Cloud Integration Option Pack

Create and control cryptographic keys in your FIPS 140-2 HSM, then securely export to the cloud

HIGHLIGHTS

Provides users of public cloud services with the ability to generate cryptographic keys in their own environment and retain control of those keys while making them available, as required, for use in the cloud of their choice.

- Control of your cryptographic keys supporting a multi or hybrid-cloud strategy
- Secure key generation using a strong entropy source
- Long term key protection using a FIPS-certified HSM
- Support for Amazon Web Services, Google Compute Engine, Microsoft Azure

Safeguard your keys in the cloud with the highest level of assurance

Protect your brand and data

Validated to the highest security standards, such as FIPS 140-2 and Common Criteria, Entrust nShield HSMs are ready to protect your data in even the most challenging and demanding security situations, whether on premises or in the cloud.

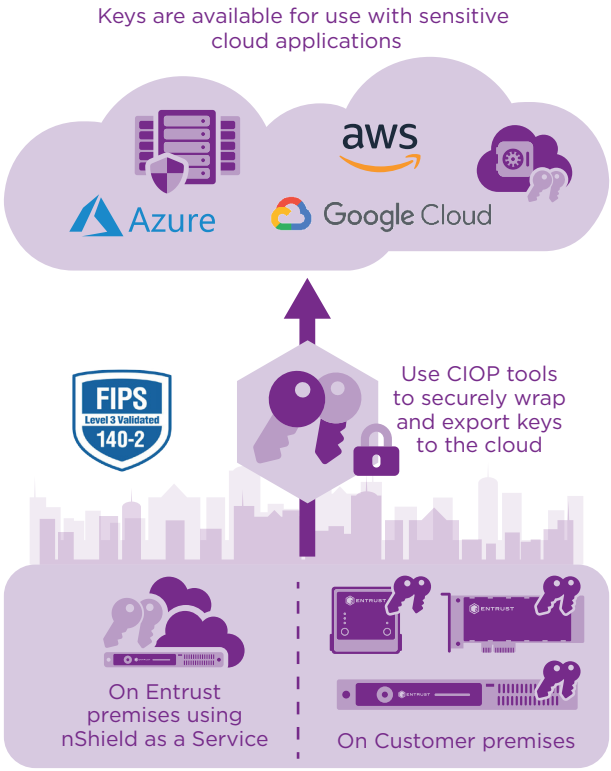

Figure 1. Encryption keys are generated in an nShield HSM, wrapped and exported securely to the cloud

LEARN MORE AT ENTRUST.COM/HSM

Cloud Integration Option Pack

Supported cloud service providers

Cloud Integration Option Pack (CIOP) provides the tools to allow you to create your cryptographic keys using an nShield HSM then wrap and securely export them to the following cloud service providers:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (using the Azure BYOK mechanism)

For customers seeking a higher level of assurance, Microsoft offers nCipher BYOK. The nCipher BYOK method provides additional assurances that the key permissions created at generation time are preserved during the transfer to Microsoft Azure Key Vault. In addition Microsoft make use of the nCipher Security World to restrict key use to a specified Azure region. This method does not require the purchase of CIOP. See **Import HSM-protected keys for Key Vault (nCipher)** for more information.

Key control in hybrid and multi-cloud environments

Cloud Integration Option Pack gives customers the control and assurance they need whether deploying a hybrid cloud strategy, single cloud service provider or a multi-cloud strategy. By bringing your cryptographic keys to the cloud service provider you avoid the difficulties associated with vendor lock-in which can make it difficult to migrate from one cloud service provider to another.

Supported configurations

- Requires nShield Security World Software v12.60 and firmware v12.60 or later for Azure BYOK
- Requires nShield Security World Software v12.40 software for AWS and Google Compute Engine
- This release has been tested for compatibility on a range of platforms including:
  - Microsoft Windows Server 2019 x64 and 2016 x64
  - Microsoft Windows 10 x64 and 7 x64
  - Red Hat Enterprise Linux 7 x64 and AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 and 11 x64
  - Oracle Enterprise Linux 7.6 x64 and 6.10 x64
- Supported HSMs
  - Compatible with all current nShield models

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com