nShield Edge 硬件安全模块

该设备经过认证，可通过 USB 连接，为桌面应用程序提供加密密钥服务

精彩亮点

nShield Edge 硬件安全模块 (HSM) 是经过 FIPS 认证的设备，可通过 USB 连接，功能齐全，能提供加密、密钥生成和密钥保护服务，为客户带来更多便利，同时节省成本。

- 最大限度提高成本效益。nShield Edge 是 nShield 系列中最经济高效的硬件安全模块
- 支持广泛多样的应用程序，包括证书颁发机构、代码签名等
- 带来强大的安全性。nShield Edge 硬件安全模块已通过 FIPS 140-2 3 级认证

专为小批量事务处理环境精心设计

适用于离线密钥生成和开发环境，同时还能提供完整的算法和 API 支持。非常适合“创建自己的密钥”(BYOK) 部署，该部署需要生成具有 FIPS 140-2 级保证的加密密钥，然后将密钥安全导出至云端。

高度轻便灵活

外形小巧轻便，配备 USB 接口，方便支持多种平台，包括笔记本电脑和其他便携设备。

经济高效，可伸缩扩展

作为 nShield 系列中性价比最高的硬件安全模块，nShield Edge 为您带来入门级硬件安全模块，让您能够随着需求的增长来扩展环境。Entrust 独一无二的 Security World 架构使您能够合并 nShield 硬件安全模块模型，构建混合资产，从而实现灵活的可伸缩性、密钥共享、无缝故障转移和负载平衡。

如需进一步了解，请访问：ENTRUST.COM/HSM

nShield Edge 硬件安全模块

技术规格

支持的加密算法（包括完整的 NIST Suite B 实施）	操作系统	应用程序编程接口 (API)	兼容性和可升级性	安全合规
• 非对称算法：RSA、Diffie-Hellman、ECMQV、DSA、El-Gamal、KCDSA、ECDSA、ECDH、Edwards（X25519、Ed25519ph） • 对称算法：AES、Arcfour、ARIA、Camellia、CAST、DES、MD5 HMAC、RIPEMD160 HMAC、SEED、SHA-1 HMAC、SHA-224 HMAC、SHA-256 HMAC、SHA-384 HMAC、SHA-512 HMAC、Tiger HMAC、3DES • 哈希/消息摘要：MD5、SHA-1、SHA-2（224、256、384、512 位）、HAS-160、RIPEMD160	• Microsoft Windows 7 x64、10 x64、Windows Server、2012 R2 x64、2016 x64、2019 x64 • Red Hat Enterprise Linux AS/ES 6 x64、x86 以及 7 x64；SUSE Enterprise Linux 11 x64 SP2、12 x64、15.1 x64 • Oracle Enterprise Linux 6.10 x64、7.6 x64	• PKCS#11、OpenSSL、Java (JCE)、Microsoft CAPI 和 CNG、nCore、Web Service（需要 Web Service 选项包）	• USB 端口（与 1.x、2.x 兼容）	• FIPS 140-2 2 级和 3 级

符合安全和环境标准	管理和监控	物理特征	性能
• UL、CE、FCC、RCM、以及加拿大 ICES RoHS2、WEEE	• 安全审计日志记录	• 便携式桌面设备，具有集成式智能读卡器 • 支架打开时的尺寸为 120 x 118 x 27 毫米（4.7 x 4.6 x 1 英寸） • 重量：340 克（0.8 磅） • 输入电压：5v 直流电，由 USB 主机设备供电 • 功耗：700mW	• NIST 建议密钥长度的签名性能： • 2048 位 RSA：2 tps • 4096 位 RSA：0.2 tps

供应型号和性能

- nShield Edge 提供 FIPS 2 级和 3 级版本
- 另外还提供了非 FIPS 开发者版本

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**

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com