제품 소개서

Luna Network HSM

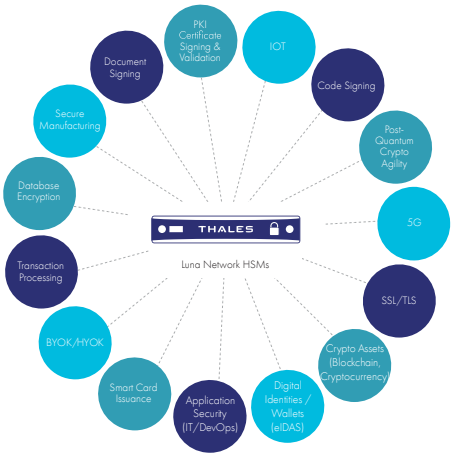
cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Thales Luna Network 하드웨어 보안 모듈(HSM)에서 암호화 키를 저장, 보호 및 관리하여 민감한 데이터와 중요 애플리케이션을 보호하세요. 이 제품은 고도의 신뢰성, 변조 방지 기능을 갖춘 네트워크 연결형 어플라이언스로 최고의 성능과 암호화 민첩성을 제공합니다.
Luna Network HSM을 다양한 애플리케이션에 통합하여 암호화 작업을 가속화하고, 암호화 키 수명 주기를 보호하며, 전체 암호화 인프라에 대한 신뢰 기반을 제공하는 방법에 대해 알아보려면 문의하십시오.

주요 특징 및 장점:



우수한 성능:

- 초당 20,000건 이상의 ECC 및 초당10,000건의 RSA 작업으로 높은 처리량 요구 사항 충족
- 효율성 향상을 위한 최소화된 지연시간

최고 수준의 보안 및 규정 준수:

- 키는 항상 FIPS 인증된 변조 방지 하드웨어에 보관
- GDPR, eIDAS, HIPAA, PCI-DSS 등의 규정 준수 요구 사항 충족
- 클라우드의 사실상 표준
- 강력한 업무 분리를 위한 다중 역할 지원
- 보안 강화를 위한 다중 인증이 포함된 다중 인원 MofN 사용
- 보안 감사 로깅
- 보안 전송 모드를 통한 고도의 보안 제공
- 이중(내부/외부) 엔트로피 소스 지원 및 주요 QRNG 벤더와의 통합으로 강력한 키 생성
- Luna Backup HSM을 사용한 하드웨어나 Data Protection on Demand를 통한 클라우드로 키를 안전하게 백업 및 복제하여 중복성, 안정성 및 재해 복구 보장

비용 절감 및 시간 절약:

- HSM 원격 관리 – 출장 필요 없음
- 감사 및 규정 준수 비용과 부담 감소
- REST API를 통한 HSM 관리 시스템 자동화
- 여러 애플리케이션 또는 테넌트 간에 HSM을 공유하여 자원을 효율적으로 관리
- 키 관리 및 규정 준수 요구 사항을 충족하는 유연한 파티션 정책
- 컨테이너에서 Luna Client를 사용하여 이식성 증가, 효율성 향상 및 오버헤드 감소
- Functional Module
  - 기본 HSM 기능 확장
  - HSM의 보안 경계 내에서 사용자 정의 코드 개발 및 배포

환경 친화적 설계:

Thales Luna HSM은 Thales의 ESG(환경, 사회 및 거버넌스) 약속에 따라 에코 디자인을 통해 각 HSM 세대별로 탄소 발자국을 측정 가능하고 현저히 감소시키며, 전력 소비 및 운영 비용을 줄이기 위해 노력합니다.

기술 사양

지원 운영체제

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

API 지원

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

암호화

- Luna PQC 기능 모듈 내의 포스트 퀀텀 메커니즘
- 완전한 Suite B 지원
- 비대칭: RSA, DSA, Diffie-Hellman, 타원 곡선 암호화 (ECDSA, ECDH, Ed25519, ECIES)와 명명된, 사용자 정의 및 Brainpool 곡선, KCDSA 등
- 대칭: AES, AES-GCM, 트리플 DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST 등
- 해시/메시지 다이제스트/HMAC: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4 등
- 키 파생: SP800-108 카운터 모드
- 키 래핑: SP800-38F
- 난수 생성: NIST 800-90A 준수 CTR-DRBG와 함께 하드웨어 기반 진정한 노이즈 소스를 사용하여 AIS 20/31의 DRG.4를 준수하도록 설계됨

5G 암호화 메커니즘:

- 가입자 인증: Milenage, Tuak, COMP128
- 가입자 개인정보 보호 : ECIES

보안 인증

- FIPS 140-2 레벨 3 인증 – 비밀번호 및 다중 인증(PED)
- FIPS 140-3 레벨 3 인증 – 비밀번호 및 다중 인증(PED)
- 보호 프로파일 EN 419 221-5에 대한 Common Criteria EAL4+(AVA_VAN.5 및 ALC_FLR.2) 인증
- eIDAS 준수를 위한 적격 서명 또는 인감 생성 장치(QSCD) 등재
- 브라질 INMETRO 승인(이전 ITI)
- 싱가포르 NITES Common Criteria 체계

호스트 인터페이스

- IPv4 and IPv6
- 포트 본딩 2가지 옵션:
  - 모든 기기에 기본 제공되는 4 x 1G RJ45 이더넷 포트
  - 광섬유 네트워크 연결을 위한 2 x 10G SFP+ 포트 및 2 x 1G(790 모델만 해당)

물리적 특성

- 표준 1U 19인치 랙 마운트 기기
- 크기: 19" x 21" x 1.725"(482.6mm x 533.4mm x 43.815mm)
- 무게: 28lb(12.7kg)
- 입력 전압: 100-240v AC, 50-60Hz
- 전력 소비: 최대 100W, 일반 84W
- 열 발산: 최대 376BTU/hr, 일반 287BTU/hr
- 온도: 작동 0°C ~ 35°C, 보관 -20°C ~ 60°C
- 상대 습도: 5% ~ 95%(38°C) 비응축

안전 및 환경 규정 준수

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

신뢰성

- 이중 핫스왑 전원 공급 장치
- 현장 수리 가능 구성 요소
- 평균 고장 간격 시간 (MTBF) 171,308 시간

관리 및 모니터링

- HA 장애 조치 / 부하 분산
- 현장 또는 클라우드에서 하드웨어 간 백업 및 복원
- SNMP, Syslog

사용 가능한 모델

요구 사항에 맞는 Luna Network HSM의 두 시리즈 중에서 선택하세요. 각 시리즈는 3가지 다른 모델로 제공됩니다.

Luna A 시리즈:

손쉬운 관리를 위한 비밀번호 인증

표준 성능 A700	기업용 성능 A750	최대 성능 A790
최대 4 MB 메모리	최대 32 MB 메모리	최대 64 MB 메모리
파티션: 5	파티션: 5	파티션: 10
최대 파티션: 5	최대 파티션: 20	최대 파티션: 100
성능:	**성능:**	**성능:**
RSA-2048: 1,000 tps	RSA-2048: 5,000 tps	RSA-2048: 10,000 tps
ECC P256: 2,000 tps	ECC P256: 10,000 tps	ECC P256: 22,000 tps
AES-GCM: 2,000 tps	AES-GCM: 10,000 tps	AES-GCM: 17,000 tps

Luna S 시리즈:

고도의 보안 사용 사례를 위한 다중 인증(PED).

표준 성능 S700	기업용 성능 S750	최대 성능 S790
최대 4 MB 메모리	최대 32 MB 메모리	최대 64 MB 메모리
파티션: 5	파티션: 5	파티션: 10
최대 파티션: 5	최대 파티션: 20	최대 파티션: 100
성능:	**성능:**	**성능:**
RSA-2048: 1,000 tps	RSA-2048: 5,000 tps	RSA-2048: 10,000 tps
ECC P256: 2,000 tps	ECC P256: 10,000 tps	ECC P256: 22,000 tps
AES-GCM: 2,000 tps	AES-GCM: 10,000 tps	AES-GCM: 17,000 tps

tps = transactions per second

문의 – 서울특별시 용산구 독서당대로 98 6층 탈레스코리아 82.2.3278.8202 cpl.thalesgroup.com/ko/contact-us