REGULATORY FRAMEWORK FOR THE

CUSTODIAN SERVICES (DIGITAL ASSET) LICENCE:

CONSULTATION PAPER[1]

05 November 2018

1 The views expressed and proposals contained in this document are not final and subject to changes following feedback received from the industry, stakeholders and the public.

Table of Contents

Introduction

Mauritius has, over the past three decades, been consolidating its good repute as an International Financial Centre with a diversified product portfolio.

With the transformative incidence of financial technology ("fintech") on the global financial services industry, one landmark development in the fintech landscape has been the emergence of Digital Assets[2] and their use as a medium of exchange for transactions over the internet. The recent years have also witnessed significant strides in evolution of the technologies underpinning these Digital Assets, including blockchain[3].

At present, "Initial Token Offering[4]" ("ITO"), the process whereby investors transfer funds, generally in the form of cryptocurrencies[5], to the ITO organiser, in return for blockchain-based tokens[6], in electronic/binary form, has significantly grown as an alternative means of raising capital[7] for project funding.

As a forward-looking regulator, the Financial Services Commission, Mauritius (the "FSC") has embarked on setting up an enabling framework for fintech. Following the issue of the FSC Guidance Note on the Recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors (the "Guidance Note") on 17 September 2018, the FSC is now establishing the regulatory framework in relation to the Custodian Services (Digital Asset) Licence which will enable its holder to provide safe-keeping services in relation to Digital Assets.

2 A Digital Asset is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status. Digital Asset is considered as encompassing a "Virtual Asset" as defined by the Financial Action Task Force (FATF) in the FATF Recommendations as updated in October 2018

3 This term refers to a decentralised digital ledger or database of transactions relating to digital assets which are recorded chronologically.

4 The terms ITO and Initial Coin Offerings, used indistinctively, refer to an offer by a company to the public or specific investors to purchase or otherwise acquire Digital Assets or tokens as a means of raising funds.

5 Cryptocurrencies, a category of digital assets, are a math-based, decentralised convertible virtual currency, protected by cryptography, a medium of exchange and/or a unit of account and/or a store of value and do not have legal tender status. The term "Cryptocurrency" is defined by the FATF in its publication entitled Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014

6 The FSC considers a "token", commonly referred to as a "coin", as an electronic/digital representation of access rights to a service or ownership rights of an asset.

7 ITOs have been considered as analogous to initial public offerings with tokens issued being comparable to traditional shares in a company.

Background and Context

Regulation 21 of the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 (the "CIS Regulations") requires every Collective Investment Scheme ("CIS") to appoint and have, at all times, a custodian. The function of the custodian will be to take the assets of the CIS into its custody for safe-keeping and to deal with those assets in accordance with the written agreement with the CIS.

With Digital Assets now being a recognised asset-class for investment by specific investors and CIS, the Digital Assets of a CIS must also be held for sake-keeping by a custodian.

The FSC however acknowledges that while fintech activities have been developing exponentially in complexity, one major growth limiting factor has been the lack of appropriate custody services for the safekeeping of Digital Assets.

In traditional financial services, a custodian fulfils three (3) key functions relating to assets, namely validation, security and trust. Currently, in the absence of licensed custodians specialised in holding Digital Assets, first-party custodianship remains the main option to safeguard clients' Digital Assets.

This creates a fundamental security concern for Digital Assets given that the loss of a private key equates to losing the ownership rights to the Digital Asset.

Under the existing regulatory framework administered by the FSC, the two (2) following types of custodian licences are being issued:

- Custodian licence under section 100 of the Securities Act 2005 (the "SA");
- Custodian (Non-CIS) pursuant to section 14 of the Financial Services Act 2007 (the "FSA").

In line with the requirements of section 100 of the SA, the holder of the first type of Custodian licence must mandatorily be a bank or a trust company which is a subsidiary of a bank. The holder of this licence is authorised to hold the assets of CIS in custody.

The second type of licence, namely the Custodian (Non-CIS) licence, issued by the FSC under section 14 of the FSA, enables the provision of custody services to clients other than CIS. Despite there being no statutory restriction, as a matter of practice, the FSC has also been issuing the Custodian (Non-CIS) licence solely to banks or bank subsidiaries owing to their financial strength, infrastructure to store physical assets, traceability of assets, speed of execution of orders, global money transfer services and reliability of records.

