nShield® 범용 하드웨어 보안 모듈

ENTRUST

SECURING A WORLD IN MOTION

목차

믿을 수 있는 보안

Entrust의 nShield 하드웨어 보안 모듈(HSM)은 기업의 가장 민감한 데이터를 보호하는 견고한 변조 방지 장치입니다. 이러한 FIPS 140-2 인증 모듈은 암호화 및 서명 키 생성, 관리, 저장 등의 암호화 기능을 수행하며, 보호되는 경계 내에서 민감한 기능 또한 실행합니다.

보안 스택에 강력한 추가 기능을 제공해드리는 nShield HSM은 다음과 같은 이점을 제공합니다.

- 더 높은 수준의 데이터 보안 및 신뢰 달성
- 중요 규제 표준 충족 및 초과
- 높은 수준의 서비스 및 비즈니스 민첩성 유지

nShield 제품군

nShield 범용 HSM 제품군은 특정 환경에 맞출 수 있도록 다음과 같은 모델을 포함합니다.

nShield Connect

네트워크 연결 어플라이언스

nShield Connect HSM은 네트워크를 통해 애플리케이션에 암호화 서비스를 제공합니다. nShield Connect HSM은 클래식 nShield Connect+ HSM과 고성능 nShield Connect XC HSM 시리즈, 두 가지 시리즈로 제공됩니다.

nShield Edge

휴대용 USB 기반 모듈

nShield Edge HSM은 편리성과 경제성을 위한 데스크톱 장치입니다. nShield Edge는 개발자에게 이상적이며 저용량 루트 키 생성과 같은 애플리케이션을 지원합니다.

nShield Solo

어플라이언스나 서버 내장을 위한 PCIe 카드

nShield Solo HSM은 로우 프로파일 PCI-익스프레스 카드 모듈로 서버 또는 플라이언스에서 호스팅되는 애플리케이션에 암호화 서비스를 제공합니다. nShield Solo HSM은 클래식 nShield Solo+ HSM, 고성능 nShield Solo XC HSM 시리즈, 두 가지 시리즈로 제공됩니다.

nShield as a Service (원문 그대로 사용)

클라우드에서 nShield HSM에 접근하기 위한 구독 기반 솔루션

nShield as a Service는 구독 모델을 통해 전용 FIPS 140-2 레벨 3 인증 nShield Connect XC HSM에 접근할 수 있게 해줍니다. 이 솔루션은 온프레미스 HSM의 기능을 제공할 뿐만 아니라 거기에 클라우드 서비스 배포의 혜택까지 더해 제공합니다. 이를 통해 고객은 클라우드 1차 목표를 달성하고 이러한 어플라이언스의 유지보수를 Entrust의 전문가에게 맡길 수 있습니다. 자체 관리 및 전체 관리 서비스 옵션으로 사용 가능합니다.

다양한 용도 지원

Entrust 고객은 공개 키 인프라(PKI), SSL/TLS 암호화 키 보호, 코드 서명, 디지털 서명 및 블록체인을 비롯한 다양한 비즈니스 애플리케이션에서 nShield HSM을 신뢰의 근원으로 삼고 있습니다. 사물인터넷의 성장으로 기기 (Device에 대한 용어 통일) ID와 인증서에 대한 수요가 증가함에 따라, nShield HSM은 디지털 인증서를 이용한 기기 인증과 같은 중요한 보안 조치를 지속적으로 지원할 것입니다.

또한 nShield HSM은 오늘날의 컴팩트 컴퓨팅 환경에 이상적인 고속 트랜잭션을 제공하는 타원 곡선 암호화 알고리즘을 비롯하여 업계에서 가장 널리 사용되는 운영 체제 및 API 등의 광범위한 암호화 알고리즘을 지원합니다

nShield 제품군의 기능

클라우드 친화적 웹 서비스 인터페이스

옵션으로 제공되는 nShield 웹 서비스 옵션 팩은 웹 서비스 호출을 통해 명령을 실행하여 애플리케이션과 HSM 간의 인터페이스를간소화합니다. 이러한 혁신적인 접근 방식은 애플리케이션을 nShield에 직접 통합할 필요를 제거하여 배포를 단순화하고 OS 및 아키텍처 설계 선택에 대한 의존성 또한 제거합니다. 클라우드 친화적인 솔루션인 웹 서비스 옵션 팩은 기존 데이터 센터뿐 아니라 클라우드에서 호스팅되는 애플리케이션과 연결됩니다.

