TECHNICAL REPORT

ISO/TR 23576

First edition
2020-12

Blockchain and distributed ledger technologies — Security management of digital asset custodians

Reference number
ISO/TR 23576:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

A digital asset custodian holds customers' digital assets for safekeeping in order to minimize the risk of their theft or loss. This document illustrates the security risks, threats, and measures which digital asset custodians consider, design, and implement in order to protect the assets of their customers, based on best practices, existing standards and research. For example, the management of signature keys for digital assets requires special attention, taking into account the specific nature of blockchains and DLT systems and the security challenges they face. A key topic discussed is the appropriate management of signature keys by digital asset custodians in order to prevent misuse and transactions by unauthorized individuals.

Blockchain and distributed ledger technologies — Security management of digital asset custodians

1 Scope

This document discusses the threats, risks, and controls related to:

— systems that provide digital asset custodian services and/or exchange services to their customers (consumers and businesses) and management of security when an incident occurs;

— asset information (including the signature key of the digital asset) that a custodian of digital assets manages.

This document is addressed to digital asset custodians that manage signature keys associated with digital asset accounts. In such a case, certain specific recommendations apply.

The following is out of scope of this document:

— core security controls of blockchain and DLT systems;

— business risks of digital asset custodians;

— segregation of customer's assets;

— governance and management issues.

2 Normative reference

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22739, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
digital asset custodian system
system that holds customers' digital assets for safekeeping in order to minimize the risk of their theft or loss

Note 1 to entry: In this document, holding assets is considered in a broad sense, as it includes for instance, the case of physically or digitally storing the assets, but also the case of holding the private keys associated with the assets, or even the case of protecting access to the assets, like holding one of the keys protecting the access to the assets.

3.2
cold wallet
cold storage
offline application or mechanism used to generate, manage, store, or use private and public keys

3.3
hot wallet
hot storage
online application or mechanism used to generate, manage, store, or use private and public keys

3.4
hardware wallet
wallet which leverages a hardware device (e.g. HSM) to generate, manage, store, or use private and public keys

3.5
deterministic wallet
wallet in which multiple key pairs are derived from a single starting point known as a seed

3.6
hierarchical deterministic wallet
deterministic wallet (3.5) in which child key pairs are derived from the master key pair

Note 1 to entry: Descendant key pairs can be derived from the child key pairs, in a hierarchical manner, hence the name of the wallet. Child key pairs can be used and shared without having to share the master key pair. It is defined within Reference [7].

4 Abbreviated terms

AML	anti-money laundering
API	application programming interface
APT	advanced persistent threat
CFT	countering financing of terrorism
DLT	distributed ledger technology
DNS	domain name system
FATF	Financial Action Task Force
FQDN	fully qualified domain name
HSM	hardware security module
SMS	short message service
ISMS	information security management system
ISP	internet service provide
KYC	know your customer
OS	operating system
OWASP	Open Web Application Security Project
PII	personally identifiable information

PKI public key infrastructure

PoW proof of work

TLS transport layer security

5 Basic description of a model of online system for digital asset custodianship

5.1 General

In this clause, an example implementation for an online digital asset custodian system is presented. This model will then be used to explain the concepts and provisions in this document. However, it is also worth noting that other types of custodian systems exist. For example, decentralized exchanges (DEXs), have quite a different implementation compared to the one illustrated in Figure 1. Furthermore, protocols like atomic swap and multisignature can be considered a type of custodian as well. Therefore, although most of the content of this document applies to any kind of custodian, some of the risks and potential controls discussed may or may not apply to other types of custodian systems.

5.2 Example of a system for digital asset custodians and its functional components

Figure 1 shows an example model for a digital asset custodian system.

