Comment for Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

Company: <u>Thales</u> (Cloud Protection and Licensing) Contact: Email Tel:

To whom it may concern:

I am writing on behalf of Thales (Cloud Protection and Licensing) to provide our feedback to the Consultation Paper on the **Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed**. We believe that enhancing the security of trading platforms to protect virtual assets investors would be crucial.

With the evolution of the virtual asset market and the increasing interconnectedness of the ecosystem with the traditional financial system, virtual asset operators should effectively mitigate the cyber risks of their platforms with a focus on **cryptographic key management**. It is essential to have strong cryptographic key management practices in place to ensure the security and integrity of the users' assets.

The consultation paper covers some of the key requirements on cryptographic requirements in Section X – Custody of Client Assets (10.8), which are critical capabilities to a secure virtual asset platform, such as secure key storage and management; limited and controlled access, and physical and logical isolation. To further enhance the alignment with the industry standard and catch up with the evolving cryptographic development, we recommend introducing cryptographic capabilities in the regulatory requirement with detail below:

1. Cryptographic capabilities:

- Support industry-standard cryptographic algorithms and key lengths, such as AES-256, RSA-2048, and ECDSA with secp256k1 curve, to ensure secure key generation, storage, and management
- Since the industry always introduces new algorithms, the system should have capabilities to allow developers to develop their own code and curve to perform cryptographic operations inside systems and make sure no cryptographic operations will be performed outside the systems.

Here are the other key capabilities of cryptographic key management for securing virtual asset trading platforms, which are included in the consultation paper (10.8):

- 1. Tamper-resistant system:
 - Ensure that any attempts to physically access or modify the system's internal components are detected, and the system can automatically erase or disable access to sensitive data in such an event which make it impossible to compromise

Comment for Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

2. Secure key storage and management:

- Private keys and seeds must be stored in a secure, encrypted format within the cryptographic key management system and with strict access control policies.
- Provide mechanisms for key backup and recovery, as well as secure key import and export, to prevent key loss or leakage.
- An air-gapped offsite backup system with the same security standard is highly recommended.

3. Limited and controlled access:

 Enforce strict access control measures to ensure that only authorized users or systems can access. This includes the use of multi-factor authentication, rolebased access control, and secure audit logging of all access attempts and actions performed on the system.

4. **Physical and logical isolation:**

The cryptographic key management system should be physically and logically isolated from other systems and networks, ensuring that any potential security vulnerabilities in surrounding systems do not compromise the security of the system and the keys that it protects.

These recommended capabilities of cryptographic key management are also listed as mandatory requirements in the following regulations or guidelines in HK and Singapore.

- 1. Positioning paper of "<u>Regulation of virtual asset trading platforms</u>" by SFC on Nov 6th, 2019
 - SFC has included the requirement on cryptographic key management in the <u>Terms and Conditions for Virtual Asset Trading Platform Operators</u> under "Custody of Client Assets".
 - 7.6: "A Platform Operator should establish and implement strong internal controls and governance procedures for private key management to ensure all cryptographic seeds and private keys are securely generated, stored and backed up."
 - 7.6(a): "Where practicable, seeds and private keys should be generated offline and kept in a secure environment, such as a Hardware Storage Module (HSM), with appropriate certification for the lifetime of the seeds or private keys."
 - URL: <u>https://www.sfc.hk/-/media/EN/files/ER/PDF/20191106-Position-Paper-and-Appendix-1-to-Position-Paper-Eng.pdf</u>
- 2. Technology Risk Management (TRM) Guidelines by the Monetary of Singapore (MAS), January 2021
 - MAS Technology Risk Management Guidelines set out the requirements of Cryptographic key management in the 10.2 section with details below:

Comment for Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

- 10.2.4: "To protect sensitive cryptographic keys, the FI should manage, process and store such keys in hardened and tamper-resistant systems, e.g. by using a hardware security module."
- 10.2.5: "Where sensitive cryptographic keys need to be transmitted, the FI should ensure these keys are not exposed during transmission. The keys should be distributed to the intended recipient via an out-of-band channel or other secure means to minimize the risk of interception."
- URL: <u>https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/trm-guidelines-18-january-2021.pdf</u>
- 3. Secure Tertiary Data Backup (STDB) Guidelines by Hong Kong Association of Banks (HKAB), April 30, 2021
 - Secure Tertiary Data Backup (STDB), which is designed for the banking landscape in Hong Kong, includes requirements on managing cryptographic keys to ensure data security with the guidance below.
 - Principle #5: "Als should implement controls to provide reasonable assurance that throughout the data extraction and ingestion processes, critical data is encrypted in accordance with industry good practices and transmitted completely and accurately on a regular basis."
 - Processes and controls should be in place to locate and catalogue encrypted files and protect associated cryptographic keys. The catalogue and cryptographic keys should be maintained on secure (e.g. tamper proof), survivable and transportable media.
 - Encrypted keys should be securely stored and restricted to authorized personnel during storage, physical transportation, STDB handover and activation.
 - URL: <u>https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-</u> <u>circular/2021/20210518e1.pdf</u>

In conclusion, we are aligned with the proposal on cryptographic key management in the consultation paper (10.8), our recommendation focuses on enhancing the requirements for **cryptographic capabilities**, which aligns the industry standards and responds to technology development on new algorithms. By implementing effective cryptographic key management practices, virtual asset operators can reduce the risk of data breaches and maintain regulatory compliance.

