Cloud Integration Option Pack

Crea e controlla le chiavi di crittografia all'interno del tuo HSM FIPS 140-2 per poi esportarle in sicurezza sul cloud

IN EVIDENZA

Fornisce agli utenti dei servizi di cloud pubblico con la capacità di generare chiavi di crittografia all'interno del proprio ambiente e mantenere il controllo di queste chiavi rendendole disponibili, in base alla necessità, per l'utilizzo nel cloud prescelto.

- Controllo delle proprie chiavi di crittografia supportando una strategia multi-cloud o ibrida
- Generazione di chiavi sicure utilizzando solida fonte di entropia
- Protezione delle chiavi nel lungo periodo grazie all'utilizzo di un HSM certificato FIPS
- Supporto di Amazon Web Services, Google Compute Engine, Microsoft Azure

Metti al sicuro le tue chiavi nel cloud il più elevato livello di protezione

Proteggi il tuo marchio e i tuoi dati

Conformi ai più elevati standard di sicurezza, come FIPS 140-2 e Common Criteria, gli HSM Entrust nShield sono pronti a proteggere i tuoi dati anche nelle situazioni di sicurezza più impegnative ed esigenti, sia on-premise che nel cloud.

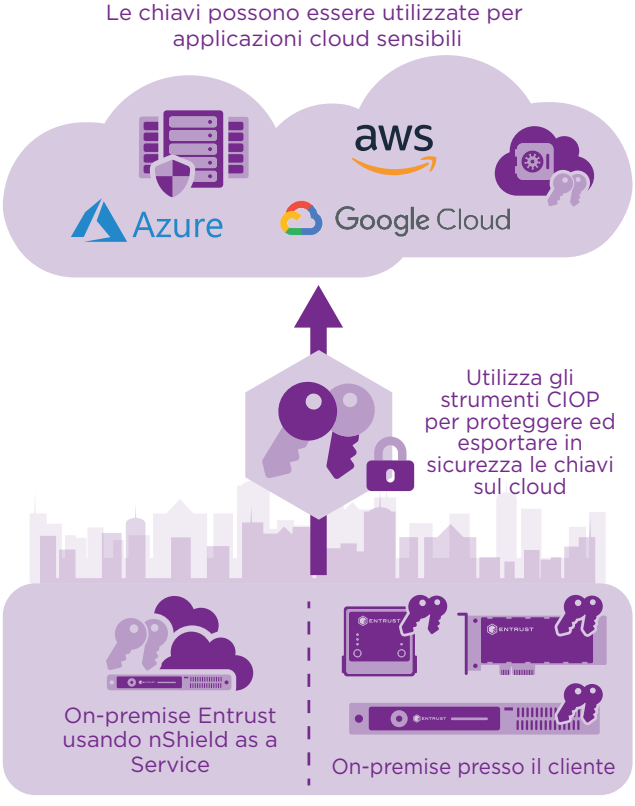

Figura 1. Le chiavi di crittografia vengono generate in un HSM nShield, per poi essere protette ed esportate in sicurezza sul cloud

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Cloud Integration Option Pack

Provider di servizi cloud supportati

Cloud Integration Option Pack (CIOP) fornisce gli strumenti che ti consentono di creare le tue chiavi di crittografia utilizzando un HSM nShield, per poi proteggerle ed esportarle in sicurezza sui seguenti provider di servizi cloud:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (utilizzando il meccanismo Azure BYOK)

Per i clienti in cerca di un livello di sicurezza superiore, Microsoft offre nCipher BYOK. Il metodo nCipher BYOK assicura ulteriormente che le autorizzazioni delle chiavi create al momento della generazione vengano preservate durante il trasferimento a Microsoft Azure Key Vault. Inoltre, Microsoft utilizza Entrust nShield Security World per limitare l'utilizzo delle chiavi a una determinata regione Azure. Questo metodo non richiede l'acquisto di CIOP. Per maggiori informazioni, consulta **Import HSM-protected keys for Key Vault (nCipher).**

Controllo delle chiavi in ambienti ibridi e multi-cloud

Cloud Integration Option Pack fornisce ai clienti il controllo e la sicurezza di cui hanno bisogno per implementare una strategia di cloud ibrido, un provider di servizi di cloud singolo o una strategia multi-cloud. Trasferendo le proprie chiavi di crittografia al provider di servizi cloud si evitano le difficoltà associate al vendor lock-in, che può complicare la migrazione da un provider di servizi cloud a un altro.

Configurazioni supportate

- Richiede il software nShield Security World v12.60 e il firmware v12.60 o versioni successive per Azure BYOK
- Richiede il software nShield Security World v12.40 per AWS e Google Compute Engine
- Questa versione è stata testata per la compatibilità su diverse piattaforme, tra cui:
  - Microsoft Windows Server 2019 x64 e 2016 x64
  - Microsoft Windows 10 x64 e 7 x64
  - Red Hat Enterprise Linux 7 x64 e AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 e 11 x64
  - Oracle Enterprise Linux 7.6 x64 e 6.10 x64
- HSM supportati
  - Compatibile con tutti gli attuali modelli nShield

Scopri di più

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.com/HSM

Per contattarci:
HSMinfo@entrust.com