BERMUDA MONETARY AUTHORITY

Digital Asset Custody Code of Practice

December 2018

1 Contents

Introduction

The safeguarding of client assets by preventing fraud or misappropriation is a primary concern of the Bermuda Monetary Authority (the Authority). Section 18 (1) of the Digital Asset Business Act 2018 (the Act) prescribes requirements relating to safeguarding client assets. Further, the Digital Asset Business Code of Practice 2018 further prescribes that a Digital Asset Business (DAB) must;

"*…ensure that any assets belonging to clients are kept segregated from the DAB's own assets. The DAB may place client assets in a trust with a qualified custodian, or have a surety bond or indemnity insurance, or implement other arrangements to ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft.*"

The growing public involvement with digital assets presents legal and operational challenges for investors, entrepreneurs and service providers, as well as the regulators who oversee them. A primary challenge is how to legally and effectively safeguard this new class of assets.

The purpose of this Digital Asset Custody Code of Practice (the Code) is to provide more clarity to the digital asset industry as to what standards the Authority will expect when considering whether a custodian is employing an acceptable level of care when safeguarding its client's digital assets.

1.1 Interpretation

A DAB should have regard to the following in interpreting the Code and how the Authority is likely to interpret a DAB's compliance with the Minimum Criteria for licensing in the Act:

- "shall" or "must" denotes that the standard is mandatory. The DAB must implement either what is prescribed in the Code, or a comparable standard that the DAB can demonstrate yields similar protection levels (having regard for its business model);
- "should," while not mandatory, denotes a strong recommendation from the Authority. A DAB may depart from it where it has documented an acceptable reason;
- "may" denotes options;
- "best practice" includes recognised standards such as those adopted by the National Institute of Standards and Technology (NIST), International Organisation for Standardization (ISO), or the Cryptocurrency Security Standard where appropriate.

However, while having regard for the interpretation of "must" and "shall" above, the DAB must be aware of the reasonably foreseeable material asset custody risks arising from its operations and wider environmental context. Ensuring that this is the case, 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. The DAB's risk assessments must be documented and retained for at least five years in a manner that allows the reports 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 manner as it thinks 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 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 nature, scale, and complexity. 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:

- *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, etc.);
- *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
- *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, and complexity.

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

1.4 Purpose, and Scope

Because of 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 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. DABs are required to adhere to the industry best practices in Custody Safekeeping, Custody Transaction Handling and Custody Operations. As practices continue to evolve and subject matter expertise emerges within the industry, consortium-recommended best practices should be considered as guidelines for specific core functions of custody. This Code addresses the three main areas of custody governance: *Custody Safekeeping*, *Custody Transaction Handling, and Custody Operations*:

Custody Safekeeping standards dictate how seeds and keys are generated and secured and how addresses and wallets are managed within the context of digital asset custody. This includes recovery protocols for compromised or corrupted seeds and keys in addition to fraud prevention measures.
Custody Transaction Handling standards dictate specific protocols for facilitating inbound and outbound transactions of an asset in custody to ensure proper due diligence is performed before transactions are authorised.
Custody Operations standards dictate operational policies and procedures, reporting and operational risk management specific to digital asset custody, as well as, traditional practices of operational risk management and fraud prevention practiced in the financial services industry.

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, inter alia, staffing, outsource partners, access controls, operational risk management, and business continuity. The business control standards are as follows:

1.5 Hot/Cold Storage & Liquidity

The DAB must have documented mechanisms in place to assess its liquidity needs, including sums required for trading and other client transaction types. These mechanisms must be used to inform the DAB's client private key storage policy. The client private key storage policy should require that the majority of client private keys, not required for client transactions, should be held in cold storage to mitigate against client loss arising from cyber-attacks. The Authority also expects that only a minimal balance should be kept in hot storage and that the mechanism and thresholds for transfer between hot, cold and other storages should be well documented and audited.