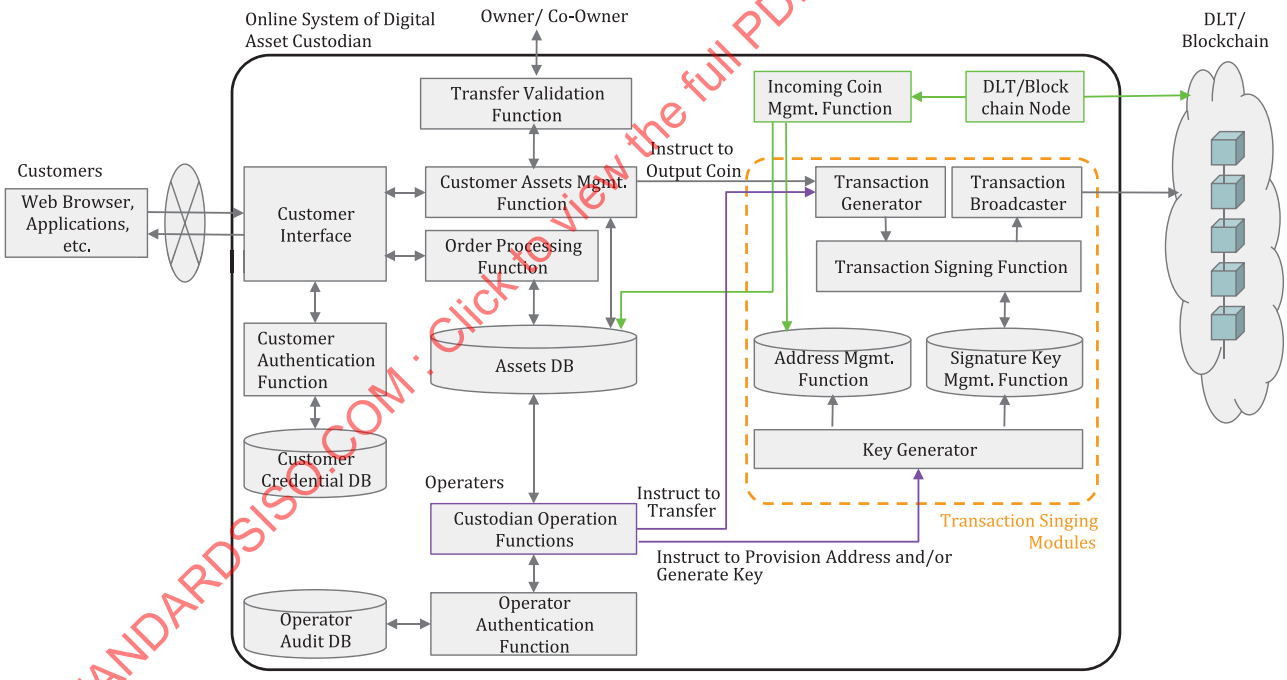

Figure 1 — Basic example model of a digital asset custodian

Table 1 — Functional components of a digital asset custodian

Functional components	Explanation
Interface (web application, APIs)	Provides screen and input functions such as login, account management (deposit/ withdrawal) and trading for the customers (users). The most common interfaces are web applications, APIs, and mobile apps.
Customer authentication function	Performs user authentication for login purposes to the system.
Customer credential database	Manages required IDs for login and verification information related to user authentication process (e.g. password verification information).

Table 1 *(continued)*

Functional components		Explanation
Transfer validation function		Verifies the granted permission to proceed to the transfer of digital data or assets by the owner or co-owners when the transfer implies the validation of multiple parties. For example, the use of multisignatures schemes to validate an authorized outgoing transaction.
Customer assets management function		A group of functions which provide customer account management. For example, these functions perform deposits or withdrawals (output coins) and, more generally, other asset manipulation processes according to user instructions. The functions provided may refer to or update asset data.
DLT / Blockchain node		A node in a DLT / blockchain system, which communicates with its peers (i.e. other nodes).
Incoming transaction management function		Verifies transactions stored in DLT / blockchain to confirm whether incoming assets refer to the specified addresses. Updates the asset database according to the transaction retrieved from the DLT / blockchain.
Order processing function		A group of functions for the management of sales instructions from customers. The order processing function performs actions related to trading of digital assets. This function refers to and updates asset data.
Assets database		Manages the record of assets both for fiat currencies and digital assets. The asset database does not include the signature keys for signing transactions. These are managed separately from the assets for each customer.
Transaction signing modules	Transaction generator	Generates transactions to be sent to the DLT / blockchain based on instructions from the customer asset management function or the custodian's operation function.
	Transaction broadcaster	Sends the signed transaction to the DLT / blockchain. Transactions are broadcasted to blockchain nodes through network protocols.
	Transaction signing function	Generates digital signatures based on the instructed transaction contents using the relevant signature key (i.e. IDs and addresses).
	Address management function	Manages verification keys related to the signature keys, or to addresses (i.e. such as values calculated from the verification keys).
	Signature key management function	Manages the signature keys of the digital assets (i.e. the keys used for the signature of the transactions). Signature keys may be stored in a cold wallet as a security measure.
	Signature key generator	Generates signature keys. The generated keys are registered in the signature key management function, and the verification keys and addresses are registered in the address management function.
Custodian operation functions		A group of functions dedicated to the custodian's operators and/or administrators. Administrator and operators can instruct the module to perform function such as generating new signature keys or transfer digital assets.
Operator authentication function		Authenticates the operators and administrators of the system.
Operator audit database		Manages auditing data related to the authentication processes of operators and administrators for the system.

