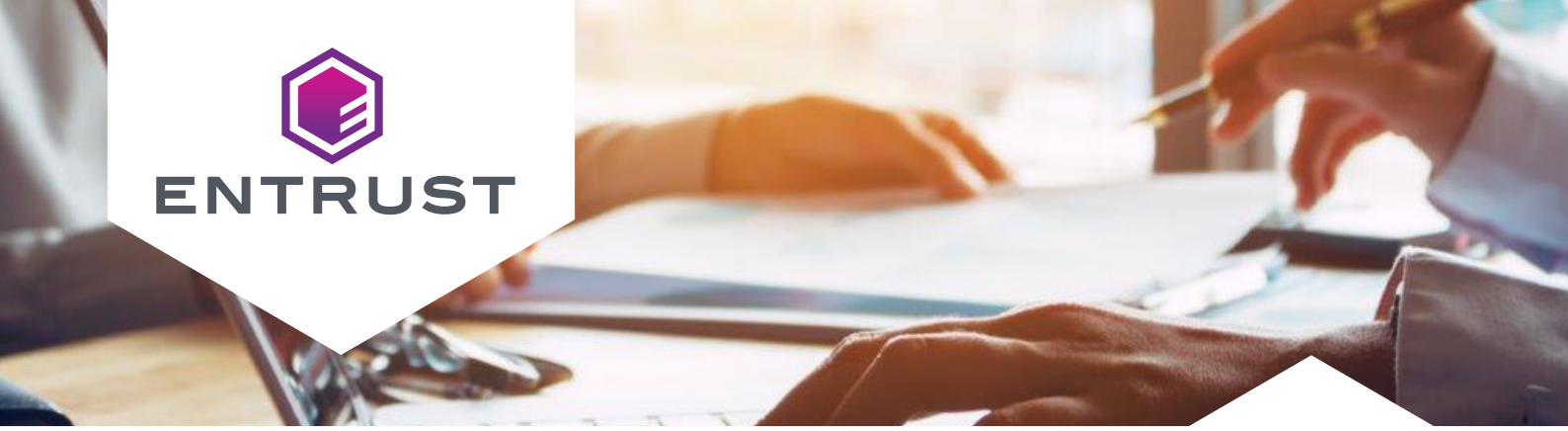

블록체인 보안

블록체인을 위한 고보장성 보안

하이라이트

- 하드웨어 보안 모듈(HSM) 신뢰점 내에서 민감한 코드 처리
- 다양한 ECC(타원 곡선 암호화) 알고리즘으로 애플리케이션 증가에 대응
- 클러스터형 HSM 배포로 암호화 기능 확장
- Entrust 전문 서비스로 신속한 구현 가능

블록체인: 기회와 난관

블록체인과 분산 원장 기술은 기존 기업과 신규 기업 모두에게 중요한 새로운 기회를 의미합니다. 블록체인 구현은 특정 비즈니스 사용 사례에 근본적인 변화를 일으켜 운영을 단순화하고 비용을 절감하며 트랜잭션을 간소화할 수 있습니다.

광범위한 블록체인 도입을 가로막는 주요 난관 중 하나는 보안입니다. 어음 교환이나 결제, 지불, 의료, 무역, 금융, 정부 지침 준수와 같은 사용 사례에는 보장 수준이 높은 보안이 필요합니다.

블록체인을 활용하는 새롭고 혁신적인 사용 사례가 계속해서 발굴되는 상황을 고려했을 때, 기업들은 처음부터 보안을 계획해야 합니다. 블록체인에 전송하는 트랜잭션마다 디지털 서명을 보장할 수 있어야만 이 혁신적인 기술의 사용을 발전시키고 이점을 누릴 수 있습니다. 따라서 블록체인 절차에 사용하는 서명 키를 보호하고 합의 로직(consensus logic)을 변조로부터 보호하는 것이 필수적입니다.

Entrust 전문 서비스가 지원하는 구현 서비스

블록체인 보안

키 보호로 시스템 보호

모든 암호화 기반 인프라와 마찬가지로 블록체인 시스템의 보안을 보장하려면 시스템의 기초인 키를 보호하는 것이 가장 중요합니다. HSM이 제공하는 강력한 키 보호 관행과 분산 원장 모델의 요구에 맞춰 확장할 수 있는 성능이 바로 블록체인 시스템의 성공을 좌우하는 요소입니다.

Entrust의 접근 방식

Entrust는 블록체인 구현과 관련된 근본적인 보안 문제인 서명 키와 합의 로직 보안 문제에 대응합니다. nShield® HSM을 통해 기업은 다음과 같은 기능을 이용할 수 있습니다.

- secp256k1, Edwards Curve(Ed25519) 등과 같은 ECC 알고리즘을 사용하여, 자신 있게 트랜잭션 서명 가능
- FIPS 인증, 변조 방지 하드웨어 범위 내에서 서명 키 보호
- nShield HSM의 고유한 CodeSafe 기능으로 서명 절차 이면의 비즈니스 로직 보호

블록체인에 전송하는 트랜잭션을 개인 키로 디지털 서명하여, 의도된 사용자로부터 전송받은 것임을 확인하고 변경 방지 가능 Entrust nShield HSM은 개인 키의 발급과 취소에 사용되는 기본 루트 키를 보호합니다.

nShield HSM의 고유한 CodeSafe 기능은 합의 논리 코드를 실행할 수 있는 안전한 환경을 제공하여, 규정을 준수하는 승인받은 트랜잭션만이 블록체인에 추가되도록 허용합니다. nShield HSM의 보안 범위 내에 있기 때문에 CodeSafe는 가장 민감한 코드에도 FIPS 140-2 레벨 3 인증 보호를 제공합니다.

또한 Entrust의 전문 서비스팀은 수십 년간 축적한 경험을 바탕으로 nShield HSM의 안전한 기반 위에 안전하고 효과적인 블록체인 애플리케이션을 구현하도록 지원해드립니다.

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.com**을 방문하면 Entrust의 신원, 접근, 통신, 데이터 관련 디지털 보안 솔루션에 관해 자세히 알아보실 수 있습니다.

에서 자세히 보기:
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com