BERMUDA MONETARY AUTHORITY

DIGITAL ASSET BUSINESS CUSTODY CODE OF PRACTICE

FEBRUARY 2024

Table of Contents

I. INTRODUCTION

Safeguarding client assets by preventing fraud or misappropriation is a primary concern of the Bermuda Monetary Authority (Authority or BMA). Section 18 (1) of the Digital Asset Business Act 2018 (Act) prescribes requirements relating to safeguarding client assets while the Digital Asset Business Code of Practice (which applies to all Digital Asset Businesses (DAB)) further prescribes that a DAB must:

> "*…ensure that any assets belonging to clients are kept segregated from the DAB's own assets. To ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft.*"

Section 18 of the Act further requires that the DAB, "*…maintain in its custody a sufficient amount of each type of digital asset in order to meet its obligations to clients.*" Therefore, custodians of digital assets are not allowed to rehypothecate, transfer (except to another qualified custodian, where appropriate) or otherwise sell digital assets held for the benefit of their customers.

The purpose of this Digital Asset Business Custody Code of Practice (Code) is to provide more clarity to the digital asset industry as to what standards the Authority expects when considering whether a custodian is employing an acceptable level of care when safeguarding its clients' digital assets. The present Code should be read in conjunction with the DAB Operational Cyber Risk Management Code of Practice.

For the purpose of this Code, custodian is defined as any DAB that has sole or partial control over digital asset keys on behalf of clients. Where a DAB outsources custody of client digital assets to a qualified custodian, the DAB must satisfy itself that the qualified custodian maintains comparable standards to those outlined in the Code.

For the specific purpose of reading this Code, DABs should have regard to the following:

1. **Must** - Denotes that the standard is mandatory; the DAB must implement either what is prescribed in the Code, or a comparable or higher standard that registrants can demonstrate yields similar protection levels (concerning its business model);
2. **Should** - While not mandatory, denotes a strong recommendation from the Authority; a registrant may depart from it where it has documented a valid reason;
3. **May** - Denotes that the standard is optional; and
4. **Best practice** - Includes recognised standards such as those adopted by the National Institute of Standards and Technology or the International Organisation for Standardization.

The DAB must regularly assess the custody risks arising from its business model and implement higher standards than outlined in the Code where best practice warrants.

Instances where higher standards may be warranted, include when a DAB has a unique business model with extraordinary risk, or there are generally accepted knowledge breakthroughs in cybersecurity risk management and mitigation strategy, etc. The DAB's risk assessments must be documented and retained for at least five years in a manner that allows the risk assessments to be provided to the Authority upon request.

1.2 Status of the Code

The Code is made pursuant to section 6 of the Act. Section 6 requires the Authority to publish, in such a manner as it sees fit, a Code that provides guidance on the duties, requirements, procedures, standards and sound principles to be observed by persons carrying on digital asset business. Failure to comply with provisions set out in the Code will be taken into account by the Authority in determining whether a licensed DAB is meeting its obligation to conduct its business in a sound and prudent manner in accordance with the Act.

1.3 Proportionality Principle

The Authority appreciates that DABs have varying risk profiles arising from the nature, scale and complexity as well as the inherent risk profile of the business and that those DABs with higher risk profiles would require more comprehensive governance and risk management frameworks to conduct business in a sound and prudent manner.

Accordingly, the Authority will assess the DAB's compliance with the Code in a proportionate manner relative to its inherent risk (i.e., nature, scale, complexity and risk profile). These elements will be considered collectively rather than individually (e.g., a DAB could be relatively small in scale but carry out extremely complex business and, therefore, would still be required to maintain a sophisticated risk management framework). In defining these elements:

1. ***Nature:*** Includes the relationship between clients and the DAB or characteristics of the service provided (e.g., a DAB that maintains custody of clients' assets versus one that outsources the custody. To provide another example, an open blockchain infrastructure and a private blockchain infrastructure are different in nature, with different inherent risks;
2. ***Scale*****:** Includes size aspects such as volume of the business conducted or the size of the balance sheet in conjunction with materiality considerations (e.g., an assessment of the impact of a DAB's failure); and
3. ***Complexity*****:** Includes items such as organisational structures and product design.

In assessing the existence of sound and prudent business conduct, the Authority will have regard for both its prudential objectives and the appropriateness of each Code provision for the DAB, taking into account that DAB's nature, scale, complexity and risk profile.

The proportionality principle discussed above applies to all sections of the Code regardless of whether the principle is explicitly mentioned.

1.4 Purpose and Scope

Due to the unique nature of their composition, digital assets require specificity in dictating safekeeping and transaction handling custody procedures. Unlike traditional assets, where the physical asset itself, or a proxy of the asset, is held in custody, digital assets are held in digital form. By definition, digital assets mean "anything that exists in binary format and comes with the right to use it and includes a digital representation of value," which can exist on a public or private distributed ledger.

In the case of a public ledger, because the information is public and distributed, transaction reversals are not normally possible (or are difficult to reverse). This makes the practice of secure transaction handling and verification of paramount importance to proper digital asset custody standards.

The Code defines a standard for operating as a custodian of digital assets and is to be adhered to by every DAB that maintains or is responsible for the custody of its client(s)' private keys. This Code is split into the following four sections:

- Business control requirements
- Technology controls - custody safekeeping
- Technology controls - custody transaction handling and operations
- Technology controls - audit

II. BUSINESS CONTROL REQUIREMENTS

A DAB must not underestimate the importance of sound business controls. There are a number of facets to business controls relating to staffing, outsourcing partners, access controls, operational risk management and business continuity. The business control standards are as follows:

2.1 Liquidity

The DAB must have documented mechanisms in place to assess its liquidity needs, including sums required for trading and other client transaction types.

2.2 Hot and Cold Storage

A risk assessment must be completed for cold storage (offline) and hot storage (online). Factors for determining the best method of storage include, but may not be limited to, nature of the assets, the volume of transactions and speed at which transactions need to be completed, the ability to reverse transactions, and the risk tolerance of the DAB's clients.

2.3 Fraud Detection and Compliance Standards

DABs must develop a protocol for fraud detection and adherence to internal compliance requirements. This should include a detection system for identifying suspicious transactions as well as a procedure for reviewing suspicious transactions.

2.4 Personnel Dedicated Roles and Responsibilities

DABs must have established roles and responsibilities for custody operations and custody operational risk management that are formally documented and formally approved by the senior management team.

2.5 Insurability and Other Protections

DABs must demonstrate that assets under custody carry appropriate insurance or other financial protections to cover or mitigate potential loss exposure.

2.6 Proof of Reserves (POR)

Section 18(3) of the Act requires that, "A ... [DAB] that has custody of one or more digital assets for one or more clients must maintain in its custody a sufficient amount of each type of digital asset in order to meet its obligations to clients." To fulfil this requirement, a DAB must maintain adequate accounting and other relevant records and adequate systems and controls to accurately track ownership and quantity of client digital assets it has taken into custody.

The DAB must have adequate segregation of duties to protect the integrity of the record-keeping process and appropriate redundancy and business continuity processes, procedures and controls to be able to access records of client digital assets in custody at all times, including post-natural and other disasters.

2.7 Collusion Mitigation

DABs must demonstrate a method for controlling the signing process that prevents a quorum of individuals from acting in bad faith and/or collusion. Collusion mitigation may be accomplished in any of the following ways including but not limited to:

1. Controls including oversight or separation of duties that prevent a linear ability to create, approve,

sign transactions and broadcast to distributed ledger networks;
2. Distribution of signatories with differing incentives (e.g., client, custodian, third parties);
3. Unknown identities of signatories among each other; and
4. Rotation of signatories, signing times or signing locations.

The risk of collusion and other malicious acts must be addressed as part of recurring operational risk assessments.

III. TECHNOLOGY CONTROLS PART I: CUSTODY SAFEKEEPING

One of the most important responsibilities of the DAB is the safekeeping of digital assets in its custody. Controls must be in place to ensure digital assets are securely created and stored. Additionally, uninterrupted availability of assets is another important requirement.

3.1 Seed generation

The secure creation of cryptographic keys and seeds requires two things to be secure: confidentiality and un-guessable numbers. Confidentiality is required to ensure that the newly created keys or seeds are not read/copied by an unintended party. Un-guessable numbers are required to ensure the newly created key cannot be guessed or determined by an unintended party.

The seed should be created using a compliant deterministic random bit generator. DABs must create safeguards in the seed and subsequent key generation process that demonstrates resistance to supposition and potential bad actor collusion (note that secure non-deterministic key generation mechanisms may also be used).

The seed must have, as a minimum, random sequence 256-bit entropy. The result must be at least a 256-bit entropy input that is encoded into a mnemonic 24-word phrase, as a minimum. DABs must then utilise a hashing function to generate a 512-bit value minimally (note that the 24-word phrase is considered the backup seed because it can be utilised to regenerate a seed).