In addition to the liquidity needs, when arriving at the minimum cold storage balance as part of the client private key storage policy, the DAB must also have regard for its ability to obtain insurance or other forms of mitigation, ensuring that its assessment is holistic. Regardless of the assessment results, in no case shall the DAB hold less than ninety percent (90%) of client private keys not being used for trading or other transactions in cold storage.

1.6 One Time Use Address

The practice of generating a new address for every transaction further ensures a client's privacy and confidentiality. However, there are potential business cases where traceability of address activity is desirable. Therefore, a custodian must exercise judgment in determining an address strategy based on the use case of its clients and must be able to provide justification for the address use strategy.

1.7 Asset Agnostic Support

Each digital asset type may have a different protocol for its wallet functionality. Regardless of these protocol differences, a DAB must demonstrate its ability to manage the same level of compliance related to Safekeeping, Recording and Transaction Handling. A DAB must demonstrate compliance with the custodian standards outlined in the Code for every asset type in its custody.

1.8 Fraud Detection and Compliance Standards

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

1.9 Proof of Asset Valuation

A DAB is required to disclose the methodology related to its asset valuation calculations and, when possible, use recognised benchmarks or observable, bona-fide, arms lengths market transactions.

A DAB should pay extra care where the current market value of an asset is a conditional element of the transaction being executed. A DAB shall ensure adherence to its client agreement and industry best practices. A DAB should also disclose the source of the asset valuation to the client and all signatories of the transaction.

1.10 Personnel Dedicated Roles and Responsibilities

DABs shall have established roles and responsibilities for Custody Operations and Custody Operational Risk Management. Responsibility for manually executed (non-automated) core functions of custody should be performed by employees who have been subject to appropriate background screenings.

1.11 Personnel Identity Verification and Background Screening

All personnel tasked with custody core function responsibilities are required to have undergone sufficient background checks in accordance with industry best practices for background screenings. Scrutiny must be given to any personnel found to be the subject of the following red flags: felonies, serious misdemeanors, and financial distress. The nature of background checks should be fortified further by separation of duties to ensure no single person may execute approval, signing, and broadcast of egress transactions.

1.12 IT Security Awareness Training must be completed Annually for All Staff

Training must include regular sensitivity awareness training around phishing and other malicious techniques used to gain unauthorised access to systems and premises via employee actions. Two training programs may be produced, one for IT staff and one for non-IT staff.

1.13 Sufficiently Skilled Resources

The Digital Asset Code of Practice requires under the section on adequate personnel that a DAB must have available suitable numbers of staff who are appropriately trained and competent to discharge their duties effectively. The DAB should ensure that the responsibilities and authority of each staff member are clear and appropriate given his/her qualifications and experience, and that staff receive the necessary training appropriate for their respective roles.

1.14 Annual Review of Training Programs

A DAB must review and document the adequacy of its training programmes at least annually, along with any relevant elements after the crystallisation, or near crystallisation, of material risk incidents. Policies and procedures must also provide for appropriate disciplinary measures for employees who violate policies and procedures.

1.15 Outsourcing and Partner Integrations

For any outsourced services or integrated partnerships, DABs shall demonstrate that proper due diligence was done in vetting the partner (affiliate, vendor or supplier) as it relates to information security, operational

risk, and financial solvency. Although services may be outsourced, responsibility for compliance with the Code remains with the DAB. The DAB must also have sufficient governance mechanisms in place to monitor the outsourced party's continued compliance with the Code.

The DAB must regularly assess the risk of IT systems or software integrations with external parties or affiliates, particularly as they relate to the risk of unauthorised access and theft of client assets in custody, and ensure that appropriate controls are implemented to mitigate the risk. These risk assessments must be documented and retained for at least five-years in a manner that allows the reports to be provided to the Authority upon request.

1.16 Supply Chain Management

For any third-party supplier of equipment that enable custody core functions (e.g. steel storage, cold storage wallets, etc.), there must be a demonstrated redundancy strategy for alternative suppliers that allows the DAB to maintain service level agreements.

