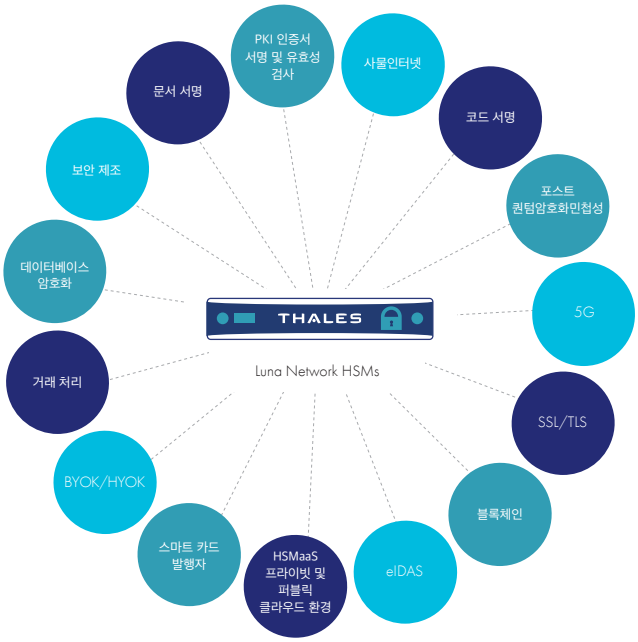
cpl.thalesgroup.com

Thales Luna Network HSM

업계 최고의 성능을 제공하는 높은 보증, 변조 방지, 네트워크 연결 어플라이언스 - 기업의 민감 데이터와 중요한 애플리케이션을 Luna Network 하드웨어 보안 모듈(HSM)의 암호화 키로 저장, 보호, 관리하여 안전하게 지키십시오.

저희 탈레스에서는 문의해주시는 고객께 Luna Network HSM을 다양한 애플리케이션과 연동하여 암호화 작업을 가속화하고 암호키 수명 주기를 안전하게 지키며 전체 암호화 인프라스트럭처에 대한 신뢰 루트를 제공하는 방법을 상세히 알려드리고 있습니다.



장점

월등한 성능:

- 고성능 사용 사례에 맞춘 초당 20,000 이상의 ECC 및 10,000 이상의 RSA 작업을 수행함으로써 높은 처리량 요구 조건 충족
- 더욱 짧은 대기 시간으로 효율성 향상

최고 수준의 보안 및 규제 준수:

- 키는 언제나 FIPS 인증을 받은, 변조 방지 하드웨어에 유지
- GDPR, eIDAS, HIPAA, PCI-DSS 등의 다양한 규제 준수 필요 충족
- 클라우드 환경을 위한 표준
- 강력한 권한관리를 위한 기능
- 보안 강화를 위한 멀티팩터 인증 기반의 다인용 MofN
- 보안 감사 로깅
- 보안 송수신 모드를 통한 안전한 전송
- 외부 Quantum RNG 시딩을 통한 고품질 키
- Luna Backup HSM를 또는 클라우드 인프라를 위해서는 Data Protection on Demand를 활용하여 하드웨어에서 암호키를 안전하게 백업하고 복제함으로써 중복성, 신뢰성 유지 및 재해복구

비용 및 시간 절감:

- HSM 원격 관리 - 이동 불필요
- 감사 및 규제 준수 비용 및 부담 경감
- 기업 시스템 자동화로 REST API를 통해 HSM 관리
- 복수의 애플리케이션 또는 테넌트 간에 HSM을 공유하여 리소스를 효율적으로 관리
- 키 관리 및 규제 준수 니즈를 충족시키는 유연한 파티션 정책
- Luna Client를 컨테이너에서 사용함으로써 휴대성과 효율성 향상 및 오버헤드 감소
- 기능 모듈
  - 기본 HSM 기능 확장
  - HSM의 안전 격리 범위 내에서 사용자 정의 코드 개발 및 배포