Yet, the existing regulatory framework applicable to the two custodian licences relate primarily to securities[8] or physical assets and are not appropriate for the safekeeping of Digital Assets.

8 The term "securities" is defined under section 2 of the SA.

To bridge this gap and provide a solution for the custody of Digital Assets to the fintech ecosystem, in line with the Budget 2018/19, the FSA has been amended to empower the FSC to issue the Custodian Services (Digital Asset) Licence under which an entity will be licensed to hold for safekeeping, the Digital Assets of its clients.

The holder of the Custodian Services (Digital Asset) Licence, which is issued under section 14 of the FSA, will be a licensee of the FSC and will be required to ensure strict compliance with the relevant Acts[9] under the administration of the FSC as well as other applicable enactments. Simultaneously the holder of the Custodian Services (Digital Asset) Licence will also be considered as a "financial institution" under the Financial Intelligence and Anti-Money Laundering Act 2002 (the "FIAMLA") and will be required to adhere to the Anti-Money Laundering and Counter-Terrorist Financing ("AMLCFT") related laws, regulations and codes AMLCFT in Mauritius including the FSC Code on the Prevention of Money Laundering and Terrorist Financing, the FIAMLA and regulations made thereunder.

Purpose of this Consultation Paper

In line with its collaborative approach, through this Consultation Paper, the FSC is pleased to present, for the comments and views of the industry, its stakeholders and the public, its perspective on the essential components of the regulatory framework for the Custodian Services (Digital Asset) Licence.

As opposed to the custody of traditional physical assets where the asset itself or its proxy is held by the custodian, blockchain-based Digital Assets are not physically held. With such inherently digitized assets, having appropriate standards for the custody of Digital Assets becomes crucial given that the transaction information pertaining to the asset is public, distributed and immutable.

This Consultation Paper sets down the proposed operational, governance and technical requirements for the Custodian Services (Digital Asset) Licence as envisioned by the FSC.

Approach

In line with section 18 of the FSA, the FSC solely issues a licence upon being satisfied that the applicant, amongst other factors, has adequate resources, infrastructure, and staff with the appropriate competence, experience and proficiency to carry out the activity for which the licence is sought.

In assessing the capacity of an entity to provide custody services for Digital Assets, the approach contemplated by the FSC will focus on three core areas for this activity, namely:

9 "Relevant Acts" is defined under section 2 of the FSA.

1. *Operational and Governance Protocols* – The policies and protocols as well as operational risk management, including fraud prevention, in relation to the custody of Digital Assets.

2. *Safekeeping of Digital Assets* – The generation and securing of seeds and keys as well as management of addresses and wallets relating to Digital Assets. This area also extends to recovery processes regarding seeds and keys which have either been corrupted or otherwise compromised.

3. *Transaction Management* – The procedures for the facilitation of incoming and outgoing transactions in relation to a Digital Asset being held in custody to ensure that appropriate Know Your Client ("KYC") and Customer Due Diligence ("CDD") measures are applied prior to any transactions being authorised.

In respect of the three aforementioned focus areas, the holder of the Custodian Services (Digital Asset) Licence will be required to comply with best standards and practices established by the industry.

The approach proposed by the FSC in some parts of this Consultation Paper is explicit and prescriptive, while in other parts, "standards" and "industry practices" have been mentioned in view of setting the minima criteria while keeping the requirements voluntarily wide. In so doing, the FSC expects that as industry expertise develops in this field of activity, these best practices and standards may then be considered to develop guidelines for specific functions of the custody of Digital Assets.

Technical Requirements

Part I. Operational and Governance Standards

1. Objective of the business

1.1. The objectives of the applicant for the Custodian Services (Digital Asset) Licence shall be limited to the safe-keeping of Digital Assets and operations arising directly from it as stated in the application. For the avoidance of doubt, a single entity applicant will not be permitted to undertake any other financial business activities[10] along with the custody of Digital Assets. Such other financial business activities will have been undertaken under by a separate entity holding the relevant licence from the FSC.

1.2. In addition, for ring-fencing purposes, a single entity will not be allowed to act as custodian for both traditional assets (securities or physical assets) and Digital Assets. An entity wishing to offer both types of custodian services shall be required to do so under separate legal entities and with appropriate licences.

