cpl.thalesgroup.com

THALES

Thales Luna PCIe HSM

通过在Thales Luna PCIe HSM(高可信、防篡改、PCIe卡)中存储、保护和管理加密密钥，保护敏感数据和关键应用。为应用程序提供专用高性能加密处理器的特定访问权限。快速将这种经济高效的解决方案直接嵌入服务器和安全设备，从而获得满足FIPS 140-2标准的保障。

联系我们并了解Luna PCIe HSM如何在密钥生命周期中保证密钥的完整性和安全性。

您需要了解的优势：

优异的性能和易用性

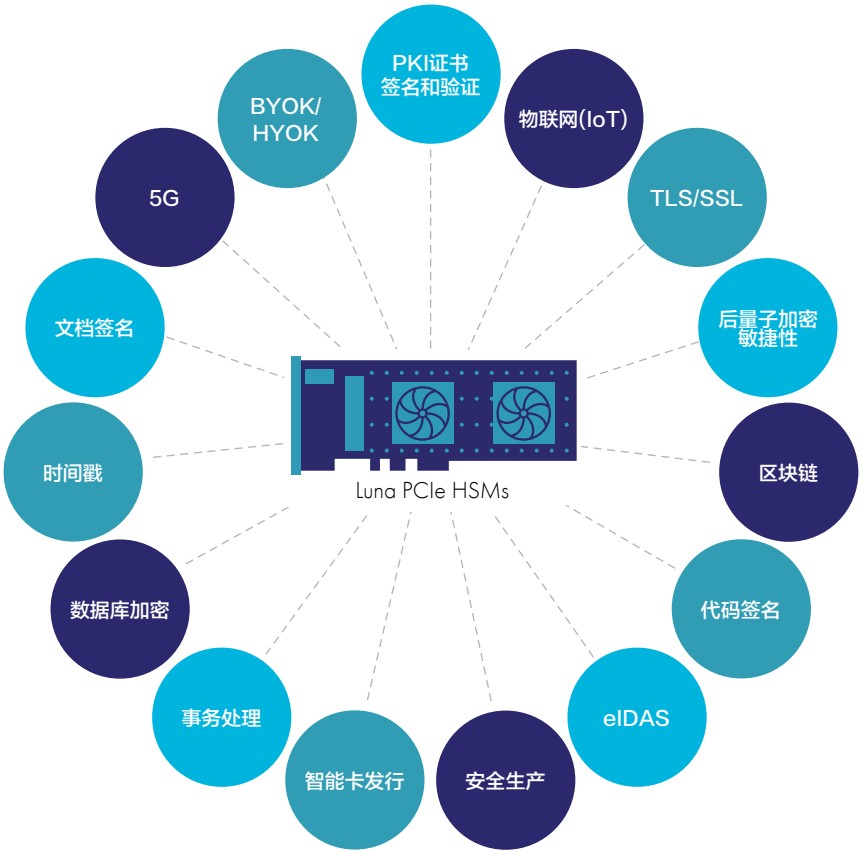
- 对于高性能应用场景，每秒可超过20,000次ECC或10,000次RSA操作，是市场上最快的HSM
- 低延迟，高效率
- 专用的应用访问权限
- 半高度PCIe卡

功能模块

- 扩展本地HSM功能
- 在HSM的安全界限内开发和部署自定义代码

最高的安全性和合规性

- 密钥一直保存在通过FIPS验证的防篡改硬件中
- 满足GDPR、eIDAS、HIPAA、PCI-DSS等的合规性要求
- 多重角色以实现高度职责分离
- 多人以MofN 多因素认证方式实现高度安全性
- 安全审核日志
- 安全运输模式提高交付可信度



技术规格

支持的操作系统

- Windows, Linux

API支持

- 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、DSA、Diffie-Hellman、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、KCDSA、SM2等
- 对称加密：AES、AES-GCM、Triple DES、DES、ARIA、SEED、SM4、RCS、RC4、RC5、CAST等
- 散列/消息摘要/HMAC：SHA-1、SHA-2、SM3等
- 密钥派生：SP800-108计数器模式
- 密钥包装：SP800-38F
- 随机数生成：符合AIS 20/31至DRG.4，使用基于硬件的真噪音源，满足NIST 800-90A的CTR-DRBG规范
- 数字钱包加密：BIP32

安全认证

- FIPS 140-2 三级 — 密码和多因素(PED)认证
- eIDAS CC EAL4+(AVA_VAN.5和ALC_FLR.2)，根据保护配置文件419221-5*

物理特性

- 半高度PCIe卡
- 尺寸：70mm x 167mm x 187mm (2.74" x 6.57" x 0.74")
- 功耗：最高18W，日常14W
- 散热：最高61.4BTU/h，日常47.8BTU/h
- 温度：运行0℃ – 50℃，存储-20℃ – 60℃
- 相对湿度：5% – 95% (38℃) 无冷凝

安全和环保合规性

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC MARK
- RoHS2, WEEE
- TAA

主机接口

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

可靠性

- 备份/恢复
- 高可用性(HA)
- 平均故障间隔(MTBF) 997,508小时

* 正在评定中

可用型号

Luna PCIe HSM有两个系列可供选择，每个都有三种不同的型号可以满足您的要求。

Luna A系列:

密码验证，方便管理。

标准性能: A700	企业性能: A750	最高性能: A790
内存: 2MB	内存: 16MB	内存: 32MB
性能: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**性能:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**性能:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S系列:

多因素(PED)身份验证，用于需要高可信度的部署环境。

标准性能: S700	企业性能: S750	最高性能: S790
内存: 2MB	内存: 16MB	内存: 32MB
性能: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**性能:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**性能:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps: 每秒处理次数

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、迁移到云，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。