The functional components described in Table 1 are intended to logically distinguish the various functions within the system, and do not represent an actual architecture of such a system. As an example, in a real-world implementation, the address management function would probably be implemented using a database. Also, there are implementations in which multiple functional components are packaged together. All the functional components of the transaction signature system could be integrated within the customer asset management system, or they could be operating as a separate system. Many implementations of Bitcoin wallets provide all functions for the transaction signature system as a single atomic system. It is also possible to imagine some of these functions being provided by an external "subcontractor" system, such as a remote server.

5.3 Examples of transactions

— Fiat currency deposit

a) The customer sends fiat currency to the custodian's bank account.

b) The custodian confirms the reception of the fiat currency transfer and updates its assets database to reflect the customer's asset status in relation to the transfer just received.

— Digital asset deposit

a) The customer transfers digital assets to an address specified by the custodian. The transfer is performed by using the customer's digital assets wallet (i.e. other custodian or web/app wallet).

b) The custodian confirms that the digital assets have been transferred to the correct address and updates its assets database to reflect the customer's asset status in relation to the transfer just received.

— Trading transaction

a) The customer accesses the interface made available by the custodian and instructs the system to perform some actions (e.g. trading).

b) The instructions to perform an action are received by the custodian and are processed by the custodian operations functions module. The result of the trade operations is processed by the custodian operations functions module which updates the asset database accordingly.

— Customer digital asset withdrawal

a) The customer accesses the interface made available by the custodian and instructs the system to transfer their digital assets to another address (i.e. output coins).

b) The instruction to output coins is processed by the customer assets management functions module. The transaction generator creates a transaction message based on the received instructions such as receiving address and the amount of digital assets to transfer.

c) The transaction message will be digitally signed by the transaction signing functions module.

d) The signed transaction message is delivered to all nodes on the DLT / blockchain by the transaction broadcaster module.

— Internal transfer by operator or administrator

a) The administrator or operator instructs the system to transfer digital assets to another address through the custodian operations functions module. For example, the digital assets may be sent between addresses managed within the custodian.

b) The instructions to output coins are then processed by the custodian operations functions module. The transaction generator creates a transaction message based on the received instructions such as receiving address and the amount of digital assets to transfer.

c) The transaction message will be digitally signed by the transaction signing functions module.

d) The signed transaction message is delivered to all nodes on the DLT / blockchain by the transaction broadcaster module.

5.4 Description of keys used for signature and encryption

5.4.1 Type of keys

Table 2 describes the different types of keys which can be used for signature and encryption within a digital asset custodian system.

Table 2 — Types of keys

Types	Description
Signature key	A signature key for signing transactions (for digital signature schemes standardized in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts))
Verification key	A public key for verification of transactions (for digital signature schemes standardized in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts)) It is common practice in public blockchains to calculate addresses as unique values derived from the verification key. In private DLT systems / blockchains this may not be necessary
Encryption/decryption key for signature key	Secret key (symmetric key cryptography) used to keep signature key confidential / protected
Master seed	A seed to generate a signature key in a deterministic wallet

5.4.2 Flow for key generation and key usage

Figure 2 shows a typical lifecycle for the different type of keys described in Table 2.

