솔루션 개요

THALES

CYBERSECURITY

Thales Luna HSMs으로 디지털 자산 보호하기

증가하는 위협과 변화하는 규제 환경에 대응하는 하드웨어 기반 디지털 신뢰의 기반

cpl.thalesgroup.com

THALES

CYBERSECURITY

디지털 자산이란 무엇일까요?

디지털자산은 암호화폐, 스테이블코인, 증권·예금·실물 자산 등의 토큰화 자산을 포함하여 디지털 형태로 표현되고 거래되는 모든 형태의 가치를 의미합니다. 이러한 자산은 블록체인과 같은 분산 플랫폼에서 생성·관리·교환되며, 탈중앙화, 프로그래머블 머니, 디지털 소유권을 기반으로 한 현대 디지털 금융의 기초를 형성합니다.

서론 : 급속한 디지털 자산 채택과 증가하는 금융 리스크

디지털 자산은 글로벌 금융의 중요한 축으로 자리잡았습니다. 스테이블코인의 거래 금액은 이미 Visa와 Mastercard의 합산 거래량을 초과하며, 국제 블록체인 결제 규모는 연간 6조 달러를 넘어섰습니다(Delphi Digital, 2025). 분산 원장 플랫폼 기반의 실물·금융 자산 토큰화 역시 자본시장, 결제, 크로스보더 정산 분야에서 기관 중심의 파일럿이 확대되며 빠르게 성장하고 있습니다(국제결제은행, 2024). 이에 따라 은행, 결제, 자본시장 등 금융기관들은 고객 수요에 부응하고 빠르게 변화하는 시장에서 경쟁력을 유지하기 위해 디지털 자산 전략을 가속화하고 있습니다.

이러한 성장은 강력한 보안 기반의 중요성을 더욱 부각시키고 있습니다. 2025년 암호자산 관련 해킹 피해는 약 34억 달러에 달했으며, 기관들이 디지털 자산 운영을 확장함에 따라 강력한 키 관리와 보안 통제가 필요하다는 사실이 재확인되고 있습니다. 성숙한 보안 프로그램을 갖춘 중앙화 플랫폼에서도 개인 키는 여전히 중요한 취약 지점으로 남아 있습니다. 2025년 1분기에는 수탁형 거래소 및 자산 플랫폼 등 중앙화 서비스가 전체 피해 자산의 88%를 차지하며, 하드웨어 수준에서 개인 키 운영을 보호하는 것이 얼마나 중요한지를 다시 한번 입증했습니다(Chainalysis, 2025).

디지털 자산 채택이 가치와 복잡성 면에서 계속 확대됨에 따라, 금융기관은 핵심에서 개인 키를 보호하도록 설계된 보안 아키텍처를 필요로 합니다. 검증된 하드웨어 보안 모듈(HSM)은 이 기반을 제공하며, 키를 보호하고 그 주변에 구축된 디지털 자산 워크플로우를 지원하는 신뢰할 수 있는 하드웨어 기반 루트 오브 트러스트(Root of Trust)를 제공합니다.

과제: 보안 격차와 확대되는 글로벌 규제

디지털 자산 이니셔티브가 가속화되는 가운데, 많은 기관들은 대규모로 안전하게 운영하기 위해 필요한 통제를 구현하는 데 여전히 어려움을 겪고 있습니다. 개인 키는 무단 접근을 차단하면서도 대량 서명, 다자 승인 워크플로우, 직무 분리를 지원하는 방식으로 생성·저장·사용되어야 합니다. 소프트웨어 기반의 키 저장 방식은 공격자들이 사기 및 도난의 주요 경로로 개인 키 탈취를 집중적으로 노리는 상황에서 점점 더 한계를 드러내고 있습니다.

