cpl.thalesgroup.com

THALES

Thales Luna USB HSM

版本 5.x 和 6.x

Thales Luna USB硬件安全模块(HSM)是一种小型化HSM设备。政府、金融机构和大型企业可以用其作为硬件加密信任根(Root of Trust)，为敏感数据、应用系统和数字身份识别降低安全风险，确保符合法规要求。Luna USB HSM非常适合用于证书颁发机构 (CA) 根密钥的保护以及概念验证 (PoC) 测试。

Thales Luna USB HSM概述

Thales Luna USB HSM提供了业界领先的密钥保护方案，其特点在于可在硬件内部维护所有密钥材料。小型化和离线密钥存储的能力使其与众不同，对需要利用HSM设备移动、运输和存储CA根密钥的客户非常有吸引力。

算法	型号
	Luna USB HSM
RSA-1024	200 tps
RSA-2048	63 tps
ECC P256	43 tps
ECIES	20 tps
AES-GCM	71 tps

加密功能

Luna USB HSM支持广泛的非对称密钥加密和密钥交换功能，并且支持所有标准对称加密算法。它还支持所有标准散列算法和消息认证码 (MAC)。Luna USB HSM提供了符合NIST SP800-90标准的硬件随机数生成能力。

Luna USB HSM支持的ECC密钥对, 可用于需要原厂生成并固化在HSM内部的数字ID的Suite B算法。

优势和特点

最安全

- 密钥始终在硬件内部
- 远程管理
- 多级访问控制
- 组件拆分，确保可信交付
- 防入侵、防篡改硬件
- 安全审核日志
- 最强的加密算法
- 支持Suite B算法
- 安全报废

应用示例

- PKI密钥生成和密钥存储(在线和离线CA密钥)
- 证书验证和签名

篡改恢复角色

Luna USB HSM有完善的篡改检测和响应电路，可在HSM受到攻击时自动使内部密钥归零。为了平衡这种极端的安全性和对最终用户的易用性，Luna USB HSM具备一项功能，可使通过身份验证的安全管理人员能够从意外篡改事件中恢复数据，让HSM迅速回复可用状态，并且不会损失任何密钥或敏感数据。

安全运输模式

Luna USB HSM篡改响应电路还可以用于安全运输模式。运输设备前，安全管理人员可使用设备的篡改恢复角色密钥以加密的方式锁定HSM。恢复角色密钥可以单独运输，然后在到达目的地后重新组合，以解密的方式验证HSM的完整性。

通用架构

Thales通用型HSM采用了标准架构，此架构中的客户端、程序开发接口、算法和身份验证方法在整个通用型HSM产品系列中都是一致的。此特点消除了为不同型号HSM开发专门应用的需求，提供了密钥在各种型号间灵活迁移的能力。

技术规格

支持的操作系统

- Windows, Linux

客户端

- 通用Luna Client

加密API

- PKCS#11、Java (JCA/JCE)、Microsoft CAPI 和 CNG、OpenSSL

加密算法

- 支持全系列Suite B加密算法
- 非对称加密：RSA (1024-8192)、DSA (1024-3072)、Diffie-Hellman、KCDSA、椭圆曲线加密算法 (ECDSA, ECDH, ECIES), 包括命名的、用户自定义曲线以及Brainpool曲线
- 对称加密：AES、RC2、RC4、RC5、CAST、DES、Triple DES、ARIA、SEED
- 散列/消息摘要/HMAC：SHA-1、SHA-2(224-512)、SSL3-MD5-MAC、SSL3-SHA-1-MAC
- 随机数生成：符合FIPS 140-2要求的DRBG(SP800-90 CTR模式)

物理特性

- 尺寸：8.5" x 6.7" x 1.7" (216mm x 170mm x 43mm)
- 重量：3.3lb (1.5kg)
- 输入电压：100-240V, 50-60Hz
- 功耗：最高26W，日常20W
- 温度：运行时0℃ – 35℃, 存储时-20℃ – 70℃
- 相对湿度：20% – 95% (38℃)无冷凝

安全认证

- FIPS 140-2 二级和三级
- BAC & EAC ePassport支持

安全和环境合规性

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- TAA

主机接口

- USB 2.0

可靠性

- MTBF: 858,824小时

关于Thales

您所信赖的能够保护您隐私的机构都依靠Thales保护他们的数据。各机构在数据安全方面必须面对的决定性时刻越来越多。无论这些决定性时刻是制定加密策略、转移到云，还是需要遵守合规要求，您都可以依靠Thales为您的数字化转型之旅保驾护航。

决定性时刻需要决定性技术。