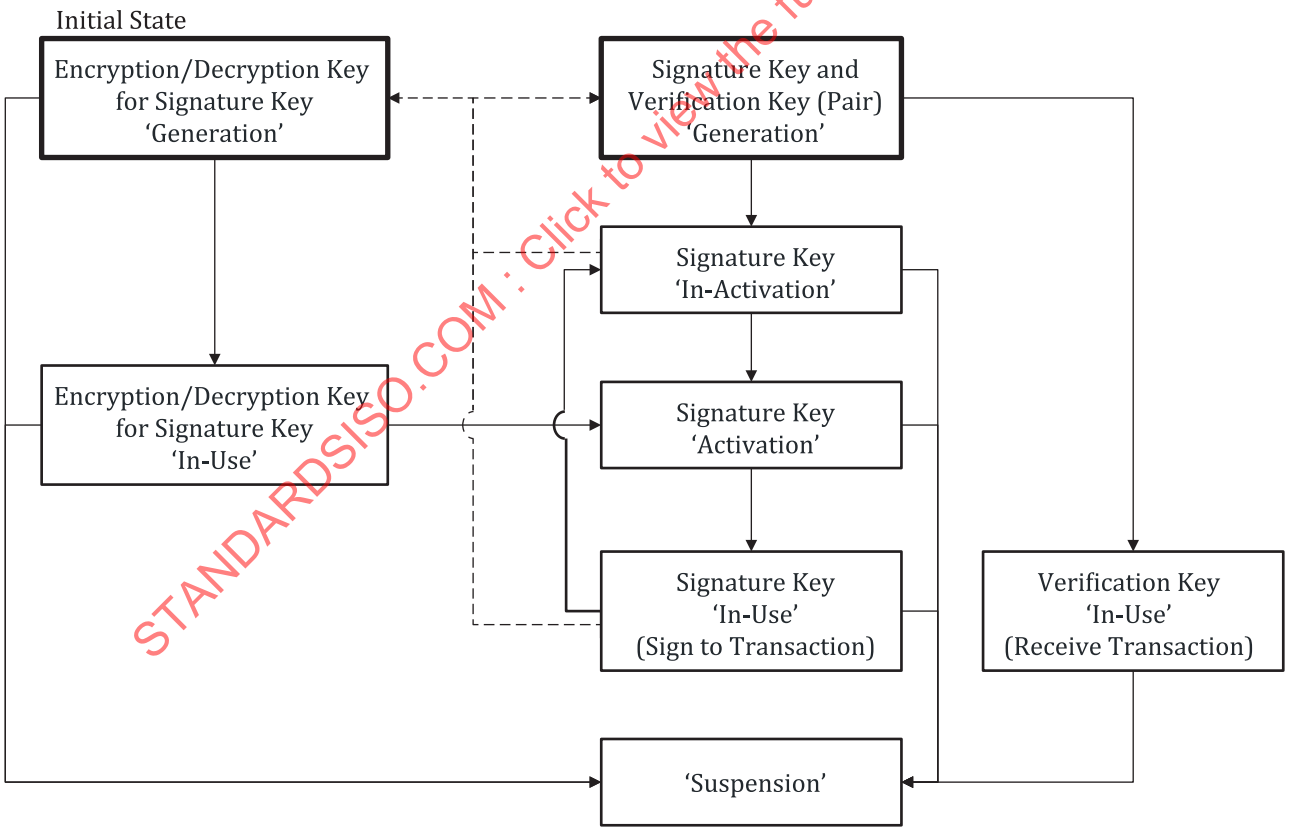

Figure 2 — Lifecycle of signature key, verification key and encryption/decryption key for signature key

After a pair of keys (signature and verification, hereafter "key pair") is generated, an address, which will be used to receive transactions, is derived from the verification key. A sender will only need this address to be able to transfer one or more assets to it.

A signature key is considered inactive, when it is stored in a manner in which it cannot directly be used to sign (i.e. if it is encrypted). As an example, within the key management function module in Figure 1, a signature key could be encrypted using a pass phrase, rendering it inactive. Decrypting the signature key will return the key in an active state.

In the example model presented in Figure 1, the activation of a key is assumed to be executed within the transaction signing function module. Activation and deactivation of keys are standard functions provided by most wallets. The signature key is only needed when a transaction needs to be signed. Therefore, these can be stored offline for increased security, until needed. On the other hand, verification keys and addresses are stored online as they are needed more often for verification purposes.