DABs must, at a minimum, utilise three individuals to perform the process of creating entropy in the creation and production of the seed, with no single person ever possessing the entirety of the seed or backup mnemonic word phrase. When a single seed is produced for a signatory, the signatory must not be involved in the production of the public and private keys.

None of the seed creators are permitted to participate in the act of cryptographically signing or having access to the systems that facilitate transactions.

3.2 Key Pair Generation

DABs must demonstrate adherence to an industry-standard method of key generation. Key generation must be performed in a manner in which a revoked signatory does not have access to the backup seed or knowledge of the phrase used in its creation. All keys must be encrypted in a manner preventing a compromised signatory from recovering the seed.

3.3 Data Sanitisation Post Seed and Key Generation

Secure deletion and destruction mechanisms must be in place to prevent unwanted artefacts from seed, key and wallet generation.

3.4 Seed and Key management procedure

A procedure must be formally documented detailing security, redundancy, backup, availability and logical access controls. This must include as a minimum:

1. Strong encryption and secure device storage are in place for client private keys that are not in use (i.e., client private keys stored in cold wallets);

2. DABs must, at all times, maintain logical access controls rendering it impossible to achieve a quorum of transaction signatures from keys stored in a single location;

3. DABs must demonstrate that once the mnemonic backup seed phrase has been generated, it is broken into at least two or more parts. DABs must demonstrate that under no circumstances will a sufficient number of backup seed phrases that could be used to facilitate a transaction be stored in any single facility;

4. Key and seed back-ups must be stored separately from the primary key and seed. Key and seed back-ups must be stored with strong encryption equal to or better than that used to protect the primary key. The seed and key backup must be protected by access controls to prevent unauthorised access; and

5. For the storage of critical seeds, keys and key parts, Hardware Security Modules (HSM) that are Federal Information Processing Standard 140-2 certified are recommended as the most secure key storage mechanism. Note that HSMs can be physical or virtual devices.

3.5 Key Access and Compromise Procedure

A formal documented procedure must be in place outlining the process to follow where a member of staff has had any access to keys or seeds. An audit trail must record every change of access including who performed the change.

A DAB must document a key compromise procedure. An event triggering the procedure must include, but not be limited to, the compromise of the whole seed, a partial seed or a key derived from a seed. In such a situation, if the underlying seed is believed to be compromised, the DAB's response procedure must include the mechanism for new wallet creation and asset migration. If it is determined by the DAB that a key is compromised, a risk event must be documented and investigated.

3.6 Key Revocation Procedure

DABs must promulgate procedures for immediately revoking a signatory's access. Procedures must follow the standard protocol around removing user access without the need to create a new wallet. Internal audits to recertify access should be performed at least quarterly.

DABs must have a written procedure document that is followed for on/off-boarding. The procedure must outline every permission to grant/revoke for every role in the information system. In addition, all grant/revoke requests must be made via an authenticated communication channel (transmitted using an encrypted protocol).

3.7 Perpetual Access

A DAB must demonstrate that it can provide clients with perpetual access to all assets in custody in the event a DAB ceases to operate or cannot fulfil its custody agreement. Any exceptions to this must be clearly defined as a service level agreement and communicated to the customer. This may include a formal

disbursement or custody transfer process.

3.8 Account Segregation

While keeping client assets separate from their own, DABs may commingle client assets in order to benefit clients; however, proper accounting must be in place to accurately allocate each holding to the respective client. Where the DAB commingles client assets, it must document and implement measures to demonstrate that the level of security achieved is commensurate with an arrangement where every client has a one-to-one relationship with a given address.

3.9 Physical Security and Access Standards for On-Site Cold Storage

For on-site cold storage, a risk assessment must assess what assets are stored at each storage facility and what associated physical controls are required. DABs must demonstrate that all storage facilities are equipped to an appropriate industry standard.

IV. TECHNOLOGY CONTROLS PART II: CUSTODY TRANSACTION HANDLING

A DAB must ensure that transactions are subject to controls to ensure they are secure and trusted and that measures are in place to prevent fraud. Transactions must be recorded in system audit records. These records must then be subject to periodic audits.

4.1 Multi-Signature Authorisation

A documented procedure must be in place detailing the use of multiple signature authorisation. DABs should use an M-of-N multi-signature standard with a minimum of three signatories required for a quorum signature standard for all transaction types. Where this is not possible, an appropriate mitigating authorisation control that uses the principle of multiple signatures must be used. Multi-signature authorisations must be audited on an annual basis.