1.17 Insurability and Other Protections

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

1.18 Service Level Agreements

Customer Service Level Agreements must be prominently and clearly communicated to clients. A reasonable time frame for completing transactions must be demonstrated consistently over time as defined by industry best practices. DABs must demonstrate competence in meeting Service Level Agreements in relation to fund access upon deposit and withdrawal requests.

1.19 Customer Identity Verification and Due Diligence

DABs must have documented policies and procedures related to client identity verification requirements for both jurisdiction and asset type. A DAB must comply with client identity verification requirements in the jurisdictions in which it operates. This must include, but is not limited to:

- Enhanced due diligence to confirm a client's identity;
- Enhanced Know Your Customer (KYC) screenings;
- Sanctions screenings; and
- Adverse media screenings.

A DAB shall demonstrate its protocols for compliance with client identity verification. This includes its practice of the new client identity verification process as well as any required ongoing screenings and transaction-specific screenings when appropriate.

1.20 Disclosures & Reporting Standards

A DAB should implement industry best standards of disclosure and operational transparency. At a minimum, there must be adherence to legally required disclosures in the jurisdictions in which it operates. Statements are to be designed to assure the integrity of the client accounts and permit clients to identify any erroneous or unauthorised transactions, withdrawals or balances.

a. *Customer Statements:* Statements must be available at least quarterly to clients upon request and must include:
   - Timeframe of statement activity;
   - All transactions specific to a client's account with dates and transaction amounts of corresponding transactions;
   - Distinct balances; and
   - Valuation of assets if required for each digital asset type.

b. *Corporate Actions:* Any action taken by a DAB that impacts existing agreements with clients related to the custody of their assets must be disclosed to the client.
c. *Service Level Agreements:* A service level agreement for custody services must be made available to clients.
d. *Digital Asset Specific Disclosures:* DABs must clearly disclose intent and obligations pertaining to airdrops, forks, metacoins, coloured coins, side chains, dividends, splits or other digital asset derivatives. DABs must also clearly disclose responsibilities for ascertaining or taking action with respect to calls, conversions, votes, exchanges, maturities, tenders, or other matters relating to assets.
e. *Changes to Account Information:* A DAB should notify clients of any changes that are made to the client's account information.

1.21 Proof of Reserves (POR)

A DAB should have a minimum amount of assets on-hand, within the organisation, to withstand the withdrawal of all client assets. This ensures sufficient liquidity for the protection of client assets. A periodic POR audit must be completed.

1.22 Operational Risk Management (ORM): ORM Programme Requirements

DABs shall have clearly documented and audited ORM programme. A DAB must have a formally established ORM programme with identified responsibilities assigned to an ORM function.

The ORM function is responsible for: 1) developing strategies to identify, assess, monitor and control/mitigate operational risk; 2) defining policies and procedures concerning operational risk management and controls; 3) defining operational risk assessment methodology; 4) and for managing a risk-reporting system for operational risk.

1.23 Operational Risk Incident Reporting

A risk incident is defined as any interruption to an executed operational procedure. The cause may be known or unknown. In the event of a risk incident, a report must be generated documenting the following:

- known cause of the incident;
- impact of the incident;
- incident resolution;
- the timeline of the incident, including duration of time to resolve the incident.

This report shall be disclosed to both senior leadership and the Board of Directors, and referenced for future revisions to the ORM documented policies and procedures.

In the event the risk incident results in revisions or additions to standard policies and procedures, the operational risk function shall establish a timeline for complying with the necessary changes and must document the compliance of meeting the goal in a timely manner.

1.24 ORM Documentation:

Policies and procedures related to operational risk must be well documented, in use and known to all affected parties. Documentation must be revisited periodically to ensure its relevance.

1.25 Proactive Scenario Planning

ORM policies and procedures must be revisited on a recurring basis to ensure all reasonably foreseeable scenarios have been considered. It must be demonstrated that the scope of scenario planning has taken into consideration current industry risks and practices and reflects possible high-severity and plausible risks.