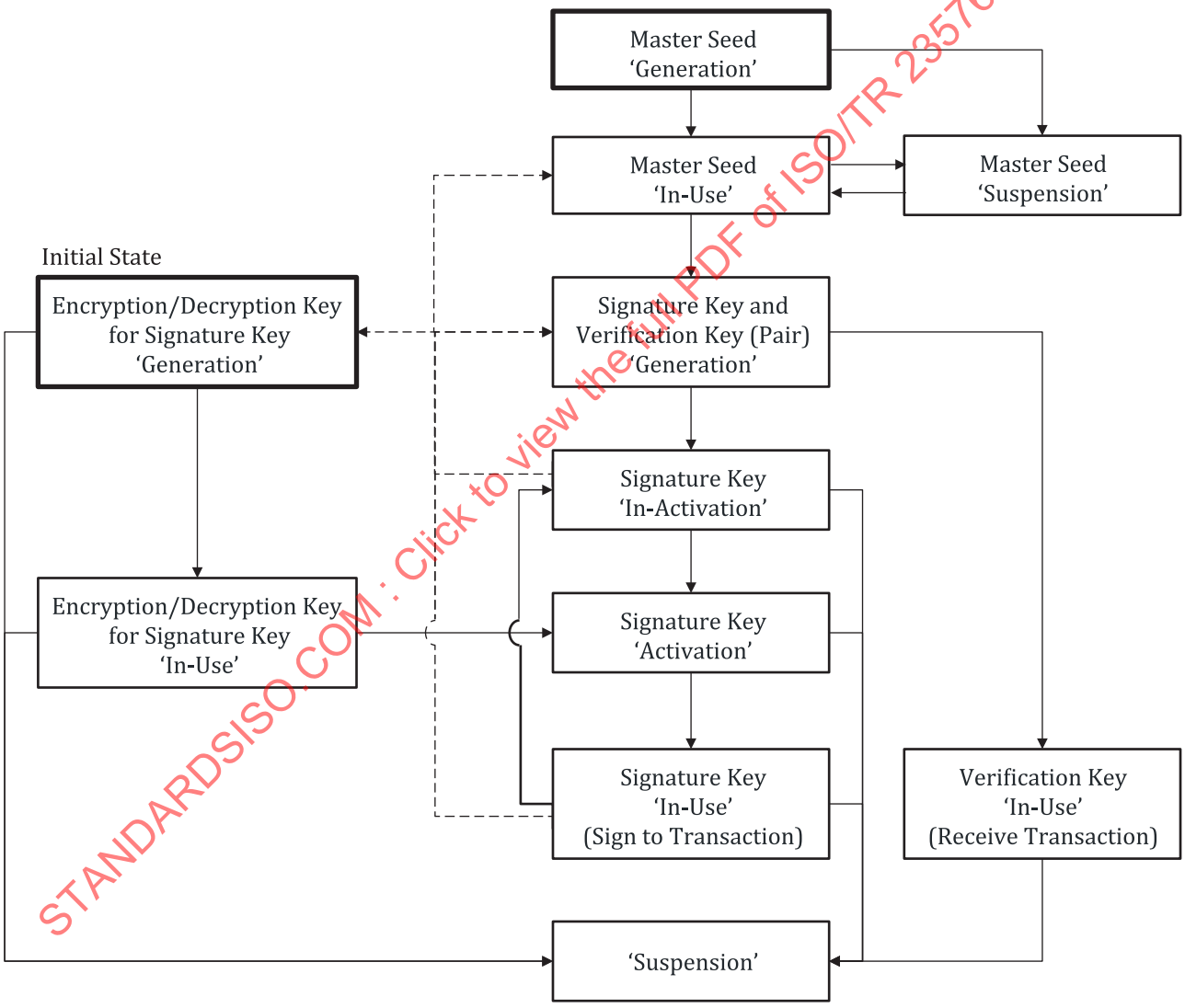

Figure 3 — Lifecycle of the signature key, verification key and encryption/decryption key for signature key in a deterministic wallet

A deterministic wallet uses a mechanism by which after generating one master seed, multiple signature key pairs are derived from it. Figure 3 shows the lifecycle of the different types of keys within a deterministic wallet. On the one hand, by backing up and restoring the master seed, all derived signature key pairs can be recalculated. On the other hand, if the master seed is compromised (i.e. stolen), all crypto assets which are managed by any of the derived keys (and related addresses) may

be stolen as well. Also, if the master seed is lost, the derived signature key pairs cannot be recalculated and access to the assets managed by these will be impossible.

An extension to the deterministic wallet model is provided by the hierarchical deterministic wallet (HD wallet). In a HD wallet, a master key pair is created from the master seed, and child key pairs are derived from the master key pair. Descendant key pairs can be derived from the child key pairs, in a hierarchical manner, hence the name of the wallet. Since child key pairs can be derived from parent key pairs, it is not necessary to access the master seed when generating the child key pairs. The possibility of using HD wallets will depend on the signature algorithm used by the digital asset in question. Therefore, for some digital assets it will not be possible to use HD Wallets.

Although this document refers mainly to the security control measures for managing signature keys, it is noted that the master seed needs an equal, if not higher, security management compared to signature keys.

5.4.3 Using multiple keys

Digital asset systems (e.g. Bitcoin) recommend or enforce the fact of not using the same key pair twice, thus producing multiple key pairs. This feature prevents easy tracking and tracing of transactions, and also protects against possible attacks on used keys, but is not relevant to the business efficiency of a digital asset custodian. Digital asset custodians, as part of the management of customers' addresses, may need to support this kind of scenario. Within a digital asset custodian, a user may have one address or multiple addresses. The number of addresses and key pairs the custodian will have to support will depend on the type and number of digital assets managed and on the method with which they are managed. For example, if a digital asset custodian is managing assets which allow inserting tags related to transactions such as Ripple or NEM, it may use only one address and distinguish different customers using the tags. On the other hand, where digital assets which cannot contain tags are managed, a custodian may use a separate address for each customer, in which case the number of addresses and key pairs would increase, or the custodian may rely on less addresses and additional balance sheets to track the ownership of assets per user, in which case potential errors or transparency issues may arise. The risk evaluation regarding the use of multiple addresses will depend not only on the type and quantity of digital assets (e.g. Bitcoin, Ethereum, etc.) but also on the use of hot and cold wallets.

5.4.4 Suspension of keys

The suspension of a key is an operation which is specific to digital asset custodians. By definition, in any DLT / blockchain-based digital asset system, no user (or system) can cancel a transaction once it has been made. Therefore, digital asset custodians are encouraged to be cautious when revoking signature keys, even after the suspension of a key. For example, if a user accidentally sends some digital assets to a suspended address, the suspended / revoked key would be needed to make the reimbursement.

