컴플라이언스 브리프

THALES
CYBERSECURITY

홍콩
디지털 자산
가이드라인
규제 준수

cpl.thalesgroup.com

THALES

CYBERSECURITY

Thales 솔루션을 통한 홍콩금융관리국**(HKMA)** 디지털 자산 가이드라인 준수 방안

디지털자산산업이지속적으로성장함에따라,홍콩금융관리국(HKMA)은 인가기관(AI: Authorized Institution)들이 디지털 자산 관련 활동에높은관심을보이고있음을확인했습니다.특히고객대상 디지털자산수탁서비스제공과,가상자산(VA)생태계의기반이 되는분산원장기술(DLT)을전통적금융시장운영에적용하는방안에 대한 관심이 높습니다.

HKMA는인가기관의디지털자산수탁서비스제공에대한가이던스와분산원장기술관련주요리스크관리고려사항에대한명확한 지침이 필요하다고 판단하여,'디지털 자산 수탁 서비스 제공에 관한준수기준'을2024년2월20일에,'분산원장기술사용관련 리스크 관리 고려사항'을 4월 16일에 각각 발표했습니다.

> 디지털자산은주로암호화기술과분산원장(DLT)또는유사기술에의존하는자산으로,가상자산(VA),토큰화증권및기타토큰화자산을 포함합니다.

"디지털 자산 수탁 서비스 제공에 관한 준수 기준"이란 무엇입니까?

국제표준및관행을참조하여,HKMA는2024년2월20일인가기관의디지털자산수탁서비스제공에관한준수기준가이던스를발표했습니다.8개범주의준수기준을포함한이가이던스는인가기관이보유한고객디지털자산의적절한보호와적정한관리를보장하는것을목표로합니다.HKMA는이미디지털자산수탁활동에 종사하고있는인가기관또는국내설립인가기관의자회사가2024년2월20일부터6개월이내에가이던스에명시된준수기준을충족함을 HKMA에 확인하도록 의무화했습니다.

Thales의 지원 방안

Thales는고객디지털자산보호에관한준수기준을충족시킴으로써 인가기관의디지털자산수탁서비스제공가이던스준수를지원합니다.인가기관은Thales의ID및데이터보안솔루션제품군을활용하여수탁중인고객디지털자산을적절히보호하고관련리스크를 적정하게 관리할 수 있습니다.

디지털 자산 수탁 서비스 제공 준수 기준

준수 기준 가이드라인	**Thales** 솔루션
C. 11) 고객 디지털 자산 보호 • 시드(Seed:키 생성용 초기값) 및 개인키의 생성·저장'-백업을 함한 시드 및 개인키를 하드웨어 보안 모듈(HSM)과 같은 안전하고 변조 방지가 가능한 환경 및 장치에서 생성·저장 • 홍콩 내 시드 및 개인키의 안전한 생성, 저장, 백업 • 암호화장치또는애플리케이션에대한접근을업무상필요한 경우에만 엄격히 제한 • 다단계인증(MFA)과같은강력한인증방식을사용하여시드및 개인키접근인증;암호화장치또는애플리케이션에대한접근 감사 추적 유지	인가기관은 Thales 하드웨어 보안 모듈(HSM)을 통해 지갑의 개인키와시드를저장,보호,관리함으로써고객디지털자산을 보호할 수 있습니다. 이 모듈은 BIP32, SLIP10 등 지갑 솔루션 프로토콜을지원하며,블록체인에서널리사용되는SECP256k1, curve25519, ed25519 등 다양한 타원곡선 암호화 알고리즘을 제공합니다. • Luna Network HSM은 FIPS 140-3 전용암호화모듈에서트랜잭션 서명을 위한 키의 전체 수명주기를 보호하여 고객 디지털 자산을 안전하게 보호합니다. Thales Luna HSM은 업계 최초로 FIPS 140-3 Level 3 인증을 획득했습니다. 안전한암호화처리,키 생성 및 보호,암호화 등을 위한강화되고 변조방지된 환경을 제공하며,비인가 장치나 사용자가 암호화 키에 접근, 수정, 사용할 수 없도록 보장합니다.

• "단일 장애지점**(Single Point of Failure)**" 방지 • 수탁 프로세스에 사용되는 스마트 컨트랙트가 높은 수준의 뢰도로 계약 취약점이나 보안 결함이 없도록 보장하는 조치 구현	• ProtectServer HSM은 Luna Network HSM과 마찬가지로, 암호화·서명·인증 서비스를 제공하는 동시에 암호화 키를 안전하게 보호하도록 설계되었습니다. Luna HSM과 ProtectServer HSM은 각각 FIPS 140-3 및 FIPS 140-2 Level 3 인증을 획득하여, 데이터 레지던시 요건을 준수하면서 홍콩 내에서 암호화 키를 안전하고 변조 방지 환경에서 관리할 수 있도록 지원합니다. 이러한 HSM에 대한 접근은 강력한 다중 인증**(MFA)**과 모든 작업에 대한 상세한 감사 추적을 통해 엄격히 통제되며, 이를 통해 보안성과 규정 준수 수준을 한층 강화합니다. 단일 장애지점(Single Point of Failure)을 방지하기 위해, 두 **HSM** 모두 로드 밸런싱을 통한 고가용성 기능을 지원하여 미션 크리티컬 환경을 보호하며, 이는 글로벌 모범 사례 및 HKMA의 보안 요건에 부합합니다.
C. 11) 고객 디지털 자산 보호 • 시드 및 개인키에 대한 적절한 오프사이트 백업 및 비상 대책 보유 - 원본 시드 및 개인키와 동일한 보안 통제를 적용해야 함. 백업된 시드 및 개인키는 원본이 저장된 주요 위치와 분리되고 해당 위치의 이벤트에 영향받지 않는 안전한 물리적 장소에 오프라인으로 보관해야 함	AI 기업은 외부 HSM에 백업을 저장하고 온프레미스 옵션을 통해 홍콩 내에서 암호화 키를 관리할 수 있습니다. • 컴플라이언스 준수 및 긴급 상황·장애·재해 발생 시 안전한 보호를 위해 Luna Backup HSM으로 키를 간편하게 백업하고 안전하게 복제하세요. Luna Backup HSM은 최고 수준의 보안성과 컴플라이언스를 제공합니다. ◦ 키는 FIPS 140-2 Level 3 인증을 받은 침입 방지·변조 감지 하드웨어 내에 항상 안전하게 보관됩니다. ◦ 원격 관리, 백업 및 복원을 통해 신속한 재해 복구가 가능합니다. ◦ LCD 터치스크린으로 펌웨어, 메모리 용량 등 주요 상태를 빠르게 확인할 수 있습니다. ◦ 독립 실행형 쿼럼(MofN) 다중 인증(MFA) 지원으로 보안성을 한층 강화합니다. Thales ProtectServer HSM은 NIST FIPS 140-2 Level 3 인증 스마트 카드를 활용하여 암호화 키의 안전한 백업·복구·이전을 위한 최고 수준의 보안성과 관리 편의성을 제공합니다. 또한 MFA 및 MofN 기반 백업을 지원하여 인증 및 권한 부여 프로세스의 보안성을 더욱 강화합니다.

"분산원장기술(DLT) 사용 관련 리스크 관리 고려사항"이란 무엇입니까?

HKMA는 인가기관이 분산원장기술 관련 사업계획이나 신규 서비스 도입 시 제출하는 문서를 검토할 때 고려하는 주요 리스크 관리 사항에 대해 더 명확한 지침을 제공하는 것이 유용하다고 판단했습니다. 분산원장기술 도입과 일반적으로 관련된 공통 리스크 영역이 있으므로, HKMA는 '거버넌스', '애플리케이션 설계 및 개발', '지속적인 유지보수 및 모니터링'의 **3**가지 주요 감독 고려사항을 담은 노트를 준비했습니다. 인가기관은 분산원장기술 관련 제출 자료를 준비할 때 이러한 고려사항을 감안할 것을 권장합니다.

Thales가 제시하는 해답

Thales는 지속적인 유지관리 및 모니터링 요건을 충족시킴으로써, AI 기업이 DLT 활용과 관련된 리스크 관리 고려사항을 준수할 수 있도록 지원합니다. AI 기업은 DLT 관련 솔루션을 설계·개발하는 과정에서 Thales의 통합 ID 및 데이터 보안 솔루션을 활용할 수 있습니다.