10 The term "financial business activities" is defined under section 2 of the FSA.

2. Minimum Stated Capital

2.1. The custodian of Digital Assets shall, at all times, have and maintain a minimum stated unimpaired capital of not less than MUR 500,000 or such higher amount as the FSC may determine.

3. Governance

3.1. An applicant for the Custodian Services (Digital Asset) Licence shall –

3.1.1. Ensure that its governance structure provides effective oversight of its activities, taking into consideration the nature, scale and complexity of its business;

3.1.2. Establish adequate internal controls and adopt strategies, policies, processes and procedures in accordance with principles of sound corporate governance and risk management;

3.1.3. Maintain its registered office and place of business in Mauritius; and

3.1.4. Have a board of directors composed of not less than 3 directors, at least one of whom shall be resident in Mauritius.

4. Representative in Mauritius

4.1. The applicant must also have, at all times, a representative in Mauritius who shall be responsible for –

4.1.1. Filing with the FSC such document as may be required under the relevant Acts and any other enactment;

4.1.2. Acting as liaison with the FSC for any correspondence, notice or summons; and

4.1.3. Maintaining records of the custodian in line with the applicable statutory requirements.

5. Staffing

5.1. The applicant will have to ensure that it is adequately staffed with the appropriate competence, experience and proficiency to properly perform its functions. It will also be required to have properly defined and documented duties and responsibilities amongst its staff regarding safe-keeping, transaction management and custody related operations.

5.2. Such staffing details and responsibility allocation plans, in line with its business needs will have to be submitted to the FSC as part of its procedure manuals at the time of the application for the Custodian Services (Digital Asset) Licence.

Background screening of personnel

5.3. The applicant will be required to subject all staff performing core custody-related tasks to prior vetting and clearance through appropriate background screenings or other appropriate tests in accordance with best industry-related standards.

5.4. Such screening may have to be conducted on a recurrent basis, depending on business needs, following the issue of the Custodian Services (Digital Asset) Licence and relevant records evidencing these personnel checks must be maintained and made available for inspection by the FSC upon request.

Manual execution of core functions

5.5. The applicant must have documented procedures such that non-automated core functions related to the custody of Digital Assets are performed only by personnel who have been subject to the abovementioned background screening.

Access to Keys, Seeds and related information

5.6. The applicant must also have appropriately documented systems to restrict access to keys, seeds and information relating to Digital Assets being held under custody solely authorised personnel on a demonstrated business needs basis.

5.7. An updated list of authorised personnel having such access must be maintained along with clearly defined procedures to enable or revoke access rights. In addition, access rights to keys, seeds and related information must be adequately logged to evidence access rights management.

6. Outsourcing

6.1. In its application, full disclosure must be made to the FSC regarding functions which the applicant proposes to outsource to any external third party and the rationale for the proposed outsourcing.

6.2. The applicant must have appropriate protocols so that the third party is subject to adequate due diligence both in terms of the fitness and propriety as well as its capacity to fulfil the outsourced function in accordance with the prescribed regulatory requirements for the custody of Digital Assets. Details of such due diligence conducted must be kept on record by the applicant.

6.3. It is to be however pointed out that the applicant shall retain full responsibility vis-à-vis the FSC for the failure by the third party to fulfil the outsourced function.

7. Redundancy strategy for equipment procurement

7.1. The applicant will have to maintain a documented redundancy strategy for the procurement of equipment used to perform core functions of the custody function from alternative suppliers in case of failure by the main supplier(s) to comply with contracts for delivery of such equipment. At any point in time, the applicant must have in place the appropriate infrastructure to ensure that the core tasks relating to its activities are fully functional at all times.

8. Insurance

8.1. Subject to availability, the applicant shall be required to subscribe to adequate insurance protection in relation to the Digital Assets being kept in custody.

8.2. At application stage, evidence that such arrangements for insurance subscription have been initiated, must be submitted to the FSC.

9. Efficiency and Performance

9.1. The applicant must demonstrate that it has, in place, appropriate systems and procedures so that it operates in an efficient manner and completes transactions in a timely manner as per industry best practices and standards.

