GIBRALTAR FINANCIAL SERVICES COMMISSION

DLT Provider Guidance Notes

Protection of Clients Assets and Money

Introduction

The purpose of this guidance note is to provide a DLT Provider, as defined in the Financial Services (Distributed Ledger Technology Providers) Regulations 2020 (the DLT Regulations), with guidance as to the operational, technical and organisational standards expected and in some circumstances required by the GFSC.

This guidance note is specifically in respect of regulatory principle 5 of the DLT Regulations (the Regulatory Principle).

The Regulatory Principle states that "***A DLT Provider must have effective arrangements in place for the protection of client assets and money when it is responsible for them"*.**

This document should be read as interpretative guidance for a DLT Provider and the examples contained in this document should be noted as indicative of good practice by a DLT Provider in connection with the Regulatory Principle.

A DLT Provider should note that the GFSC will take this document into account when reviewing a DLT Provider's practices. The operational standards expected and required by the GFSC of a DLT Provider will vary depending on the size, particular nature, scale or complexity of the DLT Provider's business.

Customer Asset Management

DLT Provider will be expected to take all reasonable precautions to protect customer assets and money in its custody or control against any eventualities and threats. Custodial assets and monies must be segregated from the DLT Provider's own assets and monies.

However, to the extent that a DLT Provider holds fiat currencies for customers (e.g. pending or following conversion to or from cryptocurrency), then any such funds must be protected, be sufficiently liquid, and be clearly segregated as customer monies with a regulated credit, e-money or payment institution, acceptable to the GFSC. Alternatively, a DLT Provider must demonstrate to the GFSC it can achieve these outcomes via other means.

A DLT Provider must put in place appropriate policies, processes and procedures to protect customer assets. A DLT Provider is expected to consider, as a minimum, the following key areas in any such processes and procedures.

Management Responsibility

A DLT Provider is expected to nominate one of its directors or senior management as being primarily responsible for customer assets and notify the GFSC of such appointment.

Systems of Controls

A DLT Provider must have appropriate systems of control to manage customer assets that are proportionate to the size of the business, the assets in custody and the risks involved in that business.

Systems of control related to IT and software should be up to date and meet latest industry protocols and standards.

Systems of control must be implemented to detect and prevent fraud and cybercrime, examples of which may include:

- Multi Factor Authentication;
- pattern analysis on internet traffic to servers;
- IP checking;
- looking for brute-force attacks on account passwords; and
- multi-level security checks of customers that request access to their accounts.

A DLT Provider should consider the appropriateness, cost and benefit of obtaining insurance to cover customer assets in addition to any other safeguards that are in place.

Systems of control are expected to be regularly stress-tested.

A DLT Provider must consider the inherent risks related to customer assets, mitigating controls and residual risk and this must be adequately recorded on the firm's risk register.

Safeguarding and Segregation

Customer assets must be held separately from a DLT Provider's own assets. Customer assets must be clearly designated and easily identifiable. Customer assets do not represent property of a DLT Provider and must therefore be protected from third party creditors of a DLT Provider.

There is an expectation that a DLT Provider will implement an appropriate contractual relationship with its customers that is reflective of these arrangements. Customers' agreement to the firm's terms and conditions will ordinarily suffice, provided the arrangements in question are adequately reflected.

A DLT Provider that uses third parties to store or safeguard customer assets will need to take all reasonable steps to ensure that the systems and controls used by the third party provider(s) comply with this guidance note and any other obligation imposed on the DLT Provider.

Furthermore, the DLT Provider should obtain formal acknowledgement that all fiat and virtual assets held by the custodian are held in trust and that the custodian is not entitled to combine the amounts with any others or to exercise any right of set-off or counterclaim against such assets in respect of any debt owed to the custodian by the DLT Provider.

A DLT Provider that manages Private Keys relating to cryptographic assets belonging to customers is encouraged to not pool values belonging to different customers using the same Keys unless it is confident that its processes and controls are sufficiently robust. A DLT Provider must adequately identify the customer(s) to which the Keys relate.

Frequent Reconciliation

A DLT Provider must take all reasonable steps to ensure that any value is applied to the correct wallets in good time.

A DLT Provider must reconcile customer virtual assets and its own assets as a minimum once a day, and customer fiat assets at least on a monthly basis.

When reconciling virtual asset movements, the firm should ensure that any internally calculated balances are reconciled to the expected balance on the underlying blockchain in question. This should be performed both at transactional level and also from a closing balance position. Any differences should be fully reconciled and investigated. Any unidentified differences leading to a lower amount of virtual asset balances on the underlying distributed ledger when compared to the internal records, should be covered by the firm until these are investigated and cleared.

This process should ideally be automated, especially when there is frequent movement in customer funds.

Record Keeping

All customer asset records are expected to be stored securely during the relationship with a customer and for a minimum of 5 years following termination of the customer relationship (subject to any contrary legal requirements). Records are expected to be comprehensive and up to date.

A DLT Provider is expected to operate continuous (near 24/7) real-time electronic record systems that are subject to a regular (i.e. as a minimum, every working day) exceptions-based review by suitable staff.

Records are expected to include any customer instructions in respect of how to manage customer assets.

Records are expected to be kept in a manner and format that provides a clear audit trail to enable an auditor to sign off on a DLT Provider's accounts and its systems and controls.

Naming and Schema

A DLT Provider must ensure that naming conventions and schema for data used to identify and protect customer assets allow the DLT Provider, the GFSC or any person appointed to step-in to manage the DLT Provider, to be able to control/manage those customer assets should the need arise.

Private Key Management

Private Keys relating to value stored on behalf of customers should be stored and secured in a manner that minimises the risk of loss or theft.

A DLT Provider in custody of virtual assets based on decentralised public networks should only store private keys in online (hot) wallets that are sufficient to meet immediate liquidity needs. Remaining private keys should be held in offline wallets (i.e. in cold storage).

The GFSC will expect DLT Providers to maintain the highest and most relevant industry standards with respect to security and management of private keys. It is acknowledged that the industry is constantly evolving, this emphasises the importance of a DLT Provider having to evolve its security practices on a regular basis in order to adequately protect customer funds. Private keys should be stored with the utmost security in mind, while also allowing sufficient liquidity to meet day-to-day requirements.

The following should be considered:

- ensuring the keys/seeds are created by the firm;
- ensuring the key/seed is generated using a random process;
- implementing multi-signature arrangements to ensure that there is no single point of failure or reliance on a single party to initiate transactions;
- ensuring that redundant keys are assigned, for example 2 out of 3, or 3 out of 5 required to sign;
- ensuring that the multisig keys are distributed across several geographical locations, and different organisational entities if possible;
- storing backups in separate geographical locations, accessible in the event that it is required as part of a DLT provider's business continuity and disaster recovery plans;
- transactions are signed in a fully offline environment, and only broadcast to the network when required, limiting the possibility of a cyber-attack;
- strong physical security measures to protect keys held offline;
- background checks on key holders;
- sign-off from separate individuals prior to keys signed by the key holders;
- existence of a key compromise protocol; and
- external security audits.

The GFSC will expect DLT Providers to adopt best practices and ensure that potential threats or vulnerabilities are mitigated.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi