HYOK(Hold Your Own Key)로 엄격히 보증하는 키 관리

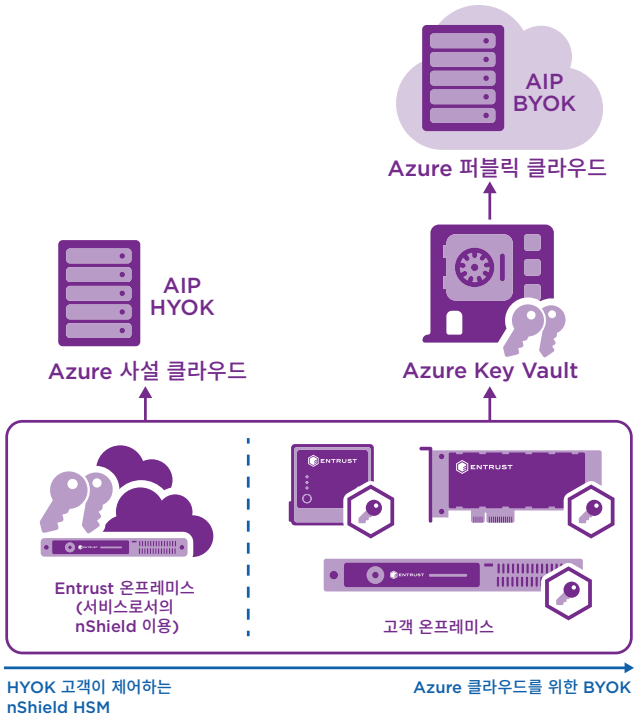
Microsoft와 Entrust, 클라우드상에서의 주도권을 확보할 수 있는 지속적인 정보 보호 및 키 관리 옵션 제공

하이라이트

- 교환 데이터의 액세스 및이용 제어
- 고객이 자체적으로 제어하는 HSM로 키 보유와 보안 가능
- FIPS 140-2 인증 수명 주기 키 관리 제공
- Microsoft에 키 노출 방지

Microsoft Azure Information Protection(AIP, 애저 정보 보호)은 데이터 유형에 관계없이 데이터 자산에 강제할 수 있는 보안 정책을 포함하여, 공동 작업 환경 내에서 교환하는 데이터를 보호합니다. 클라우드 서비스로 IT 인프라 없이 주문형 AIP를 실행할 수 있으며, 기업 외부로 벗어나는 정보에도 보호를 제공합니다.

AIP는 암호화를 이용해 데이터 액세스를 통제하고 지속적인 보안을 제공합니다. AIP 보안은 핵심 암호키에 제공되는 보호 수준에 따라 달라집니다. 암호키 노출은 중요 데이터 침해로 이어집니다.



AIP 이용 환경이 온프레미스나 하이브리드 구성 환경, 완전한 클라우드 환경이든지 상관없이 Entrust nShield® HSM이 중요 키를 통제하는 데 필수적인 주도권을 드립니다.

HYOK(Hold Your Own Key)로 엄격히 보증하는 키 관리

과제: 매우 중요한 데이터는 온프레미스상 암호키 보관 필요

콘텐츠 대부분은 Azure 상에 안전하게 보관된 키를 이용해도 괜찮지만, 자체 보안 범위 밖으로 공유하거나 전송해서는 절대 안 될 민감한 콘텐츠도 있습니다. 이런 민감한 콘텐츠의 보안은 온프레미스 내에서 구현되어야만 하며, 액세스와 공유는 엄격히 제한되어야 합니다.

자체 보안 경계 내에서 가장 중요한 데이터를 관리할 수 있도록 AIP는 Hold Your Own Key(HYOK) 옵션을
제공하는데, 이는 온프레미스 컴포넌트로 이용 가능하며 Entrust 하드웨어 보안 모듈(HSM)로 제공되는 키 관리를 포함합니다. Entrust HSM는 고객 온프레미스나 서비스로서의 nShield 환경에 배포할 수 있습니다.

