nShield® 通用硬件安全模块

ENTRUST

SECURING A WORLD IN MOTION

目录

安全可信任

Entrust 的 nShield 硬件安全模块 (HSM) 是强化版防篡改设备，可保护公司的极为敏感的数据。这些模块经过 FIPS 140-2 认证，可执行加密功能，例如生成、管理和存储加密和签名密钥，以及在其受保护的领域内执行敏感功能。

nShield 硬件安全模块是安全堆栈的一剂强心针，可帮助您：

- 实现更高级别的数据安全和信任
- 满足和超越重要法规标准要求
- 维持高服务水平和业务敏捷性

nShield 系列

为了适合您的特定环境，nShield 系列通用硬件安全模块包括以下模型：

nShield Connect

网络连接设备

nShield Connect 硬件安全模块为分布在网络上的应用程序提供加密服务。nShield Connect 硬件安全模块有两个系列可供选择：经典 nShield Connect+ 硬件安全模块和高性能 nShield Connect XC 硬件安全模块系列。

nShield Edge

便携 USB 模块

nShield Edge 硬件安全模块是桌面设备，其设计便携，经济高效。nShield Edge 是理想的开发人员工具，支持生成小批量根密钥的应用程序。

nShield Solo

嵌入设备或服务器的 PCIe 卡

nShield Solo 硬件安全模块是半高 PCI-Express 卡模块，可为服务器或设备上托管的应用程序提供加密服务。nShield Solo 硬件安全模块有两个系列可供选择：经典 nShield Solo + 硬件安全模块和高性能 nShield Solo XC 硬件安全模块系列。

nShield 即服务

基于订阅的解决方案，可用于访问云端的 nShield 硬件安全模块

nShield 即服务提供了订阅模型，可通过该模型访问使用通过 FIPS 140-2 3 级认证的专用 nShield Connect XC 硬件安全模块。该解决方案提供的特征和功能与本地硬件安全模块相同，同时结合了云服务部署的优势。客户可借此机会实现其“云优先”的目标，将这些设备的维护交给 Entrust 专家。提供自我管理和完全托管服务选项。

支持广泛多样的用途

Entrust 客户将 nShield 硬件安全模块用作各种业务应用程序的信任基础，其中包括公钥基础结构 (PKI)、SSL/TLS 加密密钥保护、代码签名、数字签名和区块链。随着物联网的发展，设备 ID 和证书的需求量也越来越大，nShield 硬件安全模块始终如一地支持关键的安全措施，例如使用数字证书的设备身份验证。

nShield 硬件安全模块还支持广泛的加密算法，包括椭圆曲线加密算法，这些算法可提供非常适合当今紧凑型计算环境的高速交易，以及业界广泛使用的操作系统和 API

nShield 系列的功能

云友好型 Web 服务接口

可选的 nShield Web Services Option Pack 通过利用 Web 服务调用执行命令，简化了应用程序和硬件安全模块之间的接口。这种创新方法无需将应用程序直接与 nShield 集成，从而简化了部署，并且不再依赖操作系统和体系结构设计选择。Web Services Option Pack 是一个云友好型解决方案，可与云以及传统数据中心托管的应用程序交互。

本地或云容器化支持

nShield Container Option Pack 可以无缝开发和部署以 Entrust 的高安全级硬件安全模块为基础的容器化应用程序或流程。此选项提供了一组预打包的脚本，这些脚本大大简化了 nShield 硬件安全模块与容器应用程序环境的集成，同时支持客户应用程序和容器化主机的动态扩展需求。

利用 nShield BYOK 对云数据进行更严格的 密钥管理

nShield BYOK（创建自己的密钥）使您可以在本地 nShield 硬件安全模块中生成强密钥，并将其安全地导出到云应用程序，无论您是使用 Amazon Web Services、Google Cloud Platform、Microsoft Azure 或三者集成都可以实现。借助 nShield BYOK，您可以增强密钥管理实践的安全性，更好地控制密钥，并确保您承担保证云端数据安全的责任。

nShield BYOK 可为您带来以下优势：

- 更安全的密钥管理实践，可增强云端敏感数据的安全性
- 使用 FIPS 认证硬件保护的 nShield 的高熵随机数字生成器，可以生成更高强度的密钥
- 更好地控制密钥 - 在您自己的环境中使用您自己的 nShield 硬件安全模块密钥，并将其安全地导出到云端

为了对加密密钥的传输和使用实行最高级别的保证和严格控制，请使用 Microsoft Azure 提供的 nShield BYOK。如果您需要集成和部署现场协助，不妨尝试选择我们的 BYOK Deployment Service Package。该服务包包括 nShield Edge、Entrust 专业服务团队提供的集成以及一年的维护支持。

对于 Amazon Web Services 和 Google Cloud Platform 版 BYOK，则建议选择 Entrust 的 Cloud Integration Option Pack (CIOP)。如需使用本地 nShield 硬件安全模块生成密钥并将其租赁到 Amazon Web Services 或 Google Cloud Platform，这个选项包可以满足您的种种需求。此外，CIOP 还支持全新的开放式平台 Microsoft Azure BYOK 机制。

利用远程监控和管理实现简化操作

nShield Monitor 和 nShield Remote Administration 适用于 nShield Solo 和 nShield Connect 硬件安全模块，可帮助您降低运营成本，同时保持对硬件安全模块资产的实时关注和全天候控制。

