cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer 3 Network HSMs

ProtectServer 3 External
ProtectServer 3+ External

Thales ProtectServer 3 Network HSM(Hardware Security Module)은 보안이 강화된 네트워크 암호화 서버로, 암호화 키가 손상되지 않게 보호하는 동시에 민감한 애플리케이션을 보호하기 위한 암호화, 서명 및 인증 서비스를 제공하도록 설계되었습니다.

ProtectServer 3 External HSM

ProtectServer 3+ External HSM

뛰어난 보안성

ProtectServer Network HSM에는 높은 보증 (High assurance) 방식으로 안전하게 암호화 처리를 수행하는 암호화 모듈이 포함되어 있습니다. 변조 방지 보안 기능과 견고한 강철 케이스를 갖추고 있는 이 어플라이언스는 물리적 공격으로부터 시스템을 보호하고, 암호화 키, PINS 등 매우 민감한 정보를 저장 및 처리할 때 최고 수준의 물리적/논리적 보호를 제공할 수 있습니다. 안전하게 저장 및 처리가 이루어지기 때문에 암호화 키가 HSM 외부에 평문 형태로 노출되는 일이 없습니다. 이를 통해 고객에게 다른 소프트웨어에서 경험할 수 없는 수준의 뛰어난 보안과 업계 조직의 보안 요구를 충족하는 공인된 수준의 기밀성과 무결성을 제공합니다.

유연한 프로그래밍

ProtectServer HSM은 애플리케이션 개발자가 자체 펌웨어를 개발하고 HSM의 보안 범위 내에서 이를 실행할 수 있도록 독보적 수준의 유연성을 제공합니다. 기능 모듈(Functionality Modules)이라고도 하는 이러한 툴킷은 맞춤형 펌웨어를 개발 및 배포하기 위한 포괄적 기능을 제공합니다. 모든 기능을 갖춘 소프트웨어 에뮬레이터가 포함된 유연한 개발 도구 덕분에 개발자는 데스크탑 컴퓨터를 사용하듯 편리하게 맞춤형 펌웨어를 테스트 및 디버그할 수 있습니다.

이점

성능

- 초당 3500건의 RSA-1024 서명

보안

- FIPS 140-2 3단계 인증*
- 물리적 변조 방지
- TRNG(True Random Number Generation)
- 핵심 재료에 대한 스마트 카드 백업

신뢰성

- 고품질 부품

손쉬운 관리

- 직관적인 GUI
- 현장에서 안전하게 업그레이드
- 원격 관리

또한 이 에뮬레이터는 ProtectServer HSM을 설치하지 않고 애플리케이션을 테스트하는 데 있어 유용한 도구로 사용됩니다. 개발자는 준비가 되었을 때 HSM을 설치하고 통신을 하드웨어로 리디렉션하기만 하면 되고, 소프트웨어를 변경할 필요가 없습니다.

손쉬운 관리

직관적인 GUI(Graphic User Interface) 의 이해하기 쉬운 탐색및 사용자 상호 작용을 통해 HSM 장치 관리 및 키 관리를 간단하게 수행할 수 있습니다. 키 수정, 추가 및 삭제 같이 긴급하고 시간이 촉박한 관리 작업을 원격으로 안전하게 수행하여 관리 비용과 응답 시간을 줄일 수 있습니다.

ProtectServer 3+ HSM

ProtectServer 3+ HSM은 ProtectServer 3 HSM에서 제공되는 기능 외에도 이중 핫스왑 전원 공급 장치를 통해 HA(High Availability) 데이터 센터를 정전으로부터 보호합니다. 또한, 어플라이언스를 두 개의 개별 전원에 연결하여 소스 중 하나에 문제가 발생해도 계속 작동이 되도록 함으로써 비즈니스 연속성을 보장합니다. 이를 통해 장치의 지속적인 작동을 보장하는 동시에, 고장난 전원 공급 장치를 정비하거나 교체하는 데 필요한 유연성을 제공합니다.

뛰어난 성능 및 확장성

ProtectServer Network HSM은 암호화 명령을 신속하게 처리합니다. 데이터 암호 전용 마이크로 프로세서, 메모리 및 TRNG(True Random Number Generator)를 포함한 특수 암호화 장치를 통해 호스트 시스템의 암호화 처리 업무를 덜어줌으로써 호스트 시스템이 더 많은 요청에 응답할 수 있게 해줍니다.

