



ENTRUST

nShield BYOK, 클라우드 고객의 데이터 보안 통제권 확대

클라우드의 편리함과 보안이 만나다

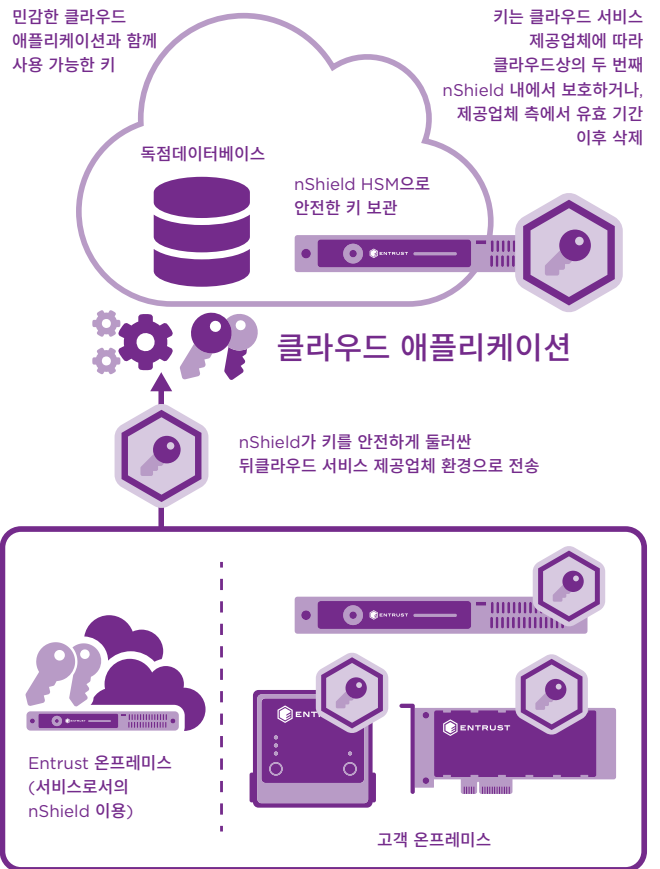


하이라이트

- 클라우드 내 중요 데이터의 보안을 강화하는 더욱 안전한 키 관리 시행
- FIPS 인증 하드웨어로 보호하는 Entrust nShield®의 고엔트로피 난수 발생기를 이용하여 더욱 강력한 키 생성
- 고객의 키 통제권 확대: 고객의 환경에서 고객이 보유한 nShield 하드웨어 보안 모듈(HSM)을 이용해 키를 생성하고 안전하게 클라우드로 내보내는 기능
- 클라우드에서 이용하는 키나, 온프레미스에서 이용하는 키나 상관없이 더욱 일관된 키 관리 작업 가능

nShield HSM을 이용하면, Amazon Web Services(AWS)를 이용하던 Google Cloud Platform(GCP)이나 Microsoft Azure를 이용하던 상관없이 클라우드 애플리케이션에 '자신의 키를 직접 전송(BYOK)'할 수 있습니다.

엄격하게 보증하는 nShield HSM은 클라우드 서비스의 유연성과 경제성을 계속 누리도록 할 뿐만 아니라 실제 키 관리 보안을 강화하며, 보다 효율적으로 키를 관리할 수 있도록 지원합니다.



Entrust만의 고유한 Security World 아키텍처는 안전한 장기 보관 기능과 마스터키의 재해 복구 보호 기능을 제공합니다.

클라우드 고객의 데이터 보안 통제권 확대

nShield BYOK의 기능

nShield BYOK(Bring Your Own Key)를 이용하면 고객이 이용하는 nShield HSM으로 중요 클라우드 호스트 애플리케이션, 데이터베이스, 대용량 기억 장치를 보호하는 데 필요한 키를 생성, 보관 및 관리할 수 있습니다. nShield BYOK는 다음과 같은 기능을 제공합니다.

- 하드웨어 신뢰점을 기반으로 합니다. nShield HSM는 매우 안정적이며, FIPS 140-2 레벨 3 인증을 받은 변조 방지 제품입니다. 이 HSM는 클라우드 서비스에 신뢰점 기능을 지원하여 암호화와 서명 키를 안전하게 생성하고 보호할 수 있도록 지원합니다.
- nShield를 이용해 키를 관리할 수 있습니다. 클라우드 호스트 애플리케이션에 있는 중요 데이터의 경우, nShield HSM으로 키를 생성하고 돌려싼 뒤 안전하게 클라우드 애플리케이션으로 전송합니다.
- 키의 가용성을 통제할 수 있습니다. 온프레미스 환경이든 서비스로서의 nShield 환경이든 상관없이, 고객이 소유한 nShield HSM은 고객이 단독 통제하게 되어있어 언제 키를 생성하고 내보낼지 자유롭게 결정할 수 있습니다. 마스터키를 통제하기 때문에, 클라우드 제공업체로의 키 전송 시점과 여부도 통제할 수 있습니다.
- 클라우드 제공업체를 선택할 수 있습니다. With nShield BYOK를 이용하면, 키마다 이용할 클라우드 제공업체를 결정할 수 있습니다. 이 경우, 온프레미스나 서비스로서의 nShield 환경이나 상관없이 다양한 애플리케이션에 적합한 클라우드를 유연하게 선택할 수 있을 뿐만 아니라, 엄격하게 보증되는 nShield 키 생성 및 보호 혜택을 누리실 수 있습니다.

nShield BYOK 이용 방법

AWS나 GCP, Azure에 nShield BYOK를 이용하려면 nShield HSM가 필요합니다. 다음 솔루션 중에서 선택하실 수 있습니다.