10. AMLCFT Systems and Controls

10.1. As part of its application document pack, the applicant will be required to submit a detailed report containing an in-depth assessment of the potential money laundering and terrorist financing ("ML/TF") risks posed by its operations as well as the measures, systems, controls and protocols which will be established in relation to those ML/TF risks. Once licensed, prior to starting its operations, the licensee will be required to have those ML/TF systems and controls in place.

10.2. For the sake of clarity, the FSC wishes to point out that the Custodian Services (Digital Asset) Licence will be issued under section 14 of the FSA and as such the holder of this licence, while being a licensee of the FSC, will simultaneously be considered as a "financial institution" under the FIAMLA.

10.3. Consequently, the holder of the Custodian Services (Digital Asset) Licence will be required to ensure strict adherence to the appropriate laws, regulations and codes relating to AMLCFT in Mauritius including the FSC Code on the Prevention of Money Laundering and Terrorist Financing, the FIAMLA and regulations made thereunder.

10.4. As part of its systems and controls to prevent ML/TF, the applicant must have in place procedures to conduct CDD and KYC as well as to ascertain the source of funds/wealth of potential clients prior to on-boarding.

11. Statutory Reporting

11.1. The applicant must have in place a system to ensure that it complies with its statutory reporting requirements as prescribed under the applicable laws.

12. Disclosure to clients

12.1. The documented procedures of the applicant must, in addition, include systems for appropriate disclosures to be made to each client, on a regular basis or alternatively at the latter's request, on transactions relating to his account(s) such as an account statement containing at a minimum, the activity period, transaction dates and amount, account balance and valuation of Digital Assets in the account, where appropriate, to enable the client to identify any unauthorized or erroneous transactions and ascertain the account's integrity.

12.2. The FSC considers that the protocols of the applicant must also cater for the following disclosures:

12.2.1. Each client to be provided with an original of the signed agreement regarding the custody of his Digital Assets at the time of on-boarding;

12.2.2. Thereafter, client to be informed of any action which is likely to impact on the signed agreement; and

12.2.3. Any occurrence which may have an incidence on the Digital Assets belonging to the client being held in custody;

12.3. In the event that such disclosures are being made to the client through a web-based service, the applicant will need to have in place a user multi-factor authentication system in line with the best industry practices.

13. Qualified licence to be issued based on value of Digital Assets under custody

13.1. If the application is successful, the applicant, will initially be issued with a qualified licence allowing it to start its operations and develop its activities. Once it is fully operational and after having held Digital Assets under custody valued at least at USD 30 million for a consecutive period of three (3) months, it will be required to inform the FSC and submit evidence thereof to the FSC. Upon being satisfied with the operations of the holder of the qualified licence, this licence will then be converted into the full Custodian Services (Digital Asset) Licence. The holder of the qualified licence shall endeavour, on a best effort basis, to be fully operational and meet the threshold of USD 30 million worth of Digital Assets under custody within six (6) months from having been issued with the qualified licence.

14. Minimum assets to be maintained as reserve

14.1. After having started its operations under the qualified licence and at all times thereafter, the applicant will also be required to maintain a minimum quantum of assets in reserve to ensure that it has sufficient liquidity to continue its operations in the event that all its clients have withdrawn their Digital Assets. The amount of this minimum reserve, which is to be notified to the FSC, will have to be maintained by the applicant in line with its operational needs.

14.2. As a general rule, the applicant will not be permitted to prevent the withdrawal by a client of its Digital Assets in line with the contract, in order to maintain the minimum reserve requirement.

15. Management of operational risks

15.1. The applicant's procedures must include a comprehensively documented operational risk management programme (ORMP) which shall include all current industry risks and be audited on an on-going basis to cater for emerging risks to its business. This ORMP, to be applied in the operations of the applicant and communicated to all relevant personnel, will need to include, at a minimum:

15.1.1. Strategies developed to identify, assess, monitor and control/mitigate operational risks;

15.1.2. Policies and protocols relating to operational risk management and controls;

15.1.3. Methodology to assess operational risks; and

15.1.4. Operational risk reporting system.

16. Custody processes and systems testing

16.1. Once it has been licensed by the FSC, the custody processes and systems in place must be tested on a scheduled recurrent basis with evidence of such tests and findings thereof being appropriately documented. Such findings must be made available to the FSC for inspection, upon request. The schedule for system testing must be included in its protocols to be submitted to the FSC at the time of application.

