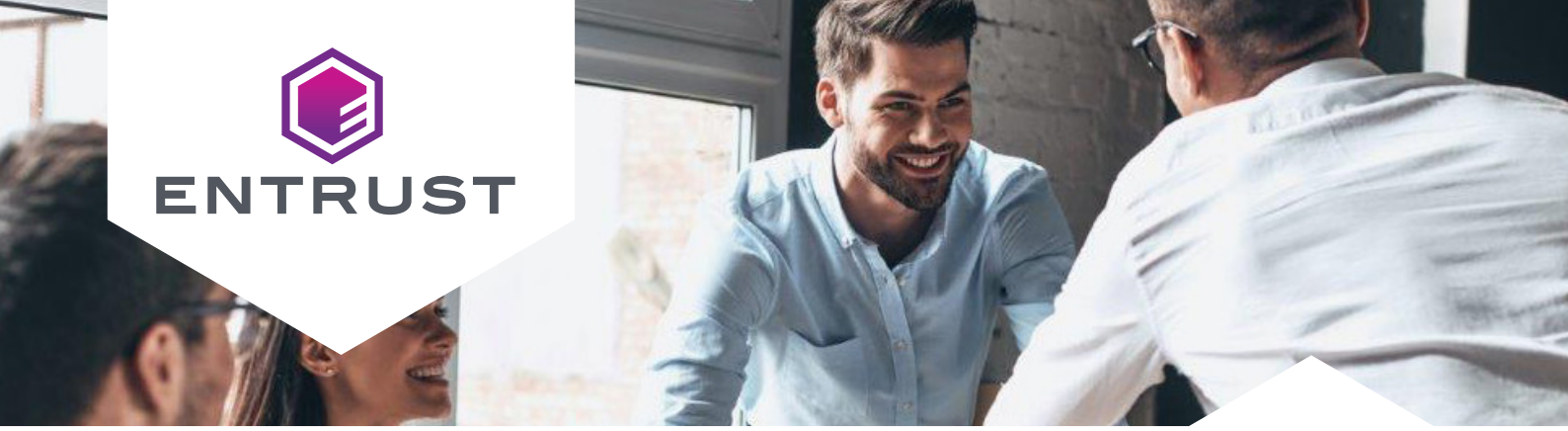


nShield Solo 硬件安全模块

经认证的 PCI-Express 卡、为独立服务器提供加密密钥服务

精彩亮点

nShield Solo 硬件安全模块 (HSM) 是经过 FIPS 认证的半高 PCI-Express 卡、为托管在服务器或设备上的应用程序提供加密服务。这些防篡改卡可执行加密、数字签名、密钥生成和保护等功能、应用到证书颁发机构、代码签名、定制软件等广泛领域。

nShield Solo 系列包括 nShield Solo+ 以及全新的高性能 nShield Solo XC。

高度灵活的架构

nCipher 独一无二的 Security World 架构使您能够结合 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

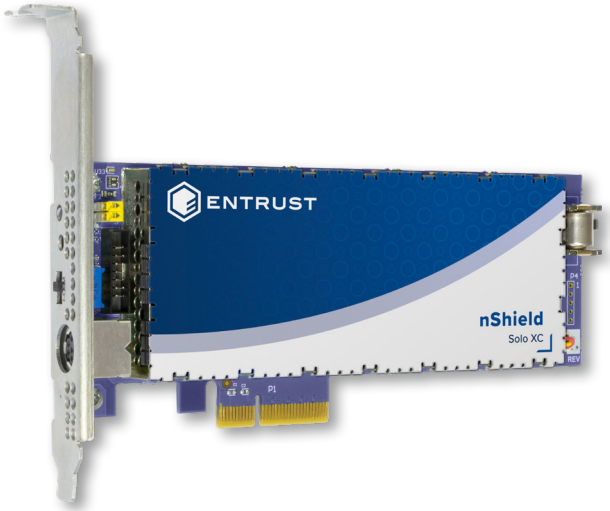
nShield Solo 硬件安全模块支持高速事务处理、非常适合企业、零售、物联网和吞吐量至关重要的其他环境。

保护专有应用程序和数据

CodeSafe 选项保证了在 nShield 领域运行敏感应用程序的环境安全。

关键功能和优点

- 快速加密事务处理、灵活实现扩展、最大限度提高性能和可用性
- 支持广泛多样的应用程序、包括证书颁发机构、代码签名等
- nShield CodeSafe 可在 nShield 的安全执行环境内保护您的应用程序
- nShield Remote Administration 有助削减成本、减少差旅



需进一步了解，请访问：ENTRUST.COM/HSM

nShield Solo 硬件安全模块

技术规格

支持的加密算法

- 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
- 具有完全许可 ECC 的完整版 Suite B 实施、包括 Brainpool 和定制曲线

支持的平台

- 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
- Solo XC 支持 VMware ESX、Microsoft Hyper-V、Linux KVM 和 Citrix XenServer 等虚拟环境

应用程序编程接口 (API)

- PKCS#11、OpenSSL、Java (JCE)、Microsoft CAPI 和 CNG、nCore 以及 Web Service（需要 Web Services Option Pack）

主机连接

- PCI Express 版本 2.0；Solo+ 连接器：1 通道、Solo XC 连接器：4 通道

安全合规

- 经 FIPS 140-2 2 级和 3 级认证
- Solo+：已通过 Common Criteria EAL4+ (AVA_VAN.5) 认证
- Solo+ 是一种公认的合格签名创建设备
- Solo XC：根据荷兰 NSCIB 规范要求、eIDAS、Common Criteria EAL4 + AVA_VAN.5 和 ALC_ FLR.2 认证符合 EN 419 221-5 安全保护轮廓
- Solo XC：符合 BSI AIS 20/31

符合安全和环境标准

- UL、UL/CA、CE、FCC、加拿大 ICES、KC、FCC、VCCI、RCM
- RoHS2、WEEE、REACH

管理和 监控

- nShield Remote Administration 和 nShield Monitor
- 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

供应型号和性能

nShield Solo 型号	500+	XC Base	6000+	XC Mid	XC High
NIST 建议密钥长度的 RSA 签名性能 (tps)					
2048 位	150	430	3,000	3,500	8,600
4096 位	80	100	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	2,400	7,515[1]	14,400[1]

注解 1：上述性能要求 nCipher 支持免费提供 ECDSA 快速 RNG 功能激活服务。

尺寸	重量		功率	
	Solo+	Solo XC	Solo+	Solo XC
56.2 × 167.1 × 15.4 毫米	230 克	280 克	10W	24W
2.2 × 6.6 × 0.6 英寸	0.5 磅	0.62 磅		

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com