동시에 주요 금융 중심지 전반에서 규제 요건이 더욱 엄격해지고 통일성을 갖춰가고 있습니다. 홍콩 SFC의 가상자산 거래 플랫폼 가이드라인, 싱가포르 MAS 고지, EU의 MiCA, 독일 BaFin 가이드라인, 스위스 FINMA 요건은 모두 수탁 통제, 키 관리, 운영 회복 탄력성, 감사 가능성에 관한 명확한 기대치를 제시하고 있습니다. 기관들은 자신들의 디지털 자산 인프라가 이제 모든 배포 모델에 걸쳐 일관된 정책 집행, 검증 가능한 키 보호, 투명한 거버넌스를 제공할 수 있다는 것을 입증해야 합니다.

이러한 요구사항을 충족하려면 개인 키를 보호하고, 거래 서명을 통제하며, 혁신을 늦추지 않으면서 규정 준수를 지원하는 신뢰할 수 있는 보안 기반이 필요합니다. 인증된 HSM은 변조 방지 하드웨어 내에서 중요한 운영을 보호하고 규제 기관과 기관 리스크 팀이 기대하는 보증을 제공함으로써 이 기반을 제공합니다.

해결방안: Luna HSM이 뒷받침하는 기관급 디지털 자산 보안

Thales Luna HSM은 인증된 변조 방지 하드웨어 내에서 개인 키와 서명 운영을 보호하는 하드웨어 루트 오브 트러스트를 제공함으로써 디지털 자산을 보호하며 온프레미스 또는 서비스 형태로 제공되어 현대 디지털 자산 플랫폼에 적합합니다. 검증된 안전한 키 생성 기능을 제공하며, 고객 소유의 FIPS 인증된 하드웨어 내에서 서명 애플리케이션에 사용되는 개인 키를 보호하여 대부분의 공격이 발생하는 애플리케이션 레이어, 온라인 시스템, 클라우드 환경으로부터 키가 완전히 격리됩니다.

변조 방지 하드웨어에서 키 생성·저장·서명을 수행함으로써 Luna HSM은 다양한 디지털 자산 수탁 모델을 강화합니다. 초기 디지털 자산 플랫폼 대부분이 소프트웨어 전용의 단순성을 우선시했던 반면, 이제 기관 고객과 규제 기관은 인증된 HSM에 의해 개인 키가 보호되기를 점점 더 기대하고 있습니다. 표준 API 뒤에서 온프레미스 또는 서비스로 배포된 하드웨어 기반 보안은 제약 없이 진화하는 커스터디 아키텍처를 지원합니다.

Luna HSM은 선도적인 커스터디 플랫폼, 블록체인 인프라, 지갑 기술, 토큰화 엔진과 통합됩니다. 고객은 일관된 보안·거버넌스·운영 통제를 유지하면서 온프레미스, 클라우드, 서비스 형태 또는 Thales Data Protection on Demand(DPoD) 클라우드 마켓플레이스를 통해 Luna HSM을 배포할 수 있습니다. 배포 모델 선택의 유연성과 암호화 민첩성(Crypto-Agile) 및 양자 내성 보안이 결합되어, 기관들은 신뢰성·성능·규제 정합성을 강화하면서 디지털 자산 역량을 확장할 수 있는 견고한 기반을 갖추게 됩니다.

Luna HSM 디지털 자산 배포 모델

클라우드, 온프레미스 또는 하이브리드 환경에서의 디지털 자산을 위한 유연한 Luna HSM 배포 옵션:

주요 장점:

완전한 키 소유권 및 인증된 보증 : 키는 고객 소유의 FIPS 검증 및 Common Criteria 인증 Luna HSM 내부에서 생성·저장·사용됩니다. 서명은 최고 수준의 보증으로 설계된 하드웨어 내에서 수행됩니다. Luna HSM에는 NIST 표준화 포스트 양자 알고리즘 지원을 포함한 암호화 민첩성(Crypto Agility)이 내장되어 있으며, 향후 신규 방식도 유연하게 채택할 수 있습니다.

기관 환경과의 원활한 통합: Luna HSM은 규제된 인프라와 통합되어 다양한 수탁 아키텍처를 지원하는 커스터디 플랫폼 및 블록체인 시스템에 연결되며, 보안·거버넌스·감사 팀의 운영 부담을 줄여줍니다.