16.2. The recurrent testing schedule must mandatorily take into consideration procedural risks as well as high impact financial risks and may also extend to:

16.2.1. Penetration testing and vulnerability scans;

16.2.2. Wallet integrity audits;

16.2.3. Key and seed generation procedures;

16.2.4. Completed transaction audit to ensure compliance with protocols;

16.2.5. Suspicious transaction handling;

16.2.6. Migration of storage devices (cold to hot storage and vice versa); and

16.2.7. Proof of reserves audits.

16.3. Systems testing must be undertaken in line with the industry's best standards and practices and may be conducted by the licensee, independent third parties or both. The participation of external parties will be highly relevant in defining risks and tests which may have been overlooked by the licensee.

17. Incident Reporting

17.1. The applicant must have in place appropriate protocols to ensure that any incident, which results in an interruption of its operations, is properly logged and documented with details of the cause of the incident, impact, method used to resolve the incident and timeframe for doing so. The procedures of the applicant will have to provide for such a report to be periodically escalated to the applicant's management and board of directors for their information. The report may also be used to update the existing custody processes and systems in view of plugging any identified gaps.

18. External Audit of policies and procedures

18.1. The applicant must have in place appropriate arrangements for its policies and procedures to be externally audited. The external audit findings must be used to address any shortcomings identified. Records of the audit findings along with documentation of any remedial actions implemented must be kept and made available for inspection by the FSC upon request. The FSC recommends that the first external audit be conducted within the first year of operation and thereafter on a recurrent basis, in line with industry best standards and practices.

19. Use of Automation

19.1. The applicant may have recourse to the use of automation in relation to its functions. The proposed automation of its functions will have to be disclosed in its procedures submitted at the time of application along with appropriate justifications.

19.2. For any use of automation to perform core and other operational functions relating to the custody of Digital Assets, the ORMP is to be duly updated to provide for scenarios to be followed in the event that the automation fails.

20. Record keeping

20.1. The systems of the applicant must have properly documented procedures relating to record keeping on its clients, including their respective identity as well as information on the Digital Assets kept under custody, including detailed transactional information. Such records must be in line with the appropriate statutory requirements and must be available for inspection upon request by the FSC.

20.2. Transactional information to be maintained on record to include:

20.2.1. Transaction time stamp;

20.2.2. Transaction type;

20.2.3. KYC/CDD on parties to the transaction;

20.2.4. Relevant signatories and transaction approval/rejection evidence;

20.2.5. Account balances; and

20.2.6. Transaction value.

20.3. The applicant may consider keeping its records and data using blockchain technology for immutability.

21. Business Continuity

Personnel Redundancy

21.1. For the purposes of business continuity, the applicants will be required to have:

21.1.1. As part of its protocols, a personnel redundancy system to ensure the continuity of its operations in the event that the primary personnel assigned to perform a non-automated core function is unavailable. This may include having back-up staff with appropriate expertise to perform the applicable function.

21.1.2. A suitable alternate site which will allow it to continue its operations uninterrupted, in the event that the primary custody location is compromised.

Disaster Recovery

21.2. The FSC will require that the applicant maintains appropriate disaster recovery facilities, with appropriate geographic segregation and equivalent security installations as the main place of business, in view of ensuring business continuity and client asset protection.

22. Statutory Compliance

22.1. The applicant, once licensed, must ensure that it complies, at all times, with all applicable laws in Mauritius, and where applicable, the relevant laws in the jurisdictions in which it operates.

Part II: Custody Safekeeping Standards

1. Key and Seed Generation

1.1. As part of its documented protocols to be submitted to the FSC at application stage, the applicant will be required to demonstrate that appropriate safeguards have been embedded in the seed creation and subsequent key generation process so that seeds and keys are sufficiently resistant to speculation or collusion.

1.2. In this respect, the applicant will be required to establish that the method to be employed for the generation of asymmetric private-public key combinations adhere to best industry standards and practices in terms of entropy, to ensure unpredictability and randomness for resilience to supposition. The method may also include an additional security measure such as a back-up mnemonic pass-phrase generated as part of the seed which may be utilized to regenerate the seed if need be.