기술 사양

지원 운영체제

- Windows, Linux, Solaris, AIX
- 가상: VMware, Hyper-V, Xen, KVM

API 지원

- PKCS#11, Java (JCA/JCE), Microsoft CAPI 및 CNG, OpenSSL
- 관리용 REST API

암호화

- Suite B 완벽 지원
- 비대칭: RSA, DSA, Diffie-Hellman, KCDSA, 표준/사용자 정의/ Brainpool ECC (ECDSA, ECDH, Ed25519, ECIES) 등
- 대칭: AES, AES-GCM, 트리플 DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST 등
- 해시/메시지 다이제스트/HMAC: SHA-1, SHA-2, SM3 등
- 키 유도: SP800-108 카운터 모드
- 키 랩핑: SP800-38F
- 난수 생성: NIST 800-90A 표준 준수 CTR-DRBG와 함께 하드웨어 기반의 트루 노이즈 소스를 사용하여 최대 DRG.4 수준의 AIS 20/31을 준수하도록 설계
- 전자지갑 암호화: BIP32
- 가입자 인증을 위한 5G 암호화 메커니즘: Milenage, Tuak 및 COMP128

보안 인증

- FIPS 140-2 레벨 3 - 비밀번호 및 멀티 팩터(PED)
- 보호 프로파일 419221-5 대비 CC EAL4+ (AVA_VAN.5 및 ALC_ FLR.2)
- eIDAS규제 충족을 위한 서명 또는 보안 생성 장비(QSCD)
- 싱가폴 NITES CC인증*
- 보호 프로파일 419221-5 대비 eIDAS CC EAL4+ (AVA_VAN.5 및 ALC_FLR.2) *

호스트 인터페이스

- 2가지 옵션: 4기가비트 이더넷 포트(포트 본딩 기능 포함) 또는 2 x 10 기가 네트워크 연결 및 2 x 1기가 포트 본딩
- IPv4 및 IPv6

물리적 특성

- 표준 1유닛 19인치 랙 마운트 어플라이언스
- 크기: 19” x 21” x 1.725” (482.6mm x 533.4mm x 43.815mm)
- 무게: 28lb (12.7kg)
- 입력 전압: 100-240V, 50-60Hz
- 소비 전력: 110W 최대, 84W 일반
- 방열: 376BTU/hr 최대, 287BTU/hr 일반
- 온도: 작동 0°C - 35°C, 보관 -20°C - 60°C
- 상대 습도: 5%에서 95%까지(38°C) 비응축

안전 및 환경 규제 준수

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC Mark
- RoHS2, WEEE
- TAA
- 인도 BIS [IS 13252 (Part 1)/IEC 60950-1]

신뢰도

- 듀얼 핫스왑 전원 공급 장치
- 현장 서비스 가능 컴포넌트
- MTBF(평균 무고장 시간) 171,308시간

관리 및 모니터링

- HA 재난 복구
- 백업 및 복원
- SNMP, Syslog

*평가 중

사용 가능 모델

Luna Network HSM의 두 시리즈 중에서 택하실 수 있습니다. 각 시리즈는 3종의 모델로 구성되어 있어 사용 요건에 따라 맞추어 선택이 가능합니다.

Luna A 시리즈:

손쉬운 관리를 위한 비밀번호 인증.

표준 성능: A700	기업용 성능: A750	최대 성능: A790
2 MB 메모리	16 MB 메모리	32 MB 메모리
파티션: 5	파티션: 5	파티션: 10
최대 파티션: 5	최대 파티션: 20	최대 파티션: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S 시리즈:

높은 보증 사용 사례를 위한 멀티 팩터(PED) 인증.

표준 성능: S700	기업용 성능: S750	최대 성능: S790
2 MB 메모리	16 MB 메모리	32 MB 메모리
파티션: 5	파티션: 5	파티션: 10
최대 파티션: 5	최대 파티션: 20	최대 파티션: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = 초당 트랜잭션

탈레스 소개

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.

> cpl.thalesgroup.com <

문의 – 사무소 위치 및 연락처 목록은 cpl.thalesgroup.com/ko/contact-us 에서 확인하실 수 있습니다.