물리 서버 또는 클라우드 대상 컨테이너형 지원

nShield 컨테이너 옵션 팩은 Entrust의 고신뢰성 하드웨어 보안 모듈에서 지원하는 컨테이너형 애플리케이션 또는 프로세스의 원활한 개발 및 배포를 가능하게 합니다. 이 옵션은 고객의 애플리케이션과 컨테이너형 호스트의 동적 확장 필요를 지원하는 동시에 컨테이너 애플리케이션 환경에 대한 nShield HSM의 통합을 크게 단순화하는 프리패지키 스크립트 세트를 제공합니다.

nShield BYOK로 더 강력해진 클라우드 데이터 관련 키 관리

nShield BYOK(Bring Your Own Key)를 사용하면 온프레미스 nShield HSM에서 강력한 키를 생성하고 아마존 웹 서비스, 구글 클라우드플랫폼, 마이크로소프트 애저 등의 클라우드 애플리케이션으로 안전하게 내보낼 수 있습니다. nShield BYOK를 사용하면 키 관리 관점의 보안을 강화하고, 키를 보다 효과적으로 제어할 수 있으며, 라우드에서 데이터를 안전하게 유지해야 하는 책임도 분담할 수 있습니다.

nShield BYOK는 다음과 같은 이점을 제공합니다.

- 클라우드상 중요 데이터의 보안을 강화하는 더욱 안전한 키 관리 시행
- FIPS 인증 하드웨어로 보호하는 nShield의 고엔트로피 난수 발생기를 이용하여 더욱 강력한 키 생성
- 키 통제력 강화: 내 환경에서 내 nShield HSM을 이용해 키를 생성하고 안전하게 클라우드로 내보내는 기능

암호화 키의 전송 및 사용에 대한 최고의 신뢰성과 엄격한 제어를 위해서 마이크로소프트 애저와 함께 nShield BYOK를 사용하십시오. 통합 및 배포에 관련하여 현장 지원이 필요한 경우, BYOK 배포 서비스 패키지를 선택해 주십시오. nShield Edge를 포함하는 패키지로, Entrust 전문 서비스팀이 통합 서비스를 제공하며 유지보수 기간 1년을 포함합니다.

아마존 웹 서비스 및 구글 클라우드 플랫폼 내 BYOK는 Entrust의 클라우드 통합 옵션 팩(CIOP)을 선택하십시오. 물리 서버 nShield HSM을 이용해 키를 생성하고 아마존 웹 서비스나 구글 클라우드 플랫폼으로 키를 임대하는 데 필요한 모든 것을 포함하는 옵션팩입니다. 또한, CIOP는 새로운 오픈 플랫폼 마이크로소프트 애저 BYOK 메커니즘을 지원합니다.

원격 모니터링 및 관리를 통해 간소화된 운영

nShield Solo 및 Connect HSM에 사용할 수 있는 nShield 모니터와 nShield 원격 관리는 HSM 리소스에 관련하여 연중무휴 24x7 최신 정보를 받아보고 관리함과 동시에 운영 비용을 절감할 수 있게 해줍니다.

- Entrust의 원격 모니터링 및 관리는 다음과 같은 에점을 제공합니다.
- nShield 모니터로 HSM 성능, 인프라 계획 및 업타임을 최적화하여 직원들에게 부하 추세, 사용 통계, 변조 이벤트, 주의 및 경고을 알립니다
- nShield 원격 관리의 강력하고 안전한 인터페이스를 통해 HSM을 관리하여 출장 비용을 절감하고 시간 소모를 줄입니다