1.3. Ideally, the applicant must have at least two distinct individuals from its personnel, involved in the process of generating entropy during seed creation. The protocols of the applicant must provide for measures ensuring that no single person ever comes into possession of all facts or knowledge of the entirety of the seed or back-up mnemonic passphrase. As a general rule, the applicant's protocols must include proper safeguards to prevent individuals who have been involved in seed creation from getting access to the systems and processes enabling the initiation of transactions through cryptographic signature.

1.4. The protocols of the applicant must also cater for seed creation and key generation to be carried out on an Air Gap Machine in physical space which is, as per industry best practices, secured to be resilient against malicious attacks, whether over the network or physically.

1.5. In the event that a single seed is produced for a signatory, the applicant's procedures must ensure that the signatory is involved in the production of the associated key. Moreover, as soon as the seed has been generated, the applicant must have systems in place to make sure that it is to be stored on an encrypted, password-secured device.

1.6. Furthermore, the applicant must demonstrate that it has in place an appropriate process according to which all digital data post seed creation and key generation, including entropy procedures, seeds, private keys, or any other sensitive wallet information created during the seed-key generation process is securely deleted using an industry

accepted deletion process for electronic media. Any such information in hard copy is also to be appropriately destroyed using pulping, cross-cut shredding or incineration.

2. Key and Seed Storage

Primary Key and Seed Storage

2.1. Regarding primary key and seed storage, the applicant must demonstrate that its protocols provide for keys and seeds which are not in use, to be stored by means of strong encryption and password-secured device, in accordance with industry best standards and practices.

2.2. In addition, at any point in time, the applicant is to have systems and procedures to ensure that:

2.2.1. Fewer than the number of keys required to initiate a transaction are stored together whether online or at a single physical location; and

2.2.2. It is impossible to initiate transactions solely using signatures stored online or at the physical address.

Back-up Storage

2.3. In terms of back-up storage, once the mnemonic back-up phrase has been generated, the applicant's protocols will have to provide for it to be broken in two or more parts with each part being kept separately in distinct tamper-proof containers stored in different physically secure locations. The protocols, must not, under any circumstances, allow a sufficient number of parts of the back-up phrase required to regenerate the seed, to be stored in a single location.

2.4. Back-up seed storage must, in accordance with industry best practices, be off-site from the place where transactions are managed and operations are conducted. Off-site physical seed storage must, at least, be maintained by a third party which is adequately equipped with safe deposit boxes enabling dual key access.

2.5. The procedures of the applicant must incorporate measures to ensure that the access to off-site back-up seed storage is restricted solely to the authorised personnel of the applicant. Prior to allowing access to the back-up seed storage, the identity of the authorised personnel will have to be verified and confirmed by the third party through multifactor identity verification and audit consistent with industry best practices.

2.6. All back-up seed storage facilities must be equipped with appropriate vaults, 24/7 video monitoring and adequate security systems for protection against forcible attacks, flood, fire, cyclone and other climatic conditions.

2.7. The applicant must also have in place systems to ensure that an internal audit of the back-up seeds is conducted, at a minimum, on a quarterly basis to assess whether they

have been tampered with or removed from secured storage. The audit results must be properly recorded with details of any incidents observed as well as any remedial actions taken, if any, and are to be provided to the FSC for inspection upon request.

Impaired Key

2.8. As part of its systems and protocols, the applicant will be required to have documented procedure to be actioned in the event that a key, seed or a part thereof is suspected to have been compromised, including but not limited to new wallet creation and migration of the relevant Digital Asset thereto.

2.9. Its protocols must also provide for the applicant to duly investigate any suspicion that a key, seed or a part thereof has been compromised. The investigation findings must be properly documented and made available for inspection by the FSC upon request.

Uninterrupted Access

2.10. The applicant must also have written procedures demonstrating that it will be able to provide its clients with uninterrupted access to their respective Digital Assets being kept under its custody in the event that it is no longer able to abide by the custody agreement or it ceases to operate. These procedures may have to extend to transferring the Digital Assets according to the instructions of the client or such other mutually agreeable arrangements.

