

제품 개요

THALES

CYBERSECURITY

Luna 8 Network HSM

디지털 신뢰의 기반



cpl.thalesgroup.com

Luna 8 Network HSM 소개

확장성, 멀티 테넌트, 고성능 보안 및 신뢰성을 제공하는 양자 내성 신뢰 기반

Luna Network 하드웨어 보안 모듈(HSM)을 통해 민감한 데이터, 신원 및 핵심 애플리케이션을 안전하게 보호하십시오. 암호화 키를 안전하게 저장, 보호 및 관리하도록 설계된 고신뢰성, 양자 내성(Quantum-Safe), tampere 방지(Tamper-Resistant) 어플라이언스는 양자내성 암호(PQC) 워크로드를 위한 확장 가능한 멀티 테넌트 보안과 업계 최고의 성능을 제공합니다. Thales가 자체 설계한 암호화 프로세서로 구동되는 Luna 8은 진화하는 비즈니스 요구사항, 새로운 위협 및 새로운 암호화 알고리즘에 신속하게 적응하는 데 필요한 높은 처리량, 강력한 보안 격리, 그리고 암호 민첩성을 제공합니다.

Luna Network HSM이 어떻게 통합을 가속화하고, 하드웨어 내에서 전체 암호화 키 수명주기를 보호하며, 컴플라이언스를 간소화하는 데 도움을 줄 수 있는지 알아보려면 당사에 문의하십시오. 광범위한 애플리케이션을 지원하는 Luna Network HSM은 전체 암호화 인프라를 보호하고 미래에도 대비할 수 있는 양자 내성 신뢰 기반을 구축할 수 있도록 지원합니다.

최고의 보안 및 컴플라이언스

- 키는 항상 변조 탐지(Tamper-evident) 하드웨어 내에 안전하게 보관
- GDPR, eIDAS, HIPAA, PCI-DSS 등의 규정 준수 요구사항 충족 설계
- 강력한 직무 분리를 위한 다중 역할 체계 지원
- 보안 강화를 위한 M of N 기반의 쿼럼 승인 및 다중 요소 인증(MFA) 지원
- Thales 자체 설계 암호 프로세서를 위한 부채널 공격(Side-channel) 보호
- 디바이스 인증(Device Attestation)을 통한 고신뢰 배포 및 공급망 무결성 보장
- 온보드 듀얼 엔트로피 소스(QRNG 양자 난수 생성기 포함) 및 외부 엔트로피 소스 지원
- 이중화, 신뢰성 및 재해 복구를 위해 Luna Backup HSM을 통한 하드웨어 간 안전한 키 백업



확장 및 운영 비용 최적화

- 어플라이언스당 1개 또는 2개의 독립된 암호 모듈 탑재 가능 (동일 랙 공간에서 2배 밀도 제공)
- 각 암호 모듈당 최대 15개 HSM 인스턴스 호스팅 (듀얼 모듈 구성 시 어플라이언스당 최대 30개 인스턴스 지원)
- 동일 하드웨어 내 보안 컨테이너 환경에서 복수의 Luna 8 펌웨어 버전 동시 실행
- API 및 CLI 도구를 통한 HSM 관리 및 운영 프로세스 자동화
- 모니터링, 로깅 및 메트릭 수집을 위한 기존 IT 인프라 도구와의 손쉬운 통합
- 대역 외(Out-of-band) 진단 및 하드웨어 사용률 메트릭 제공
- 키 관리 및 컴플라이언스 요구사항을 충족하는 유연한 보안 정책
- 컨테이너 기반 Luna Client 사용으로 뛰어난 이식성, 높은 운영 효율성 및 오버헤드 최소화

친환경 설계

Thales HSM은 친환경 설계를 통해 탄소 배출량을 현저하게 절감했습니다. Thales의 ESG(환경·사회·지배구조) 약속에 발맞추어, Luna 8은 Luna 7 대비 트랜잭션당 에너지 효율이 최대 20배 향상되었습니다.

기술 사양

지원 운영체제

- Windows, Linux
- 가상화: VMware, Hyper-V, Xen, KVM
- 지원 API (API Support)
- PKCS#11, Java (JCA/JCE), Microsoft CAPI 및 CNG, OpenSSL
- 관리 및 운영을 위한 REST API

양자내성암호 (PQC)

- ML-KEM (FIPS 203 키 캡슐화) 및 ML-DSA (FIPS 204 전자서명)
- 상태 기반 해시 서명: LMS 및 다중 레벨 HSS (RFC 8554 / NIST SP 800-208)

타원 곡선 암호화 (ECC)

- FIPS 승인 NIST Prime 곡선 (P-192, P-224, P-256, P-384, P-521) 및 Brainpool 곡선 (P192 ~ P512) - ECDSA/ECDH, ECIES 지원
- Koblitz 곡선 (secp256k1) - BIP32 계층 결정론적 지갑 키 관리
- Montgomery (X25519, X448) 및 Edwards (Ed25519, Ed448) 곡선