5.5 Characteristics of digital assets held in DLT / blockchain systems

5.5.1 General

Digital assets based on DLT / blockchain systems have some unique characteristics compared to general information systems and also from the traditional use of signature / encryption keys. When considering the risk assessment described in Clause 8 and the security requirements and measures described therein, these unique characteristics will require particular attention.

5.5.2 Importance of signature keys

As described in 5.3, by signing and transmitting a transaction with the signature key, it is possible to transfer digital assets from one address to another. Once this transaction is written to a block in a blockchain or to a ledger in a distributed ledger, and is approved, it will not be possible to revert or revoke it. In order to remedy the transaction an equal inverse transaction would be necessary. This is in contrast with how digital payments work today, in which a payment process is completed only once settled and can be cancelled or voided before it completes.

This procedure can be followed as long as the remittance is not complete, despite typically requiring considerable administrative overhead. In addition, if a signature key were to be lost or eliminated the digital assets associated with the corresponding address would be inaccessible and could not be transferred to any other address. The irreversible nature of transactions in digital asset systems requires paying extreme attention to theft, fraudulent use and elimination of signature keys.

5.5.3 Diversity of implementations

5.5.3.1 General

There are numerous digital assets (i.e. 5 500 listed on https://coinmarketcap.com on 23/05/2020) of which Bitcoin is just one implementation. The specifications vary widely between different digital assets. For example, there are differences in the encryption algorithms and hash functions used, in the methods of generating / transmitting transactions, in the wallet implementations to protect the signature key(s), to name a few. Due to these differences in specifications, effective countermeasures for one digital asset may not be effective or even possible for another one. Also, thanks to the hype-driven trend in digital assets, the appearance of new assets, and the functional expansion and specification change of existing assets, happen at an extremely fast pace.

5.5.3.2 Cryptographic algorithms of digital assets

There have been cases in which new cryptographic algorithms, which have not been sufficiently reviewed in terms of security, have been adopted by digital asset systems. Normally, when using cryptographic technology, designers tend to use cryptographic algorithms and techniques which have been scientifically verified, mathematically proven, and approved by official authorities / agencies. Instead digital assets designers are sometimes known to adopt “immature and unverified” cryptographic algorithms. To have cryptographic algorithms proven for security and approved by official authorities / agencies requires a lot of time. This seems mostly incompatible with the blockchain / distributed ledger world in which competition is extremely high, and evolution is extremely fast, therefore technology with low maturity is often used to gain competitive advantage with respect to other digital assets. In some cases, the algorithms used have not been carefully reviewed in their implementation, and therefore, the risk of vulnerabilities being discovered at a later stage and being compromised is very high (compared to mature algorithms).

5.5.4 Possibility of blockchain forks

5.5.4.1 General

In blockchains using PoW, such as Bitcoin, in some cases a temporary fork of the chain can arise. This is mainly due to two factors: specification change of software (i.e. the blockchain client), or the reorganization which takes place during normal operation. Instead, in other cases, for example due to the division of the developer community around a digital asset, a blockchain can be divided at a specific point in time, and form two completely separate chains (i.e. hard fork) from then onwards, which most of the time are operated as different digital assets entirely (e.g. Bitcoin and Bitcoin Cash). In the digital asset world, various forks have already been executed and it may be difficult to adapt or respond to all of them and each fork may introduce separate risk factors to be countered.

5.5.4.2 Rolling back due to reorganisation

When re-organisation of a chain occurs the orphan blocks and transactions are discarded. In this case, the transactions which are discarded, as a consequence of the reorganisation, will not be reflected in the main chain. This is one of the reasons for which a transaction in Bitcoin is considered truly confirmed after it has passed a least six blocks. Note that transactions that have been discarded due to a fork can still be included in subsequent blocks.

5.5.4.3 Handling forks of digital assets

As mentioned previously, there have been real-world examples of hard forks in which the two resulting chains have been managed separately and as a different crypto asset. This has happened both with Bitcoin and Ethereum. The forked coin is derived from the same underlying technology as the original coin, but sometimes new features or changes are implemented in the forked chain therefore it is not always compatible with the original one.

The two chains, until the fork, are identical (i.e. contain the same exact data and history of transactions). This exposes the forked chain to replay attacks. A replay attack is an attack in which transactions used in the original digital asset chain are retransmitted to the sender of the transaction in the forked chain (which will exist thanks to the shared history), or vice versa, therefore illegally acquiring digital assets. To countermeasure these attacks, monitoring techniques can be used to prevent these types of transactions.

Also, if the fork occurs on a digital asset held by a custodian, the user may not have access to the forked digital asset (of which they will have the same amount as the original) unless the custodian supports the forked digital asset and assigns it to the user.