Entrust 的远程监控和管理提供了以下优势：

- 利用 nShield Monitor 优化硬件安全模块性能、基础架构规划和运行时间，向员工通报知晓负载趋势、使用情况统计数据、篡改事件、警告和警报
- 通过 nShield Remote Administration 强大而安全的接口管理硬件安全模块，从而降低差旅成本并节省时间

远程配置

nShield Connect XC 型号提供了串行控制台选件，简化了硬件安全模块的机架、电缆连接和通电安装。所有其他硬件安全模块和网络配置均可远程处理。这样简化了部署和重新部署，无需反复访问数据中心。此功能支持提供商/租户模型，其中提供商控制网络配置，租户则完全掌控其密钥材料。

Security World 的高度灵活架构

nShield Security World 通过创建独一无二的灵活密钥管理环境，支持 Entrust nShield 硬件安全模块。使用 nShield Security World，您可以组合不同的 nShield 硬件安全模块模型，构建统一的生态系统，提供可扩展性、无缝故障转移和负载平衡。

“Entrust nShield 硬件安全模块是业界极为优秀的产品，让我们能够在技术中使用更复杂、更安全的芯片。”

Bill Kavadas - Memjet 信息系统高级总监

无论您部署一个还是数百个硬件安全模块，nShield Security World 都允许交互操作，让您能够管理无限数量的密钥，并自动远程备份和还原密钥材料。

nShield Security World 提供了以下优势：

- 帮助您随需求增长扩展 nShield 硬件安全模块资产
- 保留系统弹性
- 通过免除耗时较长的硬件安全模块备份任务，节省时间

CodeSafe - nShield 的安全 执行环境

nShield Solo 和 nShield Connect 硬件安全模块不仅能保护您的敏感密钥，还为运行专有应用程序提供了安全的环境。CodeSafe 选项可让您在 nShield 的 FIPS 140-2 3 级领域内开发和执行代码，保护您的应用程序，免受潜在攻击。

CodeSafe 可帮助您：

- 在认证环境内执行敏感应用程序，保护应用程序数据端点，实现高安全级保障
- 帮助安全敏感型应用程序抵御内部攻击、恶意软件和高级持续威胁等危害
- 使用代码签名，消除未授权的应用程序更改或恶意软件感染的风险

与行业领导者合作

Entrust 与行业领先的技术提供商合作交付增强的解决方案，以应对各行各业的安全挑战，帮助客户实现其数字化转型目标。通过 Entrust 技术合作伙伴项目，Entrust 与合作伙伴协作，将 nShield 硬件安全模块集成到各种安全解决方案中，包括凭据和 PKI、数据库安全性、代码签名、数字签名、特权账户管理、应用程序交付以及云和大数据智能。nShield 硬件安全模块支持我们合作伙伴的安全应用程序，提供极为强大的加密处理、密钥保护和密钥管理功能，同时促进遵守政府和行业数据安全法规。

“nShield 全新的功能（包括 nShield 即服务）非常适用于云，为客户带来了诸多可能性，这让我们非常激动。这些新功能认识到市场在不断变化；组织需要在云端提供全方位服务硬件安全模块的功能，发动可能的创新和探索商业利益。”

Ed Wood - Cryptomathic
产品管理总监

“Entrust 推出的 nShield 即服务为 F5 客户提供了增强的安全性选项，让他们能够在基于订阅的模型上实现数据主权管理。将安全从资本转移到运营支出可以让组织更加灵活，更加节省成本。”

John Morgan - F5 Networks
安全副总裁兼总经理

多功能性和高性能

nShield Connect 和 nShield Solo 硬件安全模块提供了三种性能级别，以适合您的事务处理速度适中或应用程序要求高吞吐量的环境。nShield 即服务是基于订阅的解决方案，可用于访问云端的 nShield 硬件安全模块，这是以我们最高性能的 nShield Connect XC 为基础的。

行业标准认证

Entrust 遵循严格的行业标准，可帮助您在受监管的环境中证明合规性，同时对 nShield 硬件安全模块的安全性和完整性充满信心。以下是我们遵守的标准列表一览。我们的网站和数据表提供了完整列表。

FIPS 140-2

FIPS 140-2 是全球认可的美国政府 NIST 标准，可验证加密模块的安全健壮性。所有 Entrust nShield 硬件安全模块均已通过 FIPS 140-2 2 级和 3 级认证。

FIPS Level 3 Validated 140-2

Common Criteria

Common Criteria 和 eIDAS 合规

nShield XC 和 nShield + 硬件安全模块已通过 Common Criteria EAL 4+ 认证，并被 eIDAS 法规认可为合格的签名创建设备 (QSCD)。另外，nShield Solo XC 和 Connect XC 硬件安全模块符合 Common Criteria 保护规范 EN 419 221-5“用于信任服务的加密模块”。因此，nShield 硬件安全模块可以充当欧盟成员国和企业的数字化安全基干技术。这包括支持国家身份证项目和跨境服务、电子文档和交易签名服务，以及身份验证、时间戳、安全电子邮件和长期文档保存服务。尽管这些认证属于欧洲法规的范畴，全球许多国家/地区同样也在采用这些认证。

如需进一步了解

请访问 **entrust.com/HSM**，了解我们如何在您的内部、云端和虚拟环境中保护您的业务关键信息和应用程序。

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