Compliance Brief

Complying with the Guidelines for Digital Assets in Hong Kong

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

How Thales solutions help Authorized Institutions (AIs) with Guidance on Digital Assets by Hong Kong Monetary Authority (HKMA)

As the digital asset sector continues to grow, the Hong Kong Monetary Authority (HKMA) has seen authorized institutions (AIs) increasingly interested in digital asset-related activities, in particular provision of custodial services for digital assets for clients and how to apply the distributed ledger technology (DLT) that underlies the Virtual Assets (VA) ecosystem to traditional financial market operations.

The HKMA considers it necessary to guide AIs' provision of digital asset custodial services and useful to provide more clarity on the key risk management considerations on DLT, the **Guidance on Expected Standards on Provision of Custodial Services for Digital Assets** and **Risk management considerations related to the use of DLT** were issued on 20 February and 16 April respectively.

Digital assets are assets that depend primarily on cryptography and distributed ledger (DLT) or similar technologies, and include VAs, tokenized securities and other tokenized assets.

What is the "Expected Standards on Provision of Custodial Services for Digital Assets"?

With reference to international standards and practices, the HKMA issued guidance on **Expected Standards on Provision of Custodial Services For Digital Assets** by AIs on 20 February 2024. This guidance with 8 categories of expected standards aims to ensure the adequate safeguarding and proper management of client digital assets held by authorized institutions (AIs). The HKMA has mandated that AIs or subsidiaries of locally incorporated AIs already engaging in digital asset custodial activities are to confirm with the HKMA that they meet the expected standards set out in the Guidance **within 6 months from 20 February 2024**.

How can Thales help?

Thales helps AIs comply with Guidance on the Provision of Custodial Services for Digital Assets by addressing the expected standard on **Safeguarding of client digital assets**. AIs can leverage Thales' suite of identity and data security solutions to ensure client digital assets in custody are adequately safeguarded and the risks involved are properly managed.

Expected Standards on Provision of Custodial Services For Digital Assets

Guidelines on Expected Standards	Thales Solution
C. 11) Safeguarding of client digital assets • Generating and storing seeds and private keys, including their backups, in **secure and tamper-resistant environment and devices**, such as **hardware security module (HSM)**. • Securely generating, storing and backing up **seeds and private keys in Hong Kong** • **Strictly restricting access** to cryptographic devices or applications on a need-to-know basis • Using strong authentication method, such as multi-factor authentication, to **authenticate access to seeds and private keys; maintaining audit trail** of the access to the cryptographic devices or applications	AIs can secure clients' digital assets by storing, protecting and managing private keys and seeds of wallets with Thales Hardware Security Modules (HSM). These modules support wallet solution protocols such as BIP32 and SLIP10 and offer a range of curves including SECP256k1, curve25519, and ed25519. • Luna Network HSMs protect the entire lifecycle of the keys to sign transactions in a FIPS 140-3 dedicated cryptographic module to secure client digital assets. Thales Luna HSMs are the first in the industry to receive the FIPS 140-3 Level 3 validation. It provides a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption and more; and ensures that cryptographic keys cannot be accessed, modified or used by unauthorized devices or people.

- Avoid any "**single point of failure**"
- Implementing measures to ensure that any **smart contract** used in the custody process is not subject to any contract vulnerabilities or security flaws to a high level of confidence

- ProtectServer HSMs, like the Luna Network HSMs, are designed to protect cryptographic keys against compromise while providing encryption, signing, and authentication services.

Luna and Protect Server HSMs are certified to FIPS 140-3 and FIPS 140-2 Level 3 standards respectively, ensuring secure, tamper-resistant environments for **managing cryptographic keys within Hong Kong**, in compliance with data residency requirements. Access to these HSMs is tightly controlled, with **strong multi-factor authentication and detailed audit trails** for all operations, enhancing security and regulatory compliance.

To avoid any single point of failure, both **HSMs support the high availability, features with load balancing** to protect this mission-critical environment, which aligns with the global best practices and HKMA's security expectations.

C. 11) Safeguarding of client digital assets

- Having **adequate offsite backups and contingency arrangements for seeds and private keys**, which should be subject to the same security controls as the original seeds and private keys. Backed up seeds and private keys should be kept offline in a secure physical location that is separate from and will not be affected by any event at the primary location where the original seeds and private keys are stored

AIs can store backups on external HSMs and **manage cryptographic keys in HK** with on-premises options:

- Backup easily and duplicate keys securely to the Luna Backup HSM for compliance as well as safekeeping in case of emergency, failure or disaster. Luna Backup HSM provides the highest security and compliance.
  - Keys always remain in FIPS 140-2 Level 3 validated, intrusion-resistant, tamper-evident hardware
  - Remote management, backup and restoration for quick disaster recovery
  - LCD touch screen enables quick review of status including firmware, memory capacity, and more
  - Standalone support of Quorum (MofN) multi-factor authentication for increased security
- Thales ProtectServer HSM uses NIST FIPS 140-2 Level 3 validated smart cards to provide the highest security and administrative convenience for secure backup, recovery, and transfer of cryptographic keys. It also supports backups with MFA and MofN to further enhance the security of authentication and authorization processes.

What are "Risk management considerations related to the use of distributed ledger technology"?

The HKMA considers it useful to provide more clarity on the key risk management considerations that it has regard to when reviewing the DLT-related proposals of AIs. Since some common risk areas are generally relevant to DLT adoption, the HKMA has prepared a note setting out **3 key supervisory considerations** on Governance, Application design and development, and On-going maintenance and monitoring. AIs are encouraged to take into account these considerations when preparing their DLT-related submissions.

How can Thales help?

Thales helps AIs comply with the risk management considerations related to the use of DLT by addressing the **On-going maintenance and monitoring** considerations. AIs can leverage Thales' suite of identity and data security solutions when designing and developing their DLT-related solutions.

Risk Management Considerations Related to The Use of DLT

Considerations	Thales Solution
On-going maintenance and monitoring **7. Establish level of cybersecurity commensurate with traditional technology applications** • Stay vigilant to the emerging modus operandi of threat actors and developments in **novel technologies that may affect the security of DLT applications (e.g. quantum computing)**, and regularly update their response capabilities.	Thales Luna HSMs Post-Quantum Cryptography (PQC) Functionality Module (FM) allows AIs to use the round 3 NIST finalists quantum-safe crypto mechanisms to be used today for use cases such as code-signing or others that rely on PKI. • It enables AIs to future-proof and standardize **quantum-safe digital signature algorithms**. It ensures AIs deliver secure and authenticated software/ firmware updates far into the future. • The PQC FM can be installed on the PCIe and Network HSM without making any hardware changes or upgrades. The tamper-resistant HSMs can securely create and manage **quantum-resistant keys** effectively. • It generates digital signatures seamlessly using standardized **quantum-safe public key cryptography** and includes key management capabilities for stateless and stateful key types, complying with SP 800-208 requirements. • Luna PQC FM helps validate your crypto agility by setting up **quantum-safe** PKI, TLS, or VPN with a wide variety of Thales technology partners.
On-going maintenance and monitoring **8. Securely manage private key** • Demonstrate that **robust policies and procedures** are in place to provide a level of security to any private keys held or under their management that are appropriate for the nature and risks of the application, the underlying assets associated with the keys.	AIs can manage seeds and private keys securely with Luna Network HSMs and ProtectServer HSMs. Both the HSMs support BIP32 and use Functionality Module (FM) to securely perform custom cryptography, or add custom blockchain algorithms. • Luna Network HSMs secure sensitive data and critical applications by storing, protecting, and managing cryptographic keys – high assurance, tamper-resistant, network-attached appliances offering market-leading • ProtectServer HSMs are designed to protect cryptographic keys while providing encryption, signing, and authentication services.
8. Securely manage private key • Ensure that the associated private keys (and seeds as applicable) are securely **generated, stored and backed up at all times**.	External HSMs allows AIs to store backups with options below: • AIs can backup easily and duplicate keys securely to the Luna Backup HSM for compliance as well as safekeeping in case of emergency, failure or disaster. Luna Backup HSM provides the highest security & compliance. ◦ Keys always remain in FIPS 140-2 Level 3 certified, intrusion-resistant, tamper-evident hardware ◦ Remote management, backup and restoration for quick disaster recovery ◦ LCD touch screen enables quick review of status including firmware, memory capacity, and more ◦ Standalone support of Quorum (MofN) multi-factor authentication for increased security • Thales ProtectServer HSM uses Smart Cards which provide the highest security and administrative convenience for secure backup, recovery, and transfer of cryptographic keys.