핫(Hot), 웜(Warm), 콜드(Cold) 서명 워크플로우 지원: 기관은 통제된 메커니즘을 활용해 실시간 온라인 승인 또는 완전한 오프라인 서명을 실행할 수 있습니다. 이러한 유연성은 다양한 리스크 모델과 커스터디 방식을 지원합니다.

고급 거버넌스 및 정책 통제: Luna HSM은 다중 승인 서명, 주소 화이트리스팅, 거래 한도 등 세분화된 통제를 적용합니다. 변경 불가능한 로그는 감사 가능성과 규제 투명성을 지원합니다.

자산 토큰화 및 스마트 컨트랙트 지원: Luna HSM은 토큰화된 자산의 온체인 라이프사이클을 보호하고, 스테이블코인 및 실물 자산 토큰화를 포함한 스마트 컨트랙트 상호작용 서명을 지원합니다.

디지털 자산 에코시스템 전반 연결성: Luna HSM은 온램프·오프램프, 유동성 공급자, 발행기관, 결제 플랫폼과 연동하면서도 개인 키를 하드웨어 내에 완전히 보호합니다.

글로벌 규제 준비성 내재화: Luna HSM은 SFC, MAS, MiCA, BaFin, FINMA 등 주요 프레임워크와의 정합성을 지원합니다. 키, 테넌트, 정책의 세분화된 분리를 통해 환경을 특정 사업 단위, 지역, 규제 요건에 맞게 매핑할 수 있습니다.

디지털 자산 환경에 Luna HSM 보안을 제공하는 배포 모델

Luna HSM은 다양한 폼팩터로 제공되며, 디지털 자산 에코 시스템 전반에 걸쳐 키 생성, 접근 제어, 거래 서명을 위한 인증된 하드웨어 기반 신뢰 루트를 제공합니다.

요약

디지털 자산이 기관 금융의 핵심으로 이동함에 따라 개인 키 보호의 중요성은 어느 때보다 높아졌으며, 키 침해는 디지털 자산 플랫폼 전반에서 금융 손실의 가장 큰 원인 중 하나입니다. Thales Luna HSM은 인증된 고객 소유 하드웨어 내에서 키 생성·보호·거래 서명을 수행함으로써 기관들이 이 리스크에 대응할 수 있는 신뢰할 수 있는 방법을 제공합니다. FIPS 인증 및 Common Criteria 인증 HSM 내에 키를 보관함으로써 보안 태세를 강화하고, 규제 기대치를 충족하며, 오남용 및 도난 리스크를 크게 줄일 수 있습니다. Luna HSM은 선도적인 커스터디 플랫폼, 블록체인 및 토큰화 플랫폼, 더 넓은 디지털 자산 에코시스템과 통합됩니다. 암호화 민첩성과 양자 안전성을 갖춘 기반 위에 구축되고 유연한 배포 모델로 제공되는 Luna HSM은 디지털 자산 채택을 위한 루트 오브 트러스트를 제공하여, 고객과 규제 기관에 통제력을 입증하면서 기관들이 안전하게 확장할 수 있도록 지원합니다.

Thales 소개

Thales는 사이버보안 분야의 글로벌 리더로서, 전 세계 기업, 정부, 그리고 가장 신뢰받는 조직들이 핵심 애플리케이션, 민감한 데이터, 신원 정보, 소프트웨어를 어디서든 대규모로, 최고의 ROI로 보호할 수 있도록 지원합니다. Fortune Global 500의 58%를 포함한 30,000개 이상의 고객을 보유하고 있으며, 당사 솔루션은 전 세계 148개국에 배포되어 있습니다. 혁신적인 서비스와 통합 플랫폼을 통해 Thales는 고객들이 리스크 가시성을 높이고, 사이버 위협으로부터 방어하며, 규정 준수 격차를 해소하고, 수십억 명의 소비자에게 매일 신뢰할 수 있는 디지털 경험을 제공할 수 있도록 지원합니다.

Luna HSM에 대해 자세히 알아보기

DPoD에서 Hyperledger용 Luna Cloud 체험신청

연락처 – 모든 지사 위치 및 연락처 정보는 cpl.thalesgroup.com/contact-us를 참조하시기 바랍니다.