Entrust CodeSafe®

经认证的敏感应用程序硬件保护

精彩亮点

CodeSafe：在安全环境中执行代码

- 在防篡改的硬件安全模块 (HSM) 内执行敏感应用程序，以此提供保障
- 通过 数字签名和验证代码，帮助确保完整性
- 强制实施策略，提供安全的密钥管理环境
- 将密钥与证书以独特方式与应用程序连结，实现强有力的访问权限控制
- 使用远程 CodeSafe 工具，提供便利的解决方案

CodeSafe 工具组使开发人员可以在 FIPS 认证的 nShield 硬件安全模块防篡改领域内编写和执行敏感应用程序。在安全执行环境中运行的应用程序可以对数据进行加密、解密和处理，硬件安全模块强制实施的策略可控制应用程序密钥的使用，进一步确保安全。

丰富多样的应用程序

CodeSafe 可用于保护任何类型的应用程序。这包括与银行业务、智能计量、身份验证代理、数字签名代理和定制加密进程关联的密码学和高价值业务逻辑。

确保 CodeSafe 应用程序的完整性

CodeSafe 提供多种工具，可对在 nShield 的安全执行环境中运行的应用程序进行数字签名，以便硬件安全模块在运行时验证其完整性。

Entrust CodeSafe®

关键功能和优点

CodeSafe 密钥策略实施和访问权限控制

CodeSafe 允许软件所有者定义应用程序数据（包括密钥和证书）使用情况的管理策略，并强制执行这些策略，从而保障安全的密钥管理环境。CodeSafe 还别具一格地将密钥和证书与指定的应用程序关联，确保提供强有力的访问权限控制。

保护 SSL/TLS 端点安全

CodeSafe 应用程序开发人员可以在他们的应用程序中嵌入 OpenSSL 库，以终止 nShield 硬件安全模块中的 SSL/TLS 会话，从而促进端到端加密，增强数据传输层的安全性，并减少攻击面。

远程部署和更新

管理员可从中心位置部署应用程序，无需物理访问硬件安全模块。

nShield 兼容性

CodeSafe 可用于 FIPS 140-2 3 级认证的 nShield Solo PCIe 和网络连接的 nShield Connect 硬件安全模块。兼容型号包括所有支持的 nShield Solo 和 nShield Connect 硬件安全模块，包括 XC 产品线。

硬件安全模块开发环境

CodeSafe 可兼容以下编程应用程序：

- 对于嵌入式应用程序，可兼容 C 和 C++ 编程语言
- 对于主机服务器，可兼容 C、C++ 和 Java

CodeSafe 使用入门

如需使用 CodeSafe，您需要：

- 经过 FIPS 140-2 3 级认证的 nShield Solo 或 nShield Connect 硬件安全模块
- CodeSafe 开发人员工具包
- CodeSafe 激活许可证

CodeSafe 开发人员工具包包含教程、文档和样例程序，帮助您将应用程序与 nShield 硬件安全模块集成。Entrust 专业服务团队随时待命，帮助您实现集成。

进一步了解

可应要求提供 CodeSafe 白皮书，详细阅读关于其底层技术的深入探讨。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