원격 구성

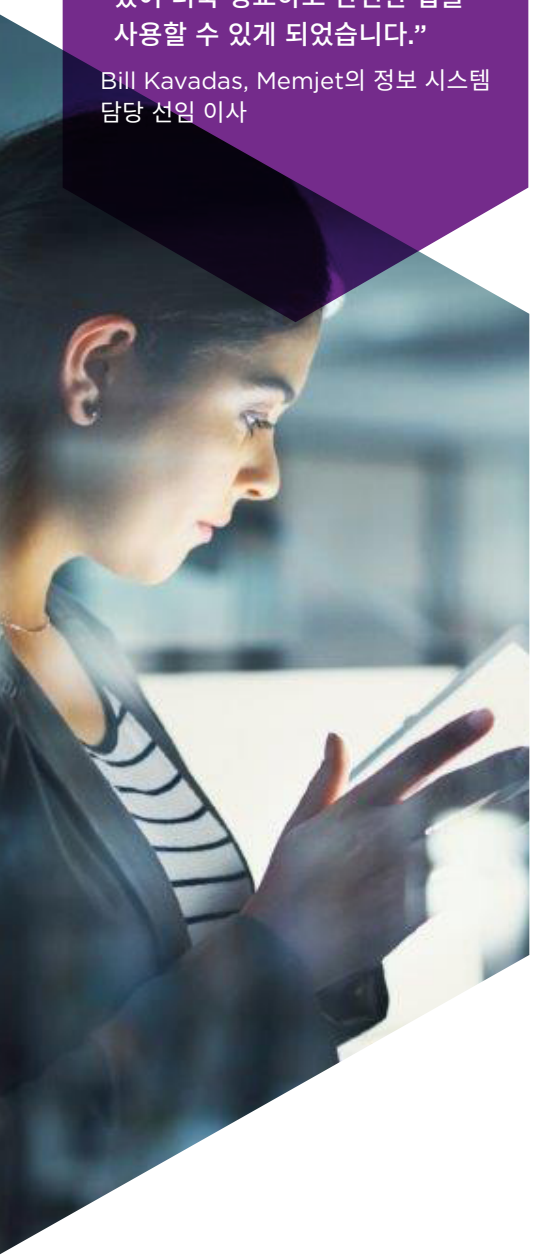
nShield Connect XC 모델은 랙 장착, 케이블 연결 및 전원 공급에 대한 HSM의 물리적 설치를 단순화하는 시리얼 콘솔 옵션을 제공합니다. 그 이후 다른 모든 HSM 및 네트워크 구성은 원격으로 실행될 수 있습니다. 따라서 데이터 센터를 재방문할 필요 없이 배포 및 재배포가 용이해집니다. 이 기능은 제공자가 네트워크 구성을 제어하고 테넌트가 키 자료를 완전히 제어하는 제공자/테넌트 모델을 지원합니다.

시큐리티 월드의 고도로 유연한 아키텍처

nShield 시큐리티 월드는 고유하며 유연한 키 관리 환경을 생성함으로써 Entrust nShield HSM을 지원합니다. nShield 시큐리티 월드를 사용하면 다양한 nShield HSM 모델을 결합하면 확장성, 매끄러운 장애 조치 그리고 부하 분산을 제공하는 통합 생태계를 구축할 수 있습니다.

“Entrust nShield HSM은 최첨단 기술로서 당사의 기술에 있어 더욱 정교하고 안전한 칩을 사용할 수 있게 되었습니다.”

Bill Kavadas, Memjet의 정보 시스템 담당 선임 이사



nShield 시큐리티 월드는 HSM을 1개를 배포하든 수백 개를 배포하든 상관없이 상호 운용성을 제공하고, 무제한의 키를 관리하며 자동 및 원격으로 키 자료를 백업 및 복원할 수 있게 해줍니다.

nShield 시큐리티 월드는 다음과 같은 이점을 제공합니다.

- 요구사항 증가에 따라 nShield HSM 리소스를 쉽게 확장할 수 있도록 지원
- 시스템 복원기능 유지
- 시간이 많이 소요되는 방식의 방식의 HSM 백업 을 제거하여 시간 절약

CodeSafe - nShield의 안전한 실행 환경

nShield Solo 및 Connect HSM은 민감한 키를 보호할 뿐만 아니라 독점적 애플리케이션을 실행할 수 있는 안전한 환경도 제공합니다. CodeSafe 옵션을 사용하면 nShield의 FIPS 140-2 레벨 3 경계 내에서 코드를 개발하고 실행할 수 있어 잠재적인 공격으로부터 애플리케이션을 보호할 수 있습니다.

CodeSafe는 다음과 같은 도움을 제공합니다.

