ENTRUST

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Scalabilità con Bring Your Own Key (BYOK)

La sfida: mantenere il controllo delle chiavi crittografiche a protezione dei dati sensibili

Rapidità di implementazione e scalabilità in base alle esigenze sono due caratteristiche che contraddistinguono i servizi cloud. Il controllo delle chiavi di crittografia e dei secret delle applicazioni è essenziale per garantire un servizio di cloud pubblico dall'a□dabilità elevata, che protegga i dati in questo ambiente.

La soluzione: Azure Key Vault di Microsoft con controllo avanzato delle chiavi da parte degli HSM nShield di Entrust

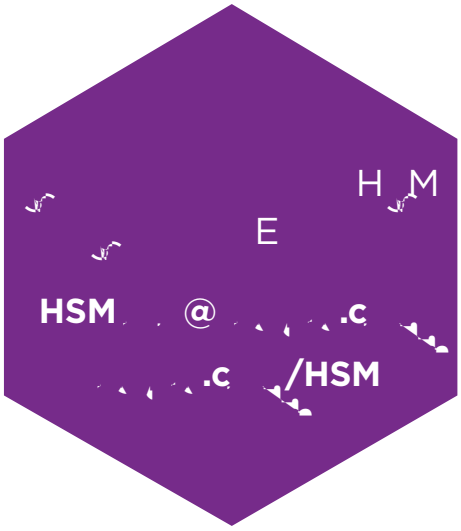
Con Azure Key Vault di Microsoft, le organizzazioni possono creare il proprio container sicuro nel cloud. Grazie alla protezione e alla gestione dei dati sensibili e delle chiavi rese possibili dagli hardware security module (HSM) nShield® di Entrust, Azure Key Vault lascia il controllo nelle mani delle aziende: gli HSM, infatti, proteggono le chiavi crittografiche nel cloud, in qualunque ambiente software si trovino, mentre le applicazioni autorizzate in esecuzione possono utilizzarle senza tuttavia vederle.

L'opzione Bring Your Own Key (BYOK) permette di utilizzare gli HSM nShield di Entrust per generare e trasferire le chiavi in modo sicuro a un HSM di proprietà di Microsoft nel cloud. Microsoft riceve una copia cache della chiave, che può essere utilizzata dalle applicazioni autorizzate all'interno di Azure. La chiave può essere replicata tra gli HSM per finalità di disaster recovery, ma l'hardware la rende invisibile all'esterno. La soluzione BYOK assicura che le chiavi rimangano all'interno di un margine di sicurezza certificato chiamato "Security World", mentre i registri di utilizzo in tempo quasi reale consentono di controllare come e quando vengono utilizzate da parte di Azure, garantendo un livello aggiuntivo di sicurezza. Il proprietario può quindi monitorarne l'utilizzo e, se necessario, revocare l'accesso.

Perché usare gli HSM di Entrust con Azure Key Vault di Microsoft?

Gli HSM nShield di Entrust proteggono e gestiscono le chiavi crittografiche utilizzate per salvaguardare i dati sensibili nel cloud. Nello specifico:

- Generano e trasferiscono in modo sicuro le chiavi crittografiche mantenendole all'interno dell'architettura Security World
- Proteggono le chiavi all'interno di un margine crittograo:



ENTRUST CORPORATRU

Scopri di più su
entrust.com/HSM