1.26 Business Continuity - Personnel Redundancy

For all critical custody functions, DABs shall have a demonstrated personnel redundancy plan in place in the event that the primary individual assigned to a particular function is unavailable.

1.27 Business Continuity - Alternate Site Plan

DABs shall maintain at least one alternate site location sufficient to recover and continue operations for an indefinite period of time. A DAB should be able to demonstrate that the alternate site has appropriate distance between it and the primary custody location to mitigate environmental and technical interruptions at both sites and adheres to all of the aforementioned criteria.

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. Uninterrupted availability of assets is another important requirement. The technology custody safekeeping control standards are as follows:

1.28 Seed Generation

The Seed should be created using a NIST (https://csrc.nist.gov/publications/detail/sp/800-90b/final) compliant deterministic random bit generator. DABs shall create safeguards in the seed and subsequent key generation process that demonstrated 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, at a minimum. DABs shall then utilise a hashing function to generate a 512-bit value minimally. It is recommended that an optional passphrase be generated as part of the seed which can be used as an additional measure of security and leveraged as a defence in brute force attacks. Note that the 24-word phrase is considered the backup seed because it can be utilised to regenerate a seed.

DABs shall, 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 nor have access to the systems that facilitate transactions.

1.29 Key Pair Generation

DABs shall demonstrate an adherence to an industry standard method of generating asymmetric private and public key combinations, such as NIST.

1.30 Data Sanitisation Post Seed and Key Generation

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

1.31 Storage of Seeds and Keys

DABs shall demonstrate that industry best practices utilising 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 wallets.

DABs shall ensure that fewer than the number of keys required to transact will ever be stored online or in any one physical location. DABs shall, at all times, maintain systems rendering it impossible to achieve a quorum of transaction signatures from keys stored in a single location. Key/seed backups must be stored in a separate location from primary key/seed.

Key/seed backups must be stored with strong encryption equal to/better than that used to protect the primary key. The seed/key backup must be protected by access controls to prevent unauthorised access.

For the storage of critical seeds, keys and key parts relating to the internal DAB core cryptographic systems, Hardware Security Modules (HSMs) that are FIPS 140-2 certified are recommended as the most secure key storage mechanism.

1.32 Back-up of Mnemonic Seed Phrase

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

1.33 Physical Security Requirements of Storage Facilities

DABs shall demonstrate that all storage facilities are equipped with vaults meeting at least a Class 1 UL rating of penetrative resistance to forcible attack. DABs shall ensure that all physical storage areas in use are monitored on a 24/7 basis and shall include reinforced concrete and steel vaults equipped with alarms, locks, and other appropriate security devices and be resistant to fire, flood, heat, earthquakes, tornadoes, or other disastrous conditions.

Access to the storage shall be limited to persons authorised by the associated entity and confirmed by the third party through multifactor identity verification and audit consistent with industry best practices.

1.34 Audit of Backup Seeds

DABs shall ensure that a regular and recurring internal audit of the backup seeds is performed on the storage devices to ensure that no backups were tampered with or removed; said audit shall occur no less than quarterly. All audits of seeds and subsequent results are to be well documented, with any risk incidents noted and necessary action taken. All audit records shall be retained for at least five years in a manner that can be made available to the Authority upon request.

1.35 Key Compromise Procedure

A DAB shall develop a documented protocol in the event there is reasonable belief that a wallet, private key or seed has been compromised. An event triggering said protocol shall include, but not be limited to, the compromise of the whole seed, 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 shall 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 should be documented and investigated (See Risk Incident Reporting).

1.36 Personnel Departures

Strict access management controls must be in place to manage access to keys. Upon departure of a signatory that had access to a wallet key or M-of-N wallet keys, a formal assessment must be conducted to determine whether a new key ceremony and accompanying migration of digital assets is required. An audit trail must record every change of access including who performed the change.

1.37 Key Revocation Procedure

DABs shall promulgate procedures for immediately revoking a signatory's access. 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 the creation. All keys must be encrypted in a manner preventing a compromised signatory from recovering the seed. Procedures shall follow the standard protocol around removing user access, without the need to create a new wallet. Periodic internal audits shall be performed on removal of user access by reviewing user access logs and verifying access as appropriate.

