HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C
G16/1C

20 February 2024

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Provision of Custodial Services for Digital Assets

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[1] for clients.

To ensure that such client digital assets held by AIs in custody are adequately safeguarded and that the risks involved are properly managed, the HKMA considers it necessary to provide guidance on AIs' provision of digital asset custodial services. With reference to international standards and practices, the HKMA sets out the expected standards in the Annex, which have incorporated flexibility for AIs to put in place operational arrangements that are commensurate with the nature, features and risks of the digital assets under custody. AIs should apply these standards in safeguarding client digital assets, whether the assets are received in the course of conducting virtual asset (VA)-related activities as an intermediary[2], distributing tokenised products, or providing standalone custodial services.

---

[1] For the purpose of this circular, the term "digital assets" refers to digital assets that depend primarily on cryptography and distributed ledger or similar technology, such as virtual assets as defined in section 53ZRA of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), tokenised securities and other tokenised assets. The term "digital assets" should be read to also cover the means of access to a digital asset, which generally refers to private keys, seeds or their backups. Limited purpose digital token, as defined in section 53ZR of the AMLO, is excluded from the scope of this circular. This circular is not applicable to custody of proprietary assets of an AI or its group companies which are not held on behalf of clients.

[2] See "Joint circular on intermediaries' virtual asset-related activities" issued by the HKMA and the Securities and Futures Commission (last updated on 22 December 2023).

In addition to the expected standards set out in the Annex, AIs are reminded to also comply with all the applicable legal and regulatory requirements when providing digital asset custodial services.

This circular applies to AIs and subsidiaries of locally incorporated AIs that conduct digital asset custodial activities. The locally incorporated AIs should ensure that the business conduct, practices and controls of such subsidiaries comply with this circular and the Annex.

Implementation

AIs which by themselves or (in the case of locally incorporated AIs) whose subsidiaries intend to provide digital asset custodial services should discuss with the HKMA in advance and demonstrate to the satisfaction of the HKMA that they meet the expected standards and requirements in this circular (as amended from time to time).

AIs or subsidiaries of locally incorporated AIs already engaging in digital asset custodial activities should review and revise as necessary their systems and controls. Such AIs or the relevant locally incorporated AIs (with subsidiaries already engaging in such activities) should notify the HKMA and confirm that they meet the expected standards in the Annex within **six months** from the date of this circular.

The HKMA will keep in view the evolving digital asset market and international regulatory landscape, and may provide further guidance as and when necessary. Should you have any questions regarding this circular, please contact Mr Kane Chau at 2878-8310 or Ms Katy Chan at 2878-1210.

Yours faithfully,

Alan Au
Executive Director (Banking Conduct)

Encl.
c.c. Securities and Futures Commission
(Attn: Mr Keith Choy, Interim Head, Intermediaries)

Annex

Guidance on Expected Standards on Provision of Custodial Services for Digital Assets by Authorized Institutions

This guidance applies to custodial activities of digital assets (i.e. assets that depend primarily on cryptography and distributed ledger or similar technology), except limited purpose digital token[1], held on behalf of clients (hereafter called "client digital assets") by authorized institutions (AIs) and subsidiaries of locally incorporated AIs[2]. As an illustration, assets covered include virtual assets (VAs)[3], tokenised securities and other tokenised assets[4]. This guidance is not applicable to custody of proprietary assets of an AI or its group companies which are not held on behalf of clients.

(A) Governance and risk management

1. Prior to launching custodial services for digital assets, an AI should undertake a comprehensive risk assessment to identify and understand the associated risks. The AI should put in place appropriate policies, procedures and control measures to manage and mitigate the identified risks, taking into account applicable legal and regulatory requirements. The board and senior management of the AI should exercise effective oversight of the risk management process to ensure that the risks associated with the custodial activities are identified, assessed, managed and mitigated both before the engagement in the custodial activities and on an ongoing basis.

---

1 As defined in section 53ZR of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO).

2 For the purposes of the rest of this Annex, the term "AI" includes a subsidiary of a locally incorporated AI which provides digital asset custodial services.

3 As defined in section 53ZRA of the AMLO.

4 "Tokenised securities" and "other tokenised assets" generally refer to digital representations of "securities" as defined under the Securities and Futures Ordinance and other real-world assets respectively, using distributed ledger or similar technology to record ownership.

2. An AI should allocate adequate resources, including the necessary manpower and expertise, for its custodial activities to ensure proper governance, operations and effective risk management. Senior management and staff engaging in the AI's custodial activities and related control functions should possess the necessary knowledge, skills and expertise to discharge their responsibilities.

3. Given the fast-evolving development in the digital asset space, an AI should ensure that sufficient training is provided to the senior management and staff involved in the custodial activities to remain competent on an ongoing basis.

4. An AI should have appropriate accountability arrangement for the custodial activities, including setting out written and clear roles and responsibilities as well as reporting lines. There should also be adequate policies and processes to identify, manage and mitigate any potential and/or actual conflicts of interest that may arise, for example, among different activities undertaken by the AI or its affiliates.

5. An AI should establish and maintain effective contingency and disaster recovery arrangements to ensure business continuity of its custodial activities.

(B) Segregation of client digital assets

6. An AI should hold client digital assets in separate client accounts[5] that are segregated from the AI's own assets to ensure that client digital assets are protected from claims of the AI's creditors in the event of an insolvency or resolution of the AI.

7. An AI should not transfer any right, interest, ownership, legal and/or beneficial titles in the client digital assets or otherwise lend, pledge, re-pledge or create any encumbrance over the client digital assets, except for

[5] Including wallet address(es) holding client digital assets on distributed ledger which should be segregated from that used for holding the AI's own assets.

(i) the settlement of transactions, and/or fees and charges owed by the client to the AI; (ii) where prior explicit written consent of the client is obtained; or (iii) where it is required by law. The AI should have adequate and effective measures to prevent the use of client digital assets for its own account or for purposes other than those agreed with its clients.

(C) Safeguarding of client digital assets

8. An AI should put in place adequate systems and controls to ensure that client digital assets are promptly and properly accounted for and adequately safeguarded. In particular, the AI should have effective control measures to minimise the risk of loss of client digital assets due to theft, fraud, negligence or other acts of misappropriation, as well as delayed access or inaccessibility of client digital assets.

9. In developing the systems and controls to safeguard client digital assets, an AI may adopt a risk-based approach, taking into account the nature, features and risks of the digital assets held in its custody. Risks may be dependent on, for example, the type of distributed ledger technology (DLT) network used (such as private-permissioned, public-permissioned and public-permissionless) as well as the mitigation measures in place. For instance, client digital assets held as permissionless tokens on a public-permissionless DLT network may be exposed to heightened cybersecurity risks, and recovery of lost assets may be difficult in the event of theft, hacking or other cyberattacks, compared with public-permissioned and private-permissioned DLT networks where there may be controls of access to the DLT networks.

10. Systems and controls to safeguard client digital assets include, among others, written policies and procedures for:

- authorising and validating access to effecting deposit, withdrawal and transfer of client digital assets, including the access to the devices storing seeds and private keys; and

- managing and safeguarding seeds and private keys of client digital assets, covering key generation, distribution, storage, use, destruction and backup.

11. In particular, an AI is expected to adopt relevant industry best practices and follow applicable international security standards in safeguarding client digital assets in a way that is commensurate with the nature, features and risks of the assets being held. While the procedures and controls set out below are not intended to be prescriptive or one-size-fits-all, they are generally required for an AI which holds client VAs. For other digital assets, an AI may adopt a risk-based approach in the implementation of the following procedures and controls commensurate with the risks posed but if such digital assets are in the form of permissionless tokens on a public-permissionless DLT network, an AI also should exercise extra caution and critically assess the implementation:

- generating and storing seeds and private keys, including their backups, in secure and tamper-resistant environment and devices, such as hardware security module (HSM). Where practicable, seeds and private keys should be generated offline with an appropriate lifetime limit;

- 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 to authorised personnel with appropriate screening and training; maintaining up-to-date documentation of how the access is authorised and validated as well as the access rights allocated; 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;

- implementing robust controls to avoid any "single point of failure" by way of, for example, using key sharding or similar technology to split

and distribute a private key among multiple personnel authorised by the AI for distributed storage so that no single party holds the entirety of the key. Generally, a certain number of key shard holders are required to act collectively to sign a transaction to ensure that no single person possesses full access, while preventing operation interruption when a single shard is lost, unavailable or stolen. To prevent "single point of failure", the use of multiple wallets, instead of one single wallet, to hold client digital assets may also be considered;

- putting in place controls to prevent and mitigate the risk of collusion among authorised personnel with access to the seeds and private keys;

- 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;

- storing a substantial portion[6] of client digital assets in cold storage unconnected to the Internet, unless otherwise justified;

- allowing deposit and withdrawal of client digital assets only through wallet addresses that belong to clients[7] (e.g. through proof of ownership test, such as message signing or micropayment test) and are whitelisted;

- 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; and

[6] Where client digital assets under custody are VAs, an AI should store 98% of the client digital assets in cold storage.

[7] "clients" also refer to clients of another AI or a licensed corporation which holds digital assets on their behalf in an account maintained with the AI.

- maintaining an appropriate insurance or compensation arrangement[8] to adequately cover any loss of client digital assets, which may arise from, among others, hacking incidents on the AI, theft or fraud (whether or not as a result of the AI's acts, errors, omissions, or gross negligence).

12. Where an AI offers a user interface or portal for clients to manage their digital assets held by the AI, effective client authentication and notification controls should be put in place, following relevant guidance set out by the Hong Kong Monetary Authority (HKMA) from time to time.

13. An AI should closely monitor the trends and developments in emerging security threats, vulnerabilities, attack and fraud risks as well as technological solutions; evaluate periodically the adequacy and robustness of the security risk controls having regard to the emerging threats and technological advancements; and put in place measures to keep the technology to safekeep client digital assets in line with relevant industry best practices and applicable international standards. The wallet storage technology used for keeping client digital assets should be tested before deployment to ensure reliability.

(D) Delegation and outsourcing

14. As a general principle[9], as far as VAs are concerned, an AI may only delegate or outsource its custody function to (i) another AI (or a subsidiary of a locally incorporated AI); or (ii) a VA trading platform[10] licensed by the Securities and Futures Commission. For digital assets other than VAs, if they are in the form of permissionless tokens on a public-permissionless DLT network, the AI should exercise extra caution and critically assess whether it is appropriate to delegate or outsource its custody function.

---

[8] Where client digital assets under custody are VAs, an AI should have in place a compensation arrangement or insurance that covers potential loss of 50% of the client digital assets in cold storage and 100% of the client digital assets in hot and other storages.

[9] See Part X paragraph 10.1 of "Guidelines for Virtual Asset Trading Platform Operators" (June 2023) and paragraph 19 of "Circular on SFC-authorised funds with exposures to virtual assets" (22 December 2023), both issued by the Securities and Futures Commission, for reference.

[10] Which may hold VAs through its Associated Entity.

15. Where an AI enters into a delegation or outsourcing arrangement in the provision of digital asset custodial services, the AI should perform appropriate due diligence before selecting and appointing the delegate or service provider. The AI should assess and be satisfied with, among others, the delegate or service provider's financial soundness, reputation, managerial skills, technical and operational capability and capacity to ensure compliance with the expected standards set out in this Annex and other applicable legal and regulatory requirements, as well as the ability and capacity to keep pace with the technological developments on the digital asset front. The due diligence assessment and its result should be documented with proper record keeping. The AI should have effective controls in place to monitor the performance of the delegate or service provider on an ongoing basis.

16. When engaging a delegate or service provider in the provision of digital asset custodial services, an AI should have the technical expertise to assess the effectiveness of the solutions deployed in safeguarding clients' digital assets, and whether it introduces any single point of failure. The AI should also fully understand the terms and conditions under which the delegate or service provider holds the client digital assets, and assess whether it will materially affect the legal rights of the client, including in the event of insolvency of the delegate or service provider. It is the AI's responsibility to ensure that the delegate or service provider segregates client digital assets properly in accordance with paragraphs 6 and 7 of this Annex.

17. An AI's contingency and disaster recovery arrangements should cover the scenario of disruption to the delegated or outsourced digital asset custodial services. The AI should also assess the delegate or service provider's resilience capabilities, including their contingency plans and procedures, to ensure availability of the custodial service.

18. An AI is reminded to also maintain relevant systems and controls as in delegation or outsourcing arrangements for traditional financial activities.

19. The ultimate responsibility and accountability for any delegated or outsourced activities rest with an AI.

(E) Disclosure

20. An AI should provide its clients with full and fair disclosure of the custodial arrangements in a clear and easily comprehensible manner including:

- the respective rights and obligations of the AI and its clients, including the clients' rights of ownership to their assets in the event of the AI entering insolvency or resolution;

- the custodial arrangement, including how client digital assets are stored and segregated, the procedures and the time taken to deposit and withdraw client digital assets, and any applicable fees and costs;

- the insurance / compensation arrangement to cover potential loss of client digital assets caused by, for example, security incidents or misappropriation;

- any existence of client digital assets commingled with assets of other clients, and the risks involved;

- the circumstances and the arrangement where the AI will take legal and/or beneficial title to the client digital assets, or otherwise transfer, lend, pledge, re-pledge or create any encumbrance over the client digital assets, and the risks involved;

- the treatment of client digital assets and their respective rights and entitlements in events such as voting, hard forks and airdrops; and

- the existence and the nature of any potential and/or actual conflicts of interest associated with the custodial activities of the AI.

(F) Record keeping and reconciliation of client digital assets

21. An AI should maintain appropriate books and records for each customer to track and record ownership of client digital assets, including the amount and the kind of assets owed to the client as well as the movement of the assets to and from the client's account. Regular and frequent reconciliation of client digital assets should be conducted on a client-by-client basis, taking into account both relevant off-chain and on-chain records. Any discrepancies noted should be addressed and escalated to senior management as appropriate in a timely manner.

22. An AI should have systems and controls in place to keep and safeguard all records relevant to the custodial activities, which shall be provided to the HKMA in a timely manner upon request.

(G) Anti-money laundering and counter-financing of terrorism

23. An AI should ensure that its anti-money laundering and counter-financing of terrorism (AML/CFT) policies, procedures and controls can effectively manage and mitigate any money laundering and terrorist financing risks relating to its custodial activities of digital assets. The AI should comply with the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) and any AML/CFT guidance issued by the HKMA on custodial activities of digital assets.

(H) Ongoing monitoring

24. An AI should regularly review its policies and procedures and conduct independent audit on its systems and controls and its compliance with the applicable requirements in respect of custody of client digital assets.