5.5.5 Risks for unapproved transactions

5.5.5.1 General

The action of signing and transmitting a transfer transaction to a DLT / blockchain node does not instantly reflect the actual transfer of the assets. In order to approve a transaction, the transaction needs to be stored in a block or ledger record which is created at set or variable time periods (e.g. average of ten minutes for Bitcoin), and then the block needs to be accepted by the majority of mining nodes. 5.5.5.2 and 5.5.5.3 provide some examples of cases in which a transaction may not be approved.

5.5.5.2 Handling unapproved transactions

Various implementations of digital assets (e.g. Bitcoin, Ethereum, etc.) which use a blockchain or a distributed ledger allow or require a fee to be specified when transmitting a transaction. The transaction fee is rewarded to the miner that creates the new block or ledger record containing that transaction. The higher the fee the more interesting it is for a miner, and therefore the higher the probability of the transaction being approved as soon as possible (i.e. in the first new block or ledger record). If a low or even null fee is sent with the transaction it may take a long time to get approved, or there is also a possibility in some cases, that the transaction will never be approved at all. In addition to transaction fee related issues, temporary forks, as described in 5.5.4.2, can produce transactions which are never authorized and are dropped (i.e. orphan transactions). Finally, double spending attacks can create a second transaction which causes the first original transaction to not be approved.

In scenarios where digital asset transfer is required immediately, such as payment for goods in a store, it may not be possible (or desirable) to wait for a transaction to be approved, and therefore it might be necessary to take the risk of accepting unapproved transactions.

5.5.5.3 Transaction failure due to vulnerabilities from digital assets specifications and implementations

Although not technically a case of unapproved transactions, in earlier versions of Bitcoin there was a vulnerability called transaction malleability. This vulnerability allowed malicious nodes to manipulate submitted transactions, effectively changing their transaction ID, and then retransmitting them with a different transaction ID, trying to make this transaction approved before the original one. This has the effect that the sender will not be able to find the original transaction ID and could be inclined to send the same amount again, effectively paying double. It is important to point out that this attack is performed after the transaction is transmitted to the chain, therefore the sender has no way of preventing this. The Bitcoin network has introduced a protocol upgrade called segregated witness, which solves this vulnerability. So, although this vulnerability is no longer present, it highlights an important issue, which

is the fact that security threats will not always be addressable by the custodian in its role of sender or receiver but might depend on vulnerabilities in the protocols of the digital assets they have in custody.

6 Basic objectives of security management for digital asset custodians

The basic objectives of a security management system for digital asset custodians are to establish, maintain and continuously improve a security-providing environment for the assets they protect. Items described in ISO/IEC 27001:2013 can be considered as general requirements for a security management system applied to the processes of a digital asset custodian. More specifically some key aspects are recommended to be taken into careful consideration due to the nature of the services provided by a digital asset custodian:

— Stakeholders (see ISO/IEC 27001:2013, Clause 4)

Protection of customers' assets is of paramount importance, especially given that these may include customers' private keys. This requires a well-defined and well-understood division of responsibilities between the customer and the custodian.

— Security policy (see ISO/IEC 27001:2013, Clause 5)

A security policy which includes security objectives and controls, as described in the following clauses, is a key objective for digital asset custodians. Disclosure to customers of the security policies related to digital asset management can have a beneficial impact and facilitate self-evaluation.

— Continuous risk evaluation and improvement (see ISO/IEC 27001:2013, Clauses 6, 8, 9 and 10)

Continuous risk monitoring specific to digital assets in addition to aligning the general security management framework is considered best practice, because risks change and increase frequently due to the rapid development of the underlying technology as described in 5.5.3.

7 Approaches to basic security controls

The following viewpoints are considered to be most relevant when formulating security objectives and controls for digital asset custodian systems:

— countermeasures to loss, theft, leaks, and general abuse of customers' asset data and signature keys;

— business requirements;

— compliance to laws and regulations;

— social responsibilities to prevent crimes such as the use of digital assets for scams and / or money laundering.

Security controls commonly used by digital asset custodians include:

— conducting a threat analysis;

— conducting a vulnerability and risk evaluation;

— defining security objectives and controls according to their actual business and systems.

Security objectives and controls are typically decided keeping in mind threats and risks specific to digital assets described in Clause 8, as well as general security objectives and controls described in ISO/IEC 27002:2013.

The following is a list of security objectives and controls described in ISO/IEC 27002:2013:

— information security policies;

— organization of information security;

— human resource security;

— asset management;

— access control;

— cryptography;

— physical and environmental security;

— operations security;

— communications security;

— system acquisition, development, and maintenance;

— supplier relationships;

— information security incident management;

— information security aspects of business continuity management;

— compliance.

Taking the above items into account is of paramount importance.

Clause 8 describes issues which are specific to digital asset custodians.

