Cloud Integration Option Pack

在 FIPS 140-2 硬件安全模块中创建和控制加密密钥，然后将其安全导出至云端

精彩亮点

可让公共云服务的用户在自己的环境中生成加密密钥，同时保留这些密钥的控制权，根据需要将其用于自己选择的云。

- 控制加密密钥，支持多云或混合云策略
- 使用强大的熵源，安全生成密钥
- 使用经 FIPS 认证的硬件安全模块，为密钥带来长期保护
- 支持 Amazon Web Services、Google Compute Engine、Microsoft Azure

利用最高级别的保障，守护云端的密钥

保护您的品牌和数据

Entrust nShield 硬件安全模块已通过 FIPS 140-2 和 Common Criteria 等最高等级的安全标准验证，可以在最具挑战和最苛刻的安全环境中为您的数据保驾护航，在本地或云端为您的数据提供保障。

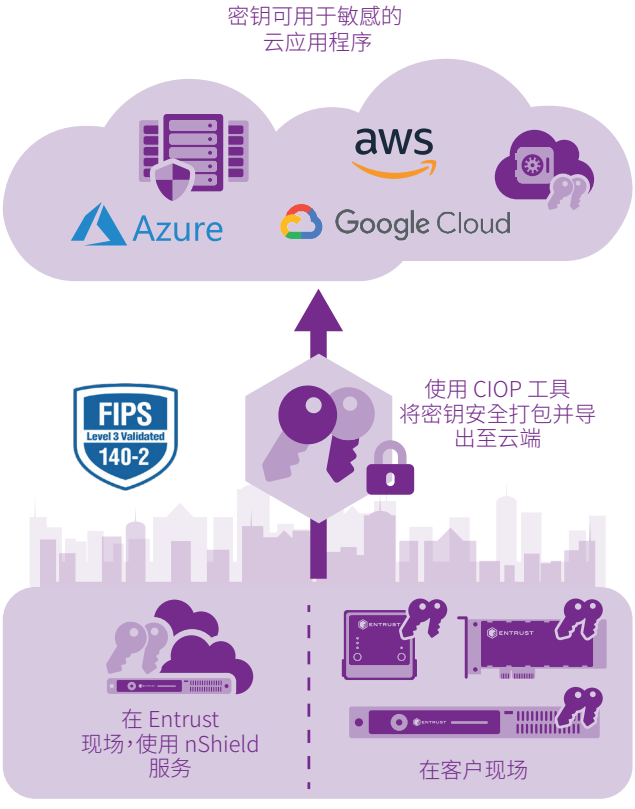

图 1. 加密密钥在 nShield 硬件安全模块中生成、打包并安全导出至云端

如需进一步了解，请访问：ENTRUST.COM/HSM

Cloud Integration Option Pack

支持的云服务提供商

Cloud Integration Option Pack (CIOP) 提供了多项工具，允许您使用 nShield 硬件安全模块创建加密密钥，然后将其包装并安全导出到以下云服务提供商：

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault（使用 Azure BYOK 机制 *）

注释*：客户如需更高级别的保障，可采用 Microsoft 提供的 nCipher BYOK。nCipher BYOK 方法提供了额外的保障，确保在将密钥转移到 Microsoft Azure Key Vault 时，生成密钥期间所创建的密钥权限得以保留。此外，Microsoft 还利用 Entrust nShield Security World 将密钥限制为仅在指定的 Azure 区域使用。该方法不要求购买 CIOP。如需了解更多信息，请参阅**将硬件安全模块保护的密钥导入至 Key Vault (nCipher)**。

混合云和多云环境的密钥控制

Cloud Integration Option Pack 为客户提供了所需的控制和保障，供其在部署混合云策略、单个云服务提供商或多云策略时使用。通过将您的加密密钥提供给云服务提供商，您可以避免与供应商锁定相关的难题，这些难题可能导致无法从一个云服务提供商迁移到另一个云服务提供商。

支持的配置

- Azure BYOK 需要使用 nShield Security World Software v12.60 和固件 v12.60 或更高版本
- AWS 和 Google Compute Engine 需要使用 nShield Security World Software v12.40 软件
- 该版本已针对一系列平台进行兼容性测试，包括：
  - Microsoft Windows Server 2019 x64 和 2016 x64
  - Microsoft Windows 10 x64 和 7 x64
  - Red Hat Enterprise Linux 7 x64 和 AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 和 11 x64
  - Oracle Enterprise Linux 7.6 x64 和 6.10 x64
- 支持的硬件安全模块
  - 与当前所有 nShield 型号兼容

进一步了解

如需进一步了解 Entrust nShield 硬件安全模块，请访问 **entrust.com/HSM**。如需进一步了解 Entrust 的身份、访问权限、通信和数据数字安全解决方案，请访问 **entrust.com**

联系我们：
HSMinfo@entrust.com