DABs must have a written checklist/procedure document that is followed for on/off-boarding. The checklist must outline every permission to grant/revoke for every role in the information system. All grant/revoke requests must be made via an Authenticated Communication Channel (transmitted using an encrypted protocol).

1.38 Perpetual Access

A DAB shall demonstrate that it can provide clients with perpetual access to all assets in custody in the event a DAB ceases to operate and/or cannot fulfill its custody agreement. This can or may include a formal disbursement or custody transfer process.

1.39 Account Segregation

While keeping client assets separate from its own, DABs may commingle client assets where such would 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.

1.40 Location Redundancy

DABs shall maintain disaster recovery and locational redundancy facilities designed to ensure business continuity and client asset preservation. Said facilities, shall meet high security installation and geographic segregation standards matching that of the primary facility and in accordance with best practice.

1.41 Physical Security and Access Standards

For on-site cold storage, a DAB shall have physical security that includes, at a minimum:

- Required badge entry that is restricted to authorised individuals, at least two of a multi-factor authentication method of something you know (login credentials), something you have (hardware or software token/access card), and something you are (biometrics) plus a safe which requires at least two authorised key holders;

- Separate segmented access controls from primary workspaces;
- Facility access control logging system which maintains access records for a minimum of one year on-site and a copy stored for three years at an off-site location;
- CCTV must cover access entry to clearly show individuals' access in/out of the safe;
- CCTV data must be kept for a minimum of one year on site and a copy stored for three years at an off-site location;
- Principles of least privilege must be documented and applied when assigning access controls, with said documentation available upon request for review by the Authority upon request.

1.42 Mandatory Reporting of Security Breaches

DABs must have documented policies and procedures to address actions taken, client notifications, and notifications to the Authority applicable to an event or suspicion of hack, theft, compromise or attack, i.e. any situation whereby a Digital Asset being kept in custody has been compromised (or cyber reporting event as defined in the Act.). Such procedures must be reviewed and audited annually and include velocity limit, freeze and/or circuit breaker actions designed to protect funds in an emergency.

As referenced in the Act, "a senior representative **shall forthwith notify** the Authority [of a Cyber Reporting Event], in such manner as … [the Authority] may direct, on its coming to … [a senior representative's] knowledge, or his having reason to believe, that an event … has occurred". As a guide, 'forthwith' shall be understood to mean that the event shall be reported within the hour of the suspicion or confirmation of an event.

"Cyber reporting event" means any act that results in unauthorised access to, disruption, or misuse of the electronic systems or information stored on such systems of a licensed undertaking including any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to such systems or information. The notification must provide the following information:

- What happened; the categories and approximate number of digital assets concerned
- When it happened
- How it happened
- Description of the likely consequences of the breach and any mitigating actions taken
- Impact to clients and any communications sent or planned

Within 14 days of such notification, the senior representative shall furnish the Authority with a report in writing setting out all of the particulars of the case that are available to him/her. The incident report must contain root-cause analysis and impact analysis. The DAB must ensure that the senior representative has sufficient resources and information to comply with his reporting requirements.

1.43 Hot/Cold Storage - Rationale for Storage Solution:

A DAB must provide rationale for its choice of storage solutions. The decision to use cold storage (offline) versus hot storage (online) must align with industry best practices for the asset in question. Factors for determining the best method of storage include, but may not be limited to, the volume of transactions and speed at which transactions need to be completed; and the risk tolerance of the DAB's clients.

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 audit. The custody transaction handling control standards is as follows:

1.44 Multi-Signature Authorisation

The benefits of a multi-signature process are well practiced and understood throughout the industry (to minimise risks of collusion). Through the implementation of a multi-signature approach, the risk of a single party initiating and completing a transaction is mitigated almost entirely. Best practice is for a DAB to implement an M-of-N multi-signature standard with a minimum of four (4) signatories required for a quorum signature standard for all transaction types.