4.2 Transaction Authorisation Requirements

A risk assessment of transaction types must be completed. This assessment must define appropriate transaction authorisation control requirements. Based on the assessment outcome, appropriate controls must be put in place. Decision approval evidence, including chain of custody, must be retained for review for five years.

4.3 Periodic Transactions Audit

Each quarter DABs must draw a sample of transactions to be audited internally to ensure that internal processes are functioning as intended. DABs must take remediation action as needed in the event faults are discovered. Integrity controls must be in place to ensure that records and audit trails cannot be changed.

1. ***Contractual Nature of Evidence:*** The evidence required for each signatory to prove true in order to authorise a transaction must be contractually agreed upon by all signatories. In the event approval signing and transaction (Tx) signing are abstracted, Tx approvers must have access and appropriate expertise to evaluate required evidence prior to an authorised signing ceremony.
2. ***Proof of Evidence:*** Each approver or signatory is required to provide proof of the evidence referenced for an authorisation.
3. ***Proof of Elapsed Time:*** Each transaction and signature action associated with a transaction must have a specific time duration tracked against each option for any transaction where the conditions of the evidence are time-based.

4. ***Auditability:*** DABs must store all evidence internally and must have it reviewed at multiple-levels within a transaction. A minimum of two separate individuals must perform reviews around a specific request. Evidence is collected based on a set checklist of necessary documentation based on the role the signatory is representing. DABs must establish controls around the processes, which must be evaluated on a periodic basis and adjusted if necessary.
5. ***Books and records:*** DABs must maintain a full audit trail of all user/admin actions. This includes specific information about each transaction, including but not limited to:
    - Date and time of the transaction
    - Transaction event type
    - Jurisdiction of the client and relevant signatories
    - Account balances and the value of the transaction

This audit log must be stored so that it is available for review by the Authority for at least five years.

V. TECHNOLOGY CONTROLS PART III: AUDIT

An annual IT audit plan must be developed and approved by the audit committee of the board or its equivalent. Audits may be carried out by a qualified internal audit resource or by qualified third parties.

5.1 Recurring Audit Requirements for Digital Assets

The following procedures must be subject to an audit every six months as a minimum frequency. Evidence of the audits must be documented and made available to the BMA upon request.

The bulleted list below details audit requirements that are referenced throughout this document and must be audited every six months as a minimum frequency:

- Key and seed generation and management processes
- Key revocation procedure - (ref 3.6)
- Multi-signature authorisations - (ref 4.1)
- Transaction system audit logs consisting of: - (ref 4.3)
    - Contractual nature of evidence - quarterly audits
    - Proof of evidence - quarterly audits
    - Proof of elapsed time - quarterly audits
    - Completed transaction audit to ensure compliance of proof of evidence protocols
- Suspicious transaction handling
- Migration of storage devices (cold to hot storage)
- Proof of solvency random address

All audit records must be retained for at least five years in a manner that can be made available to the Authority upon request.

VI. GLOSSARY:

For the purpose of the Code, the following terms and definitions shall apply:

Address: A cryptocurrency address is (usually) an encoded form of a public key from a wallet that can be used as the recipient of a transaction. In multi-signature schemes, an address may be an encoding of information, including several public keys and other information like a bitcoin Pay to Script Hash (P2SH) address.

Cold storage: A method of storing information that is not connected to the internet.

Custodian: A financial institution, including a DAB, charged with the custody of digital asset keys on behalf of clients. The custodian may have sole or partial control over the digital asset keys.

Custody: The protective care or guardianship of digital assets that are held or being transacted.

Entropy: Randomness or unpredictability within source code applied during generation of a cryptographic seed to ensure a seed cannot easily be recreated.

Evidence: The available body of facts or information indicating whether a belief or proposition is true or valid.

Multi-signature: An M-of-N method of transacting. This refers to needing a minimum number of signatures (M) out of the total available signatures on a wallet (N).

Safekeeping: The contractual responsibility of securing and preserving digital assets held in custody by a custodian.

Seed: A slice of entropy typically used to initialise a random number generator, pseudorandom number generator/deterministic random bit generator (PRNG/DRBG) or other crypto-system (e.g., hierarchical deterministic wallets, deterministic signatures).

Signatory: An individual tasked with providing one of the signatures in an M-of-N multi-signature scenario.

Signature: A cryptographic authorisation applied by a designated signatory in a transaction.

Transaction: An exchange or interaction specific to the digital assets in custody.

Transaction type: Classification of a transaction purpose and distinguishable by its purpose (e.g., “withdraw” versus “deposit” versus “fee”).