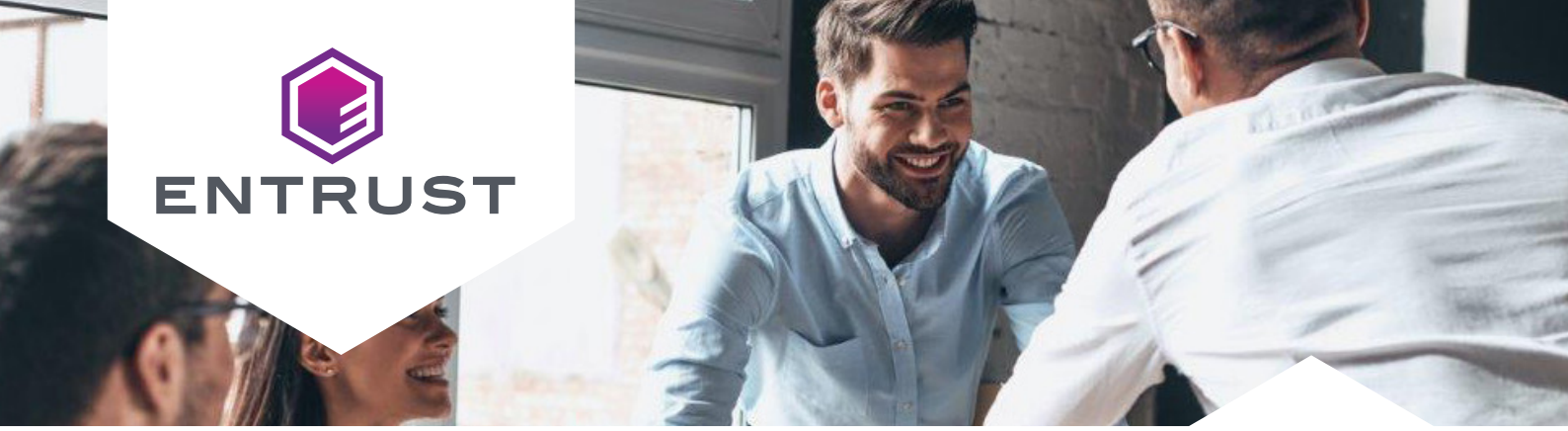


nShield Solo HSM

독립 서버에 암호키 서비스를 제공하는 인증된 PCI Express 카드

하이라이트

nShield Solo 하드웨어 보안 모듈(HSMs)은 FIPS 인증을 보유한 로우 프로파일 PCI Express 카드로 서버 또는 어플라이언스에 호스팅된 애플리케이션에 암호키 서비스를 제공합니다. 이와 같은 변조 방지 카드는 인증 기관, 코드 서명, 사용자 정의 소프트웨어 등 광범위한 애플리케이션에 걸쳐 암호화, 디지털 서명, 키 생성 및 보호와 같은 기능을 수행합니다.

nShield Solo 시리즈는 nShield Solo+ 및 새로운 고성능 nShield Solo XC도 포함합니다.

높은 유연성을 갖춘 아키텍처

고객은 엔트러스트 고유의 시큐리티 월드 아키텍처를 nShield HSM 모델과 결합하여 사용할 수 있습니다. 통합된 모듈은 확장이 용이하고, 자동화된 장애극복, 로드 밸런싱을 지원합니다.

더 많은 데이터를 더욱 신속하게 처리

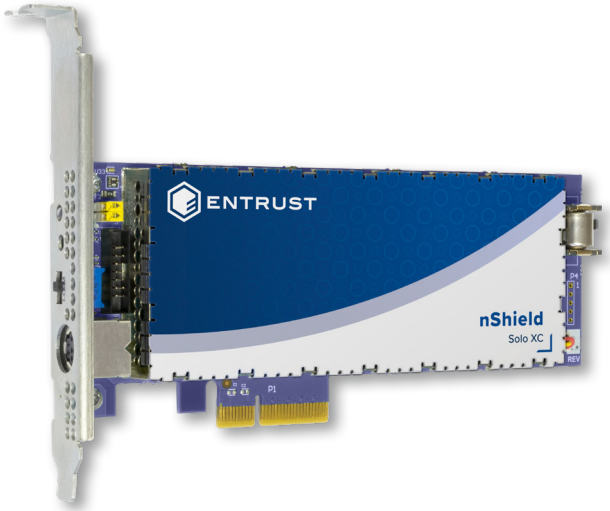
nShield Solo HSMs은 높은 처리 성능을 지원하여 기업이나 소매업 및 사물인터넷과 같은 높은 성능을 필요로 하는 환경에 이상적입니다.