DABs must ensure that all individuals with authorised access utilise individual named accounts to allow for auditing of access.

Where a DAB has various multi-signature procedures that vary depending on the risks of the transaction (value of transaction, type of wallet, risk level of client, etc), the procedures must be well documented and audited.

1.45 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:

- Controls including oversight and/or separation of duties that prevent a linear ability to create, approve, sign transactions, and broadcast to distributed ledger networks;
- Distribution of signatories with differing incentives (e.g. client, custodian, third parties, etc.);
- Unknown identities of signatories amongst each other;
- Rotation of signatories, signing times, or signing locations.

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

1.46 Evidence-based Signature Approvals

For each transaction, each signatory must demonstrate evidence which supports the decision to approve or reject a transaction. The evidence should be collected based on a set procedure and gathered with the same diligence and with the same required information each time. Documentation of decision approval must be retained and available for review upon request by the client, with a chain of custody evidencing every access.

1.47 Periodic Transactions Audit

Periodically, DABs shall draw a sample of transactions to be audited internally in order to ensure that internal processes are functioning as intended. DABs shall 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.

a. *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 Tx (transaction) signing are abstracted, Tx approvers must have access and appropriate expertise to evaluate required evidence prior to an authorised signing ceremony.

b. *Proof of Evidence:* Each Approver or signatory is required to provide proof of the evidence referenced for an authorisation.

c. *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.

d. *Auditability:* DABs shall store all evidence internally and shall have it reviewed at multiple-levels within a transaction. A minimum of four separate individuals shall 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 shall establish controls around the processes that shall be evaluated on a periodic basis and adjusted if necessary.

e. *Books and records:* DABs shall 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 transaction
- Transaction event type
- Jurisdiction of client and relevant signatories
- Account balances and the value of the transaction

1.48 Recorded Evidence & Audit Data Backups

DABs shall abide by a system whereby confirmation of evidence is recorded and stored in an auditable format. Backups of audit data are performed regularly.

1.49 Data Deletion/Sanitisation Policy (DSP)

A detailed policy covering data sanitisation requirements, procedures, and validation steps for every media type used by business. Staff are aware of how data remain on digital media after deletion, how to securely wipe data, and when secure wiping should be used.

Technology Controls Part III: Custody Operations Controls

A DAB must ensure that technology operations are subject to best practice IT operational controls to ensure a secure and stable custody operating environment is in place. These controls include testing, security breach response and the recovery of systems to meet business requirements, Disaster Recovery/business continuity. The custody operations controls are as follows:

1.50 Multi-factor Authentication

For any web-based services provided by a DAB where user authentication is required, industry best practices for multi-factor authentication must be implemented, to include at least two of four multi-factor authentication methods of something a client knows (login credentials), something a client has (hardware or software token), a characteristic or feature of the client (biometrics), and local of a client (geofencing).

1.51 IT Security Controls Applicable To All Systems

The DAB must ensure that best practice IT Security controls are in place to protect all systems. The principle of "defence in depth" must be followed. Particular rigour must be applied to ensure that all internet-facing systems are hardened and secure.

1.52 Logical Access Management

Access to systems and data shall only be granted to individuals with a demonstrated business need. Controls must be in place to ensure identification, authorisation and authentication of the individual.

A current list of access rights shall be maintained along with documented procedures for assigning and revoking access privileges. A log of all access changes shall be maintained to demonstrate proof of proper access rights management.

1.53 IT Security Testing Requirements

DABs must perform the following:

- IT Security testing of both infrastructure and applications;
- Penetration tests at least annually by an independent and qualified testing company (any new internet facing services or significant changes to existing services must be penetration tested and hardened before being presented to the internet as live services);
- Internal vulnerability scans at least quarterly;
- External vulnerability scans, i.e. of all external facing services at least monthly.