- 중요한 애플리케이션을 실행하고 인증된 환경 내에서 애플리케이션 데이터 엔드포인트를 보호하여 높은 신뢰성 달성
- 내부자 공격, 악성 프로그램 및 지속적인 지능적 위협과 같은 위험으로부터 보안에 민감한 애플리케이션 보호
- 코드 서명을 사용한 무단 애플리케이션 변경 또는 멀웨어 감염의 위험 제거

업계 선두주자와의 파트너십

Entrust는 선도적인 기술 제공업체와 협력하여 광범위한 산업 보안 문제를 해결하고 고객이 디지털 전환 목표를 달성할 수 있도록 지원하는 향상된 솔루션을 제공합니다. Entrust 기술 파트너 프로그램을 통해 Entrust는 파트너들과 협력하여 nShield HSM을 인증 및 PKI, 데이터베이스 보안, 코드 서명, 디지털 서명, 특권 계정 관리, 애플리케이션 제공, 클라우드 및 빅데이터 인텔리전스를 포함한 다양한 보안 솔루션으로 통합합니다. nShield HSM은 정부 및 업계 데이터 보안 규정 준수를 촉진함과 동시에 가장 강력한 암호화 처리, 키 보호 및 키 관리 기능을 제공하기 위해 파트너의 보안 애플리케이션을 지원합니다.

"우리는 nShield as a Service를 포함한 nShield의 새로운 클라우드 친화적 기능을 고객에게 제공할 수 있는 가능성에 대해 기쁘게 생각합니다. 이러한 신기능은 시장 변화를 인식하고 혁신과 상업적 이익을 실현하기 위해 조직이 클라우드에서 완전한 서비스 HSM의 역량을 필요로 한다는 것을 인식하고 있습니다."

Ed Wood, Cryptomathic의 제품 관리 이사

"Entrust에서 nShield as a Service를 출시함으로써 F5 고객을 위한 보안 선택의 폭을 넓히고 구독 기반 모델에서 데이터 주권을 획득할 수 있는 기능도 제공할 수 있었습니다. 보안을 자본에서 운영 지출로 전환하면 조직의 유연성과 비용 효율성을 높일 수 있습니다."

John Morgan, F5 Networks의 보안 VP겸 GM

다용도 및 고성능

nShield Connect 및 Solo HSM은 트랜잭션 속도가 보통이든 애플리케이션에서 높은 처리량을 요구하든 관계없이 환경에 맞는 3가지 성능 레벨로 제공됩니다. 클라우드에서 nShield HSM에 접근하기 위한 구독 기반 솔루션인 nShield as a Service는 최고 성능의 nShield Connect XC가 뒷받침합니다.

업계 표준 인증

Entrust는 엄격한 표준을 준수함으로써 규제 환경에서 컴플라이언스를 입증함과 동시에 nShield HSM의 보안과 무결성에 대한 높은 신뢰성을 제공합니다. 다음은 당사가 준수하는 표준의 일부 목록입니다. 전체 목록은 당사 웹사이트와 데이터시트에서 확인하실 수 있습니다.

FIPS 140-2

세계적으로 인정받는 FIPS 140-2는 암호 모듈의 보안 강건성을 검증하는 미국 정부의 NIST 표준입니다. 모든 Entrust nShield HSM은 FIPS 140-2 레벨 2 및 레벨 3 인증을 받은 바 있습니다.

공통평가기준 및 eIDAS 규제 준수

nShield XC 및 nShield + HSM은 공통평가기준 EAL 4+ 인증을 받았으며 eIDAS 규정에 따라 QSCD (Qualified Signature Creation Device/원문 그대로 사용)로 인정됩니다. 또한 nShield Solo XC 및 Connect XC HSM은 CC(Common Criteria) 보호 프로파일 EN 419 221-5 "신뢰 서비스를 위한 암호화 모듈"을 준수합니다. 따라서 nShield HSM은 EU 회원국과 기업의 디지털화를 위한 보장 중추
역할을 능히 수행할 수 있습니다. 여기에는 국가 ID 체계와 국경을 초월한 서비스, 전자 문서 및 거래 서명을 위한 서비스, 인증, 타임스탬프, 보안 이메일 및 장기 문서 보존을 위한 서비스 등이 포함됩니다. 이러한 인증은 유럽 규정의 일부로 제정되었지만, 전 세계 많은국가에서도 채택되고 있습니다.

자세한 정보

클라우드와 가상 환경에서 비즈니스에 중요한 정보와 애플리케이션을 보호하는 방법에 대해 알아보시려면 **entrust.com/ko/HSM**을 방문하십시오.

Entrust nShield HSM에 대해 더 알아보시려면

HSMinfo@entrust.com
entrust.com/ko/HSM

ENTRUST CORPORATION 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명도 넘는 동료, 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

더 자세히 알아보기
entrust.com/ko/HSM

ENTRUST

연락처:
HSMinfo@entrust.com