'분산원장기술(DLT) 사용 관련 리스크 관리 고려사항'이란?

고려사항	Thales 솔루션
지속적인 유지보수 및 모니터링 **7.** 전통적 기술 애플리케이션에 상응하는 수준의 사이버 보안 구축 • 위협행위자의 새로운 공격 수법과 분산원장기술 애플리케이션의 보안에 영향을 미칠 수 있는 신기술 발전(예: 양자컴퓨팅)에 대해 경계를 유지하고, 대응역량을 정기적으로 업데이트해야 함	Thales Luna HSM 양자내성암호(PQC) 기능모듈(FM)'을 통해 인가기관은 코드서명 또는 PKI 기반 사용사례에 NIST 3차 최종 후보 양자 보안 암호화 메커니즘을 현재 사용할 수 있습니다. • AI 기업이 양자내성 디지털 서명 알고리즘을 미래지향적으로 표준화할 수 있도록 지원합니다. 이를 통해 장기적으로 안전하고 인증된 소프트웨어/펌웨어 업데이트를 제공할 수 있습니다. • PQC FM은 하드웨어 변경이나 업그레이드 없이 PCIe 및 Network HSM에 설치할 수 있습니다. 변조 방지 기능을 갖춘 HSM은 양자내성키를 안전하고 효율적으로 생성·관리합니다. • 표준화된 양자 내성 공개 키 암호화를 통해 디지털 서명을 원활하게 생성하며, SP 800-208 요건을 준수하는 상태 비저장(Stateless) 및 상태 저장(Stateful) 키 유형에 대한 키 관리 기능을 포함합니다. • Luna PQC FM은 다양한 Thales 기술 파트너사와 함께 양자 내성 PKI, TLS 또는 VPN을 구성하여 암호화 민첩성(Crypto Agility)을 검증할 수 있습니다.
지속적인 유지보수 및 모니터링 **8.** 개인키의 안전한 관리 • 보유하거나 관리 중인 모든 개인키에 대해 애플리케이션의 성격 및 리스크, 키와 연관된 기초 자산에 적합한 수준의 보안을 제공하기 위한 강력한 정책 및 절차가 마련되어 있음을 입증해야 함	인가기관은 'Luna Network HSM' 및 'ProtectServer HSM'을 통해 시드와 개인키를 안전하게 관리할 수 있습니다. 두 HSM 모두 BIP32를 지원하며 기능모듈(FM)을 사용하여 맞춤형 암호화를 안전하게 수행하거나 맞춤형 블록체인 알고리즘을 추가합니다. • Luna Network HSM은 암호화 키를 저장, 보호, 관리하여 민감한 데이터와 핵심 애플리케이션을 보호합니다 - Luna Network HSM은 시장을 선도하는 고신뢰성, 변조 방지, 네트워크 연결형 어플라이언스입니다. • ProtectServer HSM은 암호화, 서명, 인증서비스를 제공하면서 암호화 키를 보호하도록 설계되었습니다.
8. 개인키의 안전한 관리 • 관련 개인키(및 해당되는 경우 씨드)가 항상 안전하게 생성·보관·백업되도록 보장해야 합니다.	외부 HSM을 통해 AI 기업은 아래 옵션으로 백업을 저장할 수 있습니다. • 컴플라이언스 준수 및 긴급 상황·장애·재해 발생 시 안전한 보호를 위해 AI 기업은 Luna Backup HSM으로 키를 간편하게 백업하고 안전하게 복제할 수 있습니다. Luna Backup HSM은 최고 수준의 보안성과 컴플라이언스를 제공합니다. ◦ 키는 FIPS 140-2 Level 3 인증을 받은 침입 방지·변조 감지 하드웨어 내에 항상 안전하게 보관됩니다. ◦ 원격 관리, 백업 및 복원을 통해 신속한 재해 복구가 가능합니다. ◦ LCD 터치스크린으로 펌웨어, 메모리 용량 등 주요 상태를 빠르게 확인할 수 있습니다. ◦ 독립실행형 쿼럼(MofN) 다중인증(MFA) 지원으로 보안성을 한층 강화합니다. • Thales ProtectServer HSM은 스마트 카드를 활용하여 암호화 키의 안전한 백업·복구·이전을 위한 최고 수준의 보안성과 관리 편의성을 제공합니다.