- nShield Connect: 네트워크 연결 제품
- nShield Solo: 서버 내장형 PCI 익스프레스 카드
- nShield Edge: 저용량 애플리케이션용 USB 연결 기기
- 서비스로서의 nShield: 구독제 nShield Connect HSM 사용

Entrust BYOK와 Microsoft Azure를 함께 이용하면 최고의 보장성을 확보할 수 있습니다.

참조: <https://protect-eu.mimecast.com/s/PYBnCWnYocOBORVImMJzG?domain=docs.microsoft.com> 배포 관련 지원이 필요한 경우, 다음 옵션 패키지를 구매하실 수 있습니다.

BYOK, Azure 전문 서비스

nShield Edge를 포함하는 패키지로, Entrust 전문 서비스팀이 통합 서비스를 제공하며 유지보수 기간 1년을 포함합니다.

nShield Connect, Solo, Edge HSM나 전문 서비스는 별도 구매도 가능합니다.

AWS나 GCP, 또는 Microsoft Azure에서 Microsoft 개방형 표준 방법을 사용하여 nShield BYOK를 사용하려면 다음 Entrust 패키지가 필요합니다.

클라우드 통합 옵션팩

온프레미스 nShield HSM을 이용해 키를 생성하고 돌려싼 안전하게 전송하고 AWS나 GCP, Azure BYOK를 이용하는 Microsoft Azure로 키를 임대하는 데 필요한 모든 것을 포함하는 옵션팩입니다.

nShield BYOK를 AWS GCP나 Azure와 직접 통합하거나, Entrust 전문 서비스를 이용해 원활하고 효율적으로 연결하는 서비스를 지원받으실 수 있습니다.



클라우드 고객의 데이터 보안 통제권 확대

nShield BYOK의 작동 원리

Entrust는 사용 중인 nShield HSM로 키를 생성하고, 안전하게 장기간 보관할 수 있으며 클라우드로 키를 내보낼 수 있는 메커니즘을 제공합니다. 온프레미스나 서비스로서의 nShield에서 클라우드로 키를 내보내면 다음 중 한 가지 방식으로 키를 관리할 수 있습니다.

Microsoft Azure를 이용하는 경우

Entrust BYOK를 선택하면 최고의 보장성을 확보하는 동시에 Microsoft Azure를 사용할 수 있습니다. 이는 키를 Azure에 업로드할 때 충족해야 하는 조건을 제어하고 MSFT가 해당 키로 수행할 수 있는 작업을 엄격하게 제한합니다.

Azure 인프라 내에서 실행되는 nShield HSM으로 키를 안전하게 전송하기 때문에 양 위치에서 HSM 보안을 확보할 수 있습니다.

AWS나 GCP를 이용하는 경우

클라우드에서 키를 일시적으로 사용할 수 있도록 AWS나 GCP에 키를 대여합니다. 클라우드 상의 키는 미리 정해진 기간이 경과하면 파기됩니다. 필요한 경우, HSM상에 보관한 키를 다시 대여해줄 수 있습니다.

어떤 퍼블릭 클라우드 서비스를 선택하든지 상관없이 자체 키를 생성하고 내보내는 절차를 통제하면, 클라우드상의 중요 데이터와 애플리케이션에 강력한 보안을 구축할 수 있습니다.

Entrust HSM

Entrust nShield HSM은 현재 이용 가능한 솔루션 중에서도 최고 성능을 갖추었으며 가장 안전하고 통합하기 쉬운 HSM 솔루션 중 하나로, 규정 준수를 촉진하고 기업, 금융 기관과 정부 기관에 최고 수준의 데이터 보안과 애플리케이션 보안을 제공합니다. Entrust만의 Security World 키 관리 아키텍처를 이용하면 강력하고 세분화된 방식으로 키 액세스와 사용을 통제할 수 있습니다.

관련 링크

entrust.com/HSM을 방문하면 Entrust nShield HSM에 관해 자세히 알아보실 수 있습니다.

entrust.com을 방문하면 Entrust의 신원, 접근, 통신, 데이터 관련 디지털 보안 솔루션에 관해 자세히 알아보실 수 있습니다.

Entrust nShield HSM 관련
정보 확인 및 문의

HSMinfo@entrust.com
entrust.com/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.

에서 자세히 보기:

entrust.com/HSM