Segregation of client assets

2.11. The FSC will require that the applicant maintains systems and controls ensuring that an address or wallet is ascribed to one single client and that the Digital Assets belonging to that client is kept in his designated address/wallet. Adequate procedures must also be in place to ensure that at no point in time, the Digital Assets belonging to different clients are pooled or kept together at a single address or common wallet.

Address use strategy

2.12. The FSC considers that the use of a new address for every transaction relating to a client ensures the latter's privacy and the confidentiality of his personal information. Thus, using the same client address for numerous transactions may arguably lead to more information being revealed on the client, for instance his identity or commercial investment data with resulting safety concerns. Accordingly, the protocols of the applicant must include appropriate address use strategy which justifies when a new address will be used and when recurrent use of the same client address will be made for multiple transactions.

3. Security infrastructure for on-site cold storage of Digital Assets

3.1. Regarding on-site cold storage, the applicant will have to demonstrate to the FSC that it will have in place, an adequately secured physical infrastructure, which will include but shall not be limited to, guarded access to the facilities with restricted admittance to authorised personnel only, vault/safe storage with dual key requirements and 24/7 closed-circuit television system. Access procedures will have to be adequately documented and must be made available for inspection by the FSC upon request.

Storage Strategy for Digital Assets

3.2. The procedures of the applicant must include a strategy for choosing the suiting storage for a Digital Asset being brought in custody factoring, amongst other circumstances, the volume of transactions relating thereto, the speed at which those transactions are to be executed and risk appetite of the client. This strategy for choosing the appropriate storage medium will have to be in accordance with industry best standards and practices.

Security Breaches

3.3. The protocols of the applicant will need to clearly spell out the procedures, which are to be periodically audited, to be actioned in the event, or suspicion thereof, that a security breach has occurred including hacking, attack, theft or any situation whereby a Digital Asset being kept in custody has been compromised. The systems of the applicant will have to incorporate appropriate actions specifically designed to protect the Digital Assets being held in custody in the event of security breaches. The policies of the applicant will have to extend to duly notifying the relevant client of the security incident.

Revocation of a signatory's access key to a back-up seed

3.4. Additionally, the FSC expects the applicant's protocols to include measures for the immediate revocation of the key(s) held by a signatory. Such revocation must spontaneously prevent the signatory from accessing the back-up seed or any information relation to the mnemonic phrase used in the seed creation. A revoked signatory must also not be able to recover the seed.

3.5. In practice, the FSC expects that the revocation of a signatory will only entail the removal of the latter's access to a back-up seed without the need to create a new wallet or migrate the Digital Asset in custody to another wallet. Such procedure for revocation of access must be periodically audited and user access logs must be monitored for unauthorized access by revoked signatories.

4. Asset Agnostic systems and procedures

4.1. The systems and procedures of the applicant will be expected by the FSC to be asset agnostic and ensure the same level of regulatory compliance relating to the safekeeping, transaction management and custody operations with respect to every Digital Assets type irrespective of wallet functionality protocol.

4.2. However, the applicant may choose to have the systems and protocols supporting one specific type of Digital Asset, instead of multiple types. In such a situation, the licence issued to the applicant will be restricted to the custody of the specific Digital Asset type. This licence may thereafter be extended as the systems and protocols evolves to support other types of Digital Assets.

Part III: Custody Transaction Handling Standards

1. Multi-Signature Authorisation

1.1. The protocols of the applicant must ensure that at any point in time, no single party is able to initiate and complete a transaction pertaining to a Digital Asset being held in custody. Furthermore, the applicant will mandatorily be required to mitigate the risk of collusion between the signatories in view of initiating unauthorized transactions relating to a Digital Asset under custody.

1.2. A possible consideration is for the applicant to use an M-of-N multi-signature standard, in line with the best industry practices, requiring a minimum number of signatures to have quorum for the purpose of initiating and completing a transaction. In case this approach is chosen by the applicant, the set minimum number of signatures for quorum will have to be documented by the applicant.

2. Selection of signatories

2.1. To curtail the risks of collusion or malicious acts by signatories, the applicant will be required to have an established procedure in view of designating the signatories for transactions relating to Digital Assets under custody. Such risks of collusion and other acts of bad faith by signatories must be catered for in the applicant's ORMP.