고객 맞춤형 애플리케이션과 데이터 보호

CodeSafe 옵션은 nShield 경계 내에서 민감한 어플리케이션을 실행하기 위한 안전한 환경을 제공합니다.

주요 기능 및 혜택

- 높은 암호화 트랜잭션 속도와 유연한 확장 가능성으로 성능과 가용성을 최대화
- 인증 기관, 코드 서명 등의 다양한 애플리케이션을 지원
- nShield CodeSafe는 nShield의 안전한 실행 환경에서 애플리케이션을 보호.
- nShield 원격 관리는 비용을 절감하고 출장을 줄이도록 지원.



ENTRUST.COM/ko/HSM에서 자세히 보기

nShield Solo HSM

기술 사양

지원하는 암호화 알고리즘

- 비대칭 알고리즘: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- 대칭 알고리즘: AES, Arcfour, ARIA, Camellia, CAST, DES, Triple DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC
- 해시/메시지 다이제스트: MD5, SHA-1, SHA-2 (224, 256, 384, 512 비트), HAS-160, RIPEMD160
- Brainpool 및 커스텀 커브를 포함한 완전한 라이선스 ECC를 갖춘 Full Suite B 구현

지원하는 플랫폼

- RedHat, SUSE 및 가상 머신 또는 컨테이너에서 실행되는 주요 클라우드 서비스 제공업체의 배포를 포함한 윈도우 및 리눅스 운영 체제
- VMware ESX, Microsoft Hyper-V, Linux KVM & Citrix XenServer를 포함한 Solo XC 가상 환경 지원

응용 프로그램 인터페이스(API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI 및 CNG, nCore, 및 웹 서비스(웹 서비스 옵션 팩 필요)

호스트 연결

- PCI Express 버전 2.0; Solo+ 커넥터: 1 레인, Solo XC 커넥터: 4 레인

보안 규제 준수

- FIPS 140-2 레벨 2 및 레벨 3 인증
- Solo+: Common Criteria EAL4+ (AVA_VAN.5) 인증
- Qualified Signature Creation Device 로 인정 받은 Solo+
- Solo XC: eIDAS 및 CC(Common Criteria) EAL4 + AVA_VAN.5 및 네덜란드 NSCIB 제도 하 EN 419 221-5 보호 프로파일 관련 ALC_ FLR.2 인증
- Solo XC: BSI AIS 20/31 준수

안전 및 환경 표준 준수

- UL, UL/CA, CE, FCC, 캐나다 ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

관리 및 모니터링

- nShield 원격 관리자 및 nShield 모니터
- 보안 감사 로깅
- Syslog 진단 지원 및 윈도우 성능 모니터링
- SNMP 모니터링 에이전트

사용 가능한 모델 및 성능

nShield Solo 모델	500+	XC Base	6000+	XC Mid	XC High
NIST 권장 키 길이에 대한 RSA 서명 성능(tps)					
2048 비트	150	430	3,000	3,500	8,600
4096 비트	80	100	500	850	2,025
NIST 권장 키 길이에 대한 ECC 프라임 곡선 서명 성능(tps)					
256 비트	540	680	2,400	7,515[1]	14,400[1]

규격	중량		Power	
	Solo+	Solo XC	Solo+	Solo XC
56.2 Q 167.1 Q 15.4mm	230g	280g	10W	24W
2.2 Q 6.6 Q 0.6in	0.5lb	0.62lb		

주 1: 표시된 성능에는 엔트러스트 기술지원팀에 요청하여 무료로 사용할 수 있는 ECDSA 고속 RNG 기능 활성화가 요구됩니다.

더 자세히 알아보기
entrust.com/ko/HSM

ENTRUST

연락처:
HSMinfo@entrust.com