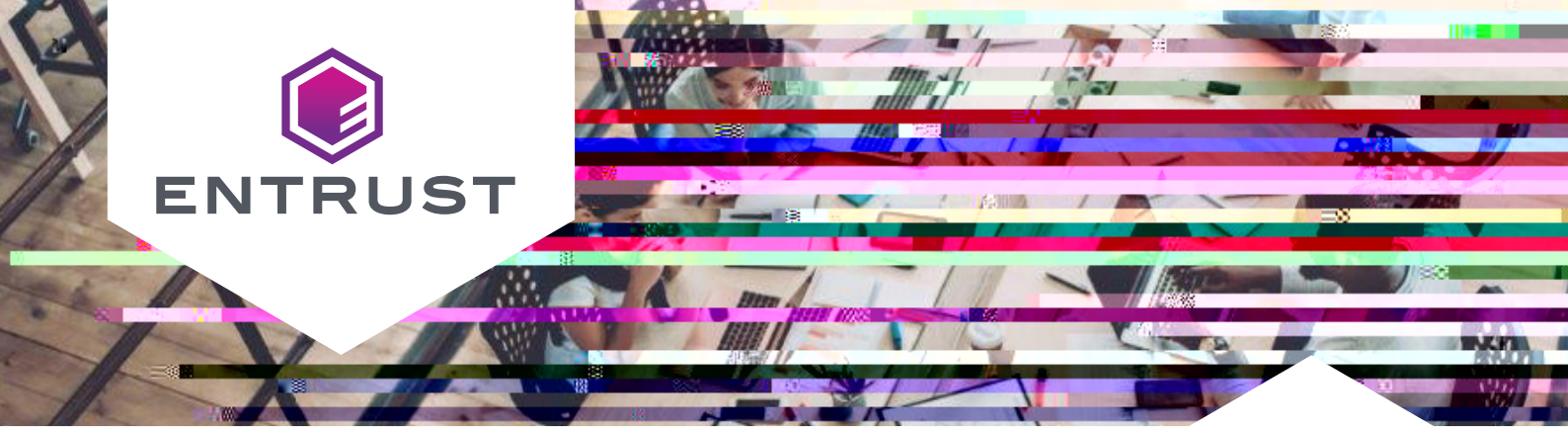

Entrust CodeSafe®

Protezione hardware certificata per applicazioni sensibili

IN EVIDENZA

CodeSafe: esecuzione del codice in un ambiente sicuro

- Protegge le applicazioni sensibili eseguendole all'interno di hardware security module (HSM) a prova di manomissione
- Aiuta a garantire l'integrità mediante firma digitale e verifica del codice
- Fornisce un ambiente sicuro per la gestione delle chiavi basata su policy
- Permette di controllare efficacemente gli accessi associando chiavi e certificati ad applicazioni in modo univoco
- Offre una soluzione pratica grazie all'utilizzo toolkit CodeSafe

CodeSafe è un tool di sviluppo che permette agli sviluppatori di scrivere ed eseguire applicazioni sensibili all'interno del perimetro sicuro degli HSM nShield con certificazione FIPS. Le applicazioni all'interno dell'ambiente di esecuzione sicuro possono crittografare, decriptare ed elaborare i dati avvalendosi inoltre dell'applicazione da parte degli HSM delle policy che disciplinano l'utilizzo delle chiavi applicazione.

Ampia gamma di applicazioni

È possibile utilizzare CodeSafe per proteggere qualunque tipo di applicazione. Alcuni esempi includono crittografia, logica di business ad alto valore associata ai servizi bancari, sistemi di misurazione intelligenti, agenti di autenticazione, agenti di firma digitale e processi di crittografia personalizzati.

Integrità delle applicazioni garantita con CodeSafe

CodeSafe fornisce gli strumenti per firmare digitalmente le applicazioni nell'ambiente di esecuzione sicuro di nShield in modo tale che la loro integrità possa essere verificata dall'HSM a runtime.

Entrust CodeSafe®

CARATTERISTICHE E VANTAGGI CHIAVE

Applicazione delle policy delle chiavi e controllo degli accessi con CodeSafe

CodeSafe consente al proprietario del software di definire i criteri che regolamentano l'utilizzo dei dati delle applicazioni, tra cui chiavi e certificati, e applicare queste policy, fornendo un ambiente sicuro per la gestione delle chiavi. Inoltre, CodeSafe associa in modo univoco le chiavi e i certificati alle applicazioni designate per garantire un rigoroso controllo degli accessi.

Endpoint SSL/TLS sicuri

Gli sviluppatori di applicazioni CodeSafe possono incorporare la libreria OpenSSL all'interno della propria applicazione per terminare le sessioni SSL/TLS all'interno dell'HSM nShield, agevolare la crittografia end-to-end, consolidare la sicurezza del livello di movimentazione dei dati e ridurre la superficie di attacco.

Implementazione e aggiornamenti da remoto

Gli amministratori possono implementare le applicazioni da un luogo centrale senza dover accedere fisicamente agli HSM.

Compatibilità con i prodotti nShield

CodeSafe è disponibile con HSM nShield Solo PCIe e Connect collegati alla rete con certificazione FIPS 140-2 livello 3. I modelli compatibili includono tutti gli HSM nShield Solo e Connect supportati, compresa la linea di prodotti XC.

Ambiente di sviluppo degli HSM

CodeSafe è compatibile con le seguenti applicazioni di programmazione:

- Linguaggi di programmazione C e C++ per applicazioni incorporate
- C, C++ e Java su server host

Requisiti per utilizzare CodeSafe

Per utilizzare CodeSafe, è necessario:

- nShield Solo o Connect HSM con certificazione FIPS 140-2 livello 3
- Kit di strumenti per sviluppatori CodeSafe
- Licenza di attivazione di CodeSafe

Il toolkit per sviluppatori CodeSafe include tutorial, documentazione e esempi per facilitare l'integrazione della tua applicazione con gli HSM nShield. Inoltre, il team dei servizi professionali Entrust è a tua disposizione per assisterti durante l'integrazione.

Scopri di più

È disponibile su richiesta un white paper CodeSafe che fornisce dettagli più approfonditi sulla tecnologia sottostante. Per ulteriori informazioni sugli HSM Entrust nShield, visita il sito **entrust.com/HSM**. Per saperne di più sulle soluzioni di sicurezza digitale di Entrust per identità, accesso, comunicazioni e data, visita il sito **entrust.com**

Scopri di più su
entrust

Per contattarci:
HSMinfo@entrust.com