Entrust nShield® HSM는 중요한 키를 보호하고 중요 데이터의 보안을 강화하는 철통같은 보안 환경을 제공합니다.

솔루션: Entrust가 제공하는 강화된 키 제어 솔루션으로 HYOK 배포

Entrust nShield HSM은 AIP 배포에 사용되는 암호키의 관리 및 사용을 엄격하게 제어합니다.

Entrust nShield HSM은 중요한 키를 보호하는 하드웨어 솔루션을 제공합니다. nShield HSM 은 소프트웨어 환경에서 완전히 독립적으로 키를 보호하고 관리하여, 키를 자체적으로 보유하고 완벽히 통제하는 주도권을 확보할 수 있습니다.

키 생성과 관리가 자체 nShield HSM 보안 범위 내에서 이루어지므로, 중요한 데이터를 주도적으로 보호할 수 있습니다.

Entrust HSM를 AIP와 HYOK와 함께 이용해야 하는 이유

Entrust HSM은 물리 서버나 클라우드, 하이브리드 구성 환경이든 상관없이 개별 데이터 보안 요건에 맞춰 AIP를 자유롭게 이용할 수 있는 유연성을 제공합니다. nShield HSM이 제공하는 기능은 다음과 같습니다.

- FIPS 140-2 인증 암호 범위 내에서 키 보안
- 역할 분리 수행과 강력한 액세스 제어 메커니즘을 이용하여, 승인된 목적으로만 키 이용 가능
- 키 관리, 보관, 중복 기능을 이용해 키 가용성 보장

Azure Key Vault를 이용해 키를 저장하고 AIP에 이용하고자 하는 경우, Entrust 키 보안 강화 또한 지원 가능합니다. 직접 관리하는 nShield HSM를 이용해 키를 생성하고 Azure Key Vault로 안전하게 전송합니다. BYOK 기능으로 클라우드상의 키와 데이터 보안에 대한 주도권을 확보할 수 있습니다.

HYOK(Hold Your Own Key)로 엄격히 보증하는 키 관리

Entrust nShield HSM 기능:

- 강력한 변조 방지 환경에서 키 보안
- 행정 업무에서 보안 기능을 분리하여 보안 정책 집행 가능
- 공공 부문, 금융 서비스, 기업 관련 규제 요건 준수
- FIPS 140-2 레벨 및 CC 인증

Entrust nShield HSM을 구체적인 요구 성능과 예산 상황에 맞춰 이용하실 수 있습니다:

- 대용량 키 생성 및 관리가 필요한 경우 (또는 하이브리드 배포 작업의 일환인 경우), nShield Solo HSM 내장형 embedded PCI 익스프레스 카드 및 nShield Connect HSM 네트워크 연결 제품이 고성능 하드웨어 보안 제공
- 고객 온프레미스나 서비스로서의 nShield 환경에 nShield Connect HSM 배포 가능
- BYOK 기능의 일부인 저용량 온프레미스 키 생성이 필요한 경우, nShield Edge HSM이 편리한 USB 연결 하드웨어 보안 제공

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.

Microsoft

마이크로소프트는 기업들이 콘텐츠를 생성하고 공유하며 공동 프로세스를 구축하는 방식을 혁신했습니다. Microsoft 솔루션에 기반한 시스템은 생산성을 극대화합니다. 데이터를 보호하기 위해 Microsoft AIP는 암호화를 차용하여 신뢰할 수 있는 비즈니스 환경을 구축하며 이 환경은 다음과 같은 기능을 제공합니다.

- 기업 간 신원 관리
- 인증용 인증서 배포
- 데이터 자원에 대한 사용자 액세스 권한 통제
- 종합 정보 보호 제공

www.microsoft.com

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

ENTRUST

연락처:
HSMinfo@entrust.com