1.54 Application Development Life Cycle & Secure Development Practices

Decentralised applications (dApps) must be subject to a formal development life cycle, i.e. a software development life cycle (SDLC). This should formalise the following activities:

- Design, Build, Test, Deploy, Monitor;
- Secure application development in line with best practice standards for example the OWASP (Open Web Application Security Project) and the Decentralised Application Security Project (DASP).

1.55 Recurring Testing Requirements for Digital Assets

Procedures that support custody services must be tested on a regularly scheduled and recurring basis. Proof of tested procedures and corresponding results must be documented and made available to auditors upon request. A testing schedule should be defined relative to procedural risk and potentially high impact risk incidents (risks having potentially the largest possible fiscal impact). Recurring testing shall include:

- Wallet integrity audits
- Key and seed generation procedures
- Completed transaction audit to ensure compliance of proof of evidence protocols
- Suspicious transaction handling
- Migration of storage devices (cold to hot storage) and
- Proof of solvency random address audits

Testing shall include participation by both employees and external parties. External parties shall be viewed as critical in defining risks and test scenarios potentially overlooked by employees. Testing standards shall adhere to best industry practices.

1.56 Disaster Recovery

The IT operations function must review the business continuity requirements as outlined in the BCP document. IT operations must then ensure that the systems listed in the BCP plan can be recovered as per the business requirements. A Disaster Recovery document (DR) must be in place to document recovery procedures. An annual DR test must take place and the results written up in a DR test report.

1.57 External Audit

A DAB shall prove that it has been subject to third-party custody audits. Documentation regarding the scope of the audit, audit findings and resolution to any issues identified during the audit shall be maintained for a period of not less than five years.

1.58 Automation Scrutiny and Justification

A DAB may in its discretion employ risk mitigation tools designed to automate a core function. This includes, but is not limited to transaction signatures that have received and passed a demonstrated risk assessment performed by a qualified third party. Corresponding operational risk procedures shall be documented. Risk monitoring mechanisms shall be put in place to identify failures in automation when and if they occur.

Definitions:

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/or other information as in the case of a bitcoin 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 the digital assets of its clients.

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). A common form of this is to use a 2-of-3 approach, which means of 3 total available signatories; at least 2 are required to approve a transaction before broadcasting.

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.

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 PRNG/DRBG or other crypto-system (e.g. HD Wallets, deterministic signatures).

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).

Consultation on Digital Asset Custody Code of Practice 2018

This document outlines the Bermuda Monetary Authority's (the Authority's) proposed digital asset custody standards for licensed digital asset businesses that are responsible for the custody of client private keys.

The views of the digital asset business industry, and of other interested persons, on the proposals set out in this document are invited. Comments should be sent to the Authority, addressed to innovate@bma.bm no later than 18 January 2019.

Please find eight suggested questions below – for you to answer. Please also raise any other comments/feedback on this page.

1) *Section 1.5.* Is the threshold of 90% of digital assets to be held in cold storage at all times appropriate? Provide examples of business situations where it might be acceptable to be below this threshold.

2) *Section 1.8.* What are some of the best practices in terms of suspicious transaction identification and review?

3) *Section 1.9.* Asset valuation is a challenge for some of digital assets, should the Authority prescribe valuation methodologies before industry standards emerge? Is yes, indicate which make valuation methodologies would be appropriate.

4) *Section 1.17.* If available, give information about availability of risk mitigation measures and industry standards around capital level requirements.

5) *Section 1.20.* What additional information, if any, should be provided in the Customer Statement to ensure proper disclosure to customer and usability by third party service providers (e.g. auditors, other financial service providers, etc.)?

6) *Section 1.31.* Should the Authority prescribe specific security levels for HSM compliant with FIPS 140-2? Should the prescribed level be dependent on risk characteristics or risk measures?

7) *Section 1.35, 1.36, 1.37.* Are our requirements aligned with best practices in terms of access control and management of key revocation? Is there distinctions that should be made dependent on the access control architecture?

8) *Section 1.44.* The Authority understands that the balance between the number of private keys in existence and the number of private keys required to initiate a transaction is crucial. Should the Authority provide additional latitude and, if so, under which circumstances?