ProtectServer Network HSM은 초당 최대 3500건의 RSA-1024 서명 작업을 처리하는 등 대칭 및 비대칭 암호화 성능 수준이 광범위하기 때문에 다양한 보안 애플리케이션 처리 요구 사항을 충족할 수 있습니다. 이중 네트워크 인터페이스가 포함되어 있어 선택에 따라 HSM을 동일한 서브넷 또는 다른 서브넷에 통합할 수 있습니다. 또한, 서로 다른 네트워크에서 HSM을 공유하도록 하여 여러 비즈니스 도메인을 보호하거나 단일 네트워크 내에서 리던던시를 제공할 수 있습니다.

뿐만 아니라, 연동이 가능한 HSM 개수나 관리가 가능한 키 개수에 제한이 없기 때문에 손쉽게 높은 수준의 확장성, 안정성 및 리던던시를 달성하고 처리량을 늘릴 수 있습니다.

편리성

스마트 카드는 암호화 키를 안전하게 백업, 복구 및 전송할 수 있도록 최고 수준의 보안 및 관리 편의성을 제공합니다. 현장에서 비용 효율적으로 업그레이드를 수행할 수 있기 때문에 서비스 센터로의 반품 비용을 줄일 수 있습니다. 또한 ProtectServer HSM은 호환되는 PIN 패드를 통해 주요 구성 요소 입력을 지원합니다.

MFA(Multi-Factor Authentication)

ProtectServer HSM은 MFA를 지원합니다. 이 인증 체계는 기억하고 있는 토큰 PIN과 110 OTP 토큰에서 무작위로 생성되는 6자리 숫자를 모두 요구하는 방식으로 보안을 한 단계 강화합니다.

기술 사양

제공 모델:

- PSE 3는 PL25, PL220 및 PL3500 성능 모델로 제공
- PSE 3+는 PL3500 성능 모델로 제공

운영 체제

- Windows, Linux

암호화 API

- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL

암호화 방식

- 비대칭: RSA, DSA, Diffie-Hellman, 명명, 사전 정의 및 Brainpool 곡선을 이용한 타원 곡선 암호화(ECDSA, ECDH, Ed25519) 등
- 대칭: AES, AES-GCM, AES-CCM, AES-GMAC, Triple DES, DES, CAST 128, RC2, RC4, SEED, ARIA 등
- 해싱: SHA-1, SHA-2, SHA-3, MD5, MD2, RIPEMD 128, RIPEMD 160, DES MDC2 PAD1 등
- 메시지 인증 코드: SHA-1, SHA-2, SHA-3, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC, CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC, ARIA MAC, VISA CVV
- 디지털 지갑 암호화: BIP32
- 가입자 인증을 위한 5G 암호화 메커니즘: MILENAGE 및 TUAK
- 상호 운영성을 위한 ANSI X9 TR-31 키 블록 지원

물리적 특성

- 랙 마운트형
  - 표준 1U 19" 랙 마운트 어플라이언스
- 치수
  - 437mm x 270mm x 44mm (17.20” x 9.84” x 1.73”) (PSE 3)
  - 482.6mm x 533.4mm x 43.815mm (19” x 21” x 1.725”) (PSE 3+)
- 무게
  - 3.1kg(6.83파운드) (PSE 3)
  - 12.7kg(28파운드) (PSE 3+)
- 입력 전압
  - 100-240V, 50-60Hz (PSE 3)
  - 100-240V, 50-60Hz (PSE 3+)
- 전력 소비량
  - 최대 90W, 일반 58W (PSE 3)
  - 최대 100W, 일반 84W (PSE 3+)
- 온도
  - 작동 시 0° ~ 35°C, 보관 시 -20 ~ 60°C
- 상대 습도
  - 5 ~ 85% (38°C) 비응축 (PSE 3)
  - 5 ~ 95% (38°C) 비응축(PSE 3+)

호스트 인터페이스

- 포트 본딩이 지원되는 2개의 기가비트 이더넷 포트 (PSE 3)
- 포트 본딩이 지원되는 4개의 기가비트 이더넷 포트 (PSE 3+)
- IPv4 및 IPv6

보안 인증

- FIPS 140-2 3단계*

관리 및 모니터링

- HA(High Availability) / WLD(Work Load Distribution)
- SNMP, Syslog
- 백업/복원

안전 및 환경 규정 준수

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

안정성:

- 이중 핫스왑 전원 공급 장치 (PSE 3+)
- MTBF(Mean Time Between Failure) 165637 시간 (PSE 3)
- MTBF(Mean Time Between Failure) 171,308 시간 (PSE 3+)

* 특허 출원 중

탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션

연락처 – 모든 사무실 위치 및 연락처 정보는 cpl.thalesgroup.com/contact-us를 참조하시기 바랍니다.