2.2. Methods which may be contemplated by an applicant to mitigate the risk of collusion amongst designated signatories may include:

2.2.1. Identities of signatories being unknown to each other; and

2.2.2. Signatories having differing incentives (for instance, the client or his representative, the applicant and other possible third parties such as a bank or law firm).

3. Justification for approval/rejection of a transaction by a signatory

3.1. The applicant will have to demonstrate that as part of its protocols, each signatory will be required to document the rationale to approve or reject a transaction in relation to a Digital Asset under custody. The rationale under which a transaction may be approved or rejected by a signatory, the evidence to be kept on record as well as the time frame to validate or reject the transaction, may be contractually agreed between the client, the custodian and the signatories. Any transaction approval/rejection and supporting justifications must be properly logged and made available to the FSC for inspection upon request.

3.2. The applicant will also be required to maintain a detailed log for any change in the chain of access to a Digital Asset.

3.3. Records of transaction approval/rejection and supporting justifications as well as any change in the change of access to a Digital Asset, may also be made available, upon request, for review by the owner of the Digital Asset subject to the transaction.

4. Detection of suspicious or fraudulent transactions

4.1. The applicant must have a documented system for detection of suspicious or fraudulent transactions as well as the procedure for reviewing suspicious transactions with clear actions to be implemented based on the findings of the review, in line with the requirements of the relevant enactments.

5. Valuation of the Digital Asset under custody and evidence thereof

5.1. In the event that the current market value is amongst the underpinning reasons for a transaction involving a Digital Asset being kept in custody, prior to the transaction, the protocols of the applicant must provide for disclosure, to the client and signatories, of the source of the valuation and the methodology used for such valuation. This valuation methodology will have to be in accordance with the industry best standards and practices for the calculation of the real-time valuation of Digital Assets at the time of transaction.

Conclusion

This Consultation Paper contains the FSC's perspective on the regulatory framework for the Custodian Services (Digital Asset) Licence, on which, in line with its collaborative approach, the FSC is seeking feedback from the industry, its stakeholders and the public.

The consultation period will span from 05 November 2018 to 30 November 2018. Interested parties are invited to send their comments, feedback and suggestions in relation to the regulatory framework proposed in this Paper during the consultation period by email on csda@fscmauritius.org.

Glossary of Terms

Air Gap Machine	A computer specifically designed so that it is impossible for it to connect to the internet. The computer is designed without a microphone, network card, hardwired network connectivity and Bluetooth.
Cold Storage	A method of storing Digital Asset or information whereby the device used for storage is not connected to the Internet.
Custodian	The entity entrusted with the custody of Digital Assets.
Custody	The safekeeping of Digital Assets being held or transacted.
Digital Assets	Any token, in electronic/binary form, which is representative of either the holder's access rights to a service or ownership of an asset. A Digital Asset, in this respect, includes a digital representation of value which: • is used as a medium of exchange, unit of account, or store of value but which is not legal tender, even if it is denominated in legal tender; • represents assets such as debt or equity in the promoter; or • provides access to a blockchain-based application, service or product. A Digital Asset, however, exclude: • any transaction in which a business, as part of an affinity or reward programme, grants value which cannot be exchanged for legal tender, bank credit or any Digital Asset; or • a digital representation of value issued for use within an online gaming platform.
Entropy	Unpredictability or randomness within the source code which is used to generate a cryptographic seed which ensures that a seed cannot be simply recreated.
Multi-Signature	The requirement for a minimum of number of signatures (M) out of the total number of available signatures (N) for a wallet in order for a transaction to be initiated. Also referred to as "multi-sig" or M-of-N transacting method.
Signatory	An individual providing one of the signatures in an M-of-N multi-signature transacting method.
Signature	An authorization protected by cryptography which is applied by a designated signatory to initiate a transaction.
Safekeeping	The contractual obligation according to which a custodian is required to secure and preserve Digital Assets kept being held in custody.

Seed	An alphanumeric phrase generated through the process of entropy. The alphanumeric phrase is a list of words from a specific word set which are used to create a mnemonic. This mnemonic stores all required information to use a key or apply a signature.
Transaction	An exchange or operation specific to a Digital Asset being held in custody.
Transaction Type	Classification of a transaction according to its specific purpose. Transaction types will include deposit and withdrawal.