nShield Connect 硬件安全模块

应用程序安全的关键在于密钥保存

精彩亮点

功能齐全

nShield Connect 硬件安全模块 (HSM) 设备经过 FIPS 140-2 和 Common Criteria EAL4+ (EN 419 221-5) 认证，可跨网络提供可扩展的高可用性加密密钥服务。

- 快速加密事务处理，灵活实现扩展
- 整合 150 多个首屈一指的应用程序提供商解决方案
- CodeSafe 选项可在 nShield 的安全执行环境中保护您的应用程序和业务逻辑

nShield Connect 硬件安全模块是防篡改平台，可在多个应用程序中执行加密、数字签名和密钥生成以及保护等功能，包括：

- 证书颁发机构
- 代码签名
- 定制软件
- 云和容器化应用程序
- Web Service
- 区块链
- 数据库加密

nShield Connect 系列包括 nShield Connect+ 以及高性能 nShield Connect XC。

如需进一步了解，请访问：ENTRUST.COM/HSM

nShield Connect 硬件安全模块

关键功能和优点

高度灵活的架构

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、无缝故障转移和负载平衡。

快速处理更多数据

nShield Connect 硬件安全模块支持高速事务处理，非常适合企业、零售和物联网等吞吐量至关重要的环境。

强大的远程功能选项

无需访问数据中心

nShield Remote Administration - 允许安全地为远程硬件安全模块提供授权智能卡，以执行维护任务，包括固件升级、注册新硬件安全模块和重新分配/重新配置现有硬件安全模块。提供单独的数据表。

远程配置 - Connect XC 的串行控制台版本可为数据中心工作人员提供简化安装、远程网络配置和前面板设置。

nShield Monitor 提供了统一仪表板，在可此管理所有 nShield 硬件安全模块，优化操作，增加正常运行时间。提供单独的数据表。

保护专有应用程序

CodeSafe 选项为在 nShield FIPS 140-2 物理领域内运行敏感应用程序提供了安全的环境。如需更多详细信息，请参考 CodeSafe 数据表。

供应型号和性能

nShield Connect 型号	500+	XC Base	1500+	6000+	XC Mid	XC High
NIST 建议密钥长度的 RSA 签名性能 (tps)：						
2048 位	150	430	450	3,000	3,500	8,600
4096 位	80	100	190	500	850	2,025
NIST 建议密钥长度的 ECC 主要曲线签名性能 (tps)：						
256 位	540	680	1,260	2,400	7,515[2]	14,400[2]
客户端许可证						
随附	3	3	3	3	3	3
最高数量	10	10	20	无限制[1]	20	无限制[1]

注解 1：需要企业客户端许可证。

注解 2：上述性能要求 nCipher 支持免费提供 ECDSA 高速 RNG 功能激活服务。

nShield Connect 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）	支持的平台	应用程序编程接口 (API)	主机连接	安全合规
• 非对称算法：RSA、Diffie-Hellman、ECMQV、DSA、El-Gamal、KCDSA、ECDSA（包括 NIST、Brainpool 和 secp256k1 曲线）、ECDH、Edwards（Ed25519、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	• Windows 和 Linux 操作系统，包括 RedHat、SUSE 以及主流云提供商的虚拟机或容器版本	• PKCS#11、OpenSSL、Java (JCE)、Microsoft CAPI/CNG 以及 Web Service（需要 Web Services Option Pack）	• 双千兆级以太网端口（两个网段）	• 经 FIPS 140-2 2 级 和 3 级认证 • 经 IPv6 认证，符合 USGv6 Ready • Connect XC：根据荷兰 NSCIB 规范要求，eIDAS 和 Common Criteria EAL4 + AVA_VAN.5 和 ALC_ FLR.2 认证符合 EN 419 221-5 安全保护轮廓 • Connect+：已通过 Common Criteria EAL4+ (AVA_VAN.5) 认证 • Connect+：公认的合格签名创建设备 • Connect XC：符合 BSI AIS 20/31

符合安全和环境标准	高可用性	管理和监控	物理特征
• UL、CE、FCC、RCM 加拿大 ICES RoHS2、WEEE	• 所有固态存储 • 可现场维修的风扇架、双热插拔电源	• nShield Remote Configuration（可在串行控制台配置的 Connect XC 型号中使用） • nShield Remote Administration（另行购买） • nShield Monitor（另行购买） • 安全审计日志记录 • 系统日志诊断支持和 Windows 性能监控 • SNMP 监控代理程序	• 标准 1U 19 英寸机架尺寸：43.4 x 430 x 705 毫米（1.7 x 16.9 x 27.8 英寸） • 重量：11.5 千克（25.4 磅） • 输入电压：100-240V AC 自动切换 50-60Hz • 功耗：110V AC、60Hz 时最高达 2.0A | 220V AC、50Hz 时最高达 1.0A • 散热：327.6 至 362.0 BTU/小时（全负荷） • 可靠性 - MTBF（小时）[3]，Connect XC：107,384 小时，Connect+：99,284 小时

注解 3：依据 Telcordia SR-332“电子设备可靠性预测程序”MTBF 标准，在 25 摄氏度的工作温度下计算得出

如需进一步了解 Entrust nShield 硬件安全模块

HSMinfo@entrust.com
entrust.com/HSM

关于 ENTRUST CORPORATION

Entrust 支持受信任的身份、付款和数据保护，为世界的安全运转保驾护航。如今，无论是处理跨境业务、购买商品、访问电子政府服务还是登录公司网络，人们都比以往更加需要顺畅安全的体验。Entrust 提供了无与伦比的数字安全和凭证颁发解决方案，直接打通这些交互的核心。Entrust 在 150 多个国家/地区拥有 2,500 多位同事以及巨大的全球合作伙伴和客户网络，因而深受全球大多数托管组织的信任。

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com