비대칭 및 대칭

- 비대칭: RSA (최대 4096비트) - 표준 PKCS#1 v1.5, OAEP 및 FIPS 승인 PSS 확률적 서명 생성 지원
- 대칭: AES (128, 192, 256비트) - ECB, CBC, CBC-PAD, CTR, GCM, GMAC, Key Wrap 및 512비트 AES-XTS 모드 지원, ARIA, SEED 지원
- 레거시: Triple-DES (3DES) CBC/ECB (하위 호환 복호화/인래핑 전용 지원)

보안 해시, KDF 및 통신사/통신망

- SHA-2 및 SHA-3 보안 해시 (224 ~ 512비트) 및 HMAC
- SHAKE-128, SHAKE-256 확장 가능 출력 함수 (XOF)
- 키 파생: NIST SP 800-108 카운터 모드
- 키 래핑: NIST SP 800-38F
- 3GPP 모바일 셀룰러 통신 보안: MILENAGE, TUAK, COMP 128 가입자 인증 프로파일

디지털 월렛 및 블록체인 수탁

- BIP32 및 SLIP10 계층 결정론적(HD) 키 관리

난수 생성(RNG)

- 하드웨어 기반 트루 노이즈 소스 및 NIST 800-90A 준수 HMAC_DRBG를 결합하여 AIS 20/31 DRG.4 표준 준수 설계
- 보안 인증
- FIPS 140-3 Level 3*
- Common Criteria EAL4+ (AVA_VAN.5 및 ALC_FLR.2) - 보호 프로파일 EN 419 221-5 인증*
- eIDAS 2 준수를 위한 적격 서명/인장 생성 장치(QSCD) 등재*

네트워크 (Network)

- 4x 10G SFP+ (멀티모드 또는 싱글모드 광케이블 및 RJ45 구리선)
- IPv4, IPv6*, 포트 본딩(Port Bonding)* 지원
- 베이스보드 관리 컨트롤러(BMC) 전용 1x 1G RJ45 이더넷 포트

물리적 특성

- 표준 1U 19인치 랙 장착형 어플라이언스
- 크기:
 - 17.44" (W) x 21.95" (D) x 1.71" (H)
 - 443mm (W) x 557.6mm (D) x 43.5mm (H)
- 무게:
 - 단일 모듈 어플라이언스: 12kg (26.5lbs)
 - 듀얼 모듈 어플라이언스: 13.6kg (30lbs)
- 입력 전압: 100-240V AC, 50-60Hz
- 일반 소비전력:
 - 단일 모듈 어플라이언스 ~ 135W
 - 듀얼 모듈 어플라이언스 ~ 270W
- 최대 소비전력:
 - 단일 모듈 어플라이언스 ~ 225W
 - 듀얼 모듈 어플라이언스 ~ 450W
- 온도: 작동 0°C ~ 40°C, 보관 -20°C ~ 60°C
- 상대 습도: 5% ~ 95% (38°C, 비응축)

안전 및 환경 규정 준수

- 80 PLUS Platinum 인증
- UL, CSA, CE
- FCC, CE
- RoHS3, WEEE
- TAA
- 인도 BIS [IS 13252 (Part 1)/IEC 60950-1]*

신뢰성 (Reliability)

- 이중 핫스왑 지원 전원 공급 장치 및 팬
- 평균 무고장 시간 (MTBF)
 - 단일 모듈 어플라이언스: 289,444시간
 - 듀얼 모듈 어플라이언스: 171,236시간

관리 및 모니터링

- 양자 내성 HA 페일오버 / 로드 밸런싱(부하 분산)
- 하드웨어 간 양자 안전 백업 및 복원
- 대역 외(out-of-band) 진단을 위한 rsyslog 및 BMC



제공되는 Luna Network HSM 모델

모델 (MODELS)			
	Luna 100 (기본 성능 / Standard)	Luna 150 (엔터프라이즈 성능)	Luna 190 (최고 성능)
보안 컨테이너 수	1개	최대 6개	최대 15개
키 저장 용량	128 MB	1024 MB	4096 MB

Luna 8 Network HSM은 처리 성능, 암호화 키 저장 용량 및 지원되는 컨테이너 수에 따라 세 가지 모델로 제공됩니다. 각 모델은 일반적인 구축 배포 요구사항에 최적화되어 있어 환경에 적합한 솔루션을 쉽게 선택할 수 있습니다. 각 보안 컨테이너는 완벽히 격리된 Luna 8 HSM 인스턴스를 호스팅하며 최대 10개의 파티션을 지원합니다.

Thales 소개

Thales는 사이버 보안 분야의 글로벌 리더로서, 전 세계 기업, 정부 및 신뢰받는 기관들이 중요 애플리케이션, 민감한 데이터, 신원 및 소프트웨어를 규모에 관계없이 최고의 ROI로 안전하게 보호할 수 있도록 지원합니다. Fortune Global 500대 기업의 58%를 포함한 30,000 개 이상의 고객사를 보유하고 있으며, 148개국에 솔루션이 배포되어 있습니다. 혁신적인 서비스와 통합 플랫폼을 통해 Thales는 위험에 대한 가시성을 확보하고 사이버 위협을 방어하며 컴플라이언스 격차를 해소하고 매일 수십억 명의 사용자에게 신뢰할 수 있는 디지털 경험을 제공합니다.