8 Digital asset custodians' risks

8.1 General

The main risks related to digital asset custodians can be divided into two main categories: risks related to the system / platform of the digital asset custodian, and risks caused by external factors such as a DLT / blockchain protocol outside the control of the custodian. The risks related to the system / platform of the digital asset custodian are organized in terms of threats, factors, and actors that pose a threat. The risks related to external factors such as DLT systems / blockchains or misuse are organized in terms of possible incidents and / or threats. There might also be risks which are inherent to systems and operations which will be different for each custodian.

Overall risks are identified based on both the "general" risks described in this clause, and the specific risks brought by the specific systems and operations each business operator (i.e. custodian) will have. After identifying all risks, it is desirable to determine the priority of the control measures, by evaluating the impact each threat can have on the business.

8.2 Risks related to the system / platform of the digital asset custodian

8.2.1 General

This subclause describe the typical risks to the asset data held by the digital asset custodian system. With reference to the basic model illustrated in Figure 1, and focusing on the protection of customer assets, it is particularly important to safeguard the signature keys used in the transaction signing function, and the asset data itself. If the signature keys and their surrounding environment are not secure, it is possible for a malicious entity to create malicious transactions using legitimate signature keys and transmit these transactions to the DLT / blockchain. Once a transaction is sent to the DLT / blockchain and has been validated, it cannot be cancelled, even if it was created maliciously. Therefore, it is widely accepted that implementing protective measures to prevent theft and / or misuse of signature keys is of utmost importance. Additionally, best practices indicate it would be necessary to carefully evaluate all risks and vulnerabilities related to the management of signature keys and design and implement appropriate safety countermeasures. In addition to the fraudulent use of signature

keys, the eventuality of the loss of a signature key is another risk which is considered relevant. When a signature key is lost it is impossible to access the digital assets stored in the addresses corresponding to that key. Risks related to signature keys, which refer to the signature transaction function (based of the basic model in Figure 1), and the surrounding environment will be discussed in 8.2.2

Regarding the asset data itself, since the contents of the data, the format of the data, and the management of the data vary considerably from custodian to custodian, this document will rely on a general abstract model. Typical contents for asset data might be the total amount of digital assets and fiat currency deposited by the customer, the amount of digital assets and fiat currency held by the custodian, customer account numbers, customer addresses, etc. In line with common practices in similar systems, this data is considered extremely important, as if such data were overwritten or manipulated by a malicious entity, it would cause potential damage to customers and / or impede the operation of the custodian system. The risks associated with asset data are discussed in 8.2.3.

In addition to protecting important information such as transaction signature keys and asset data, it is also necessary to consider risks such as system outages, so that customers can always be able to have access to their assets. Risks related to system outages are discussed in 8.2.4.

Finally, risks inherent to each individual custodian system and risks related to cooperation / use of external business operators are also relevant.

In general, it is recommended to conduct a detailed risk assessment of the actual digital asset custodian's system implementation.

8.2.2 Signature key risks

8.2.2.1 General

As previously mentioned, the unique characteristics of DLT systems / blockchains make signature keys extremely powerful as in most cases they have total control over an account. Moreover, seen as most crypto-asset systems provide at least some degree of anonymity, and as transactions are not reversible, the risks are even more severe. In this subclause, the risks of fraudulent use, which could lead to the loss, leakage or theft of the keys and damage of values, are discussed. Also, supply chain risks are considered, for example when introducing a wallet to manage signature keys.

8.2.2.2 Risk analysis on signature keys

Risk analysis may depend on the assumed threats, system configuration, threat modelling, and so on. A case study is presented below, based on the threats, factors and components described in Table 3 as an example.

Table 3 — Threats, factors, and components regarding signature keys

Threats	Factors of threats	Components involved
— Loss — Leakage, theft — Fraudulent use	— Human error — Legitimate users' malice — Spoofing — Intrusions from outside — Unintended behaviours arising from implementations	— Custodian operation modules — Transaction signing modules — Customer asset management function implementation — Incoming transaction management function implementation

Factors of threats are intended as follows:

Human error: An act that an authorized user (including an administrator) of the system accidentally performed. For example, an operation to transfer $ 1 000 is incorrectly executed for $ 1 000 000.

Legitimate users' malice: Acts performed by a legitimate user of the system (including administrators) with malicious intent (i.e. internal fraud). For example, theft or unauthorized use of another user's or customer's signature key. This subclause focuses on identifying acts that can be seen as factors, but the purpose and objectives of these acts are not taken into consideration.

Spoofing: An act in which an unauthorized user impersonates a legitimate user (or more accurately some kind of authorized operation). For example, an internal user without administrator privilege accesses the system with administrator authority.

Intrusions from outside: An act in which an external user accesses the system maliciously in a manner other than spoofing. For example, by using malicious intrusion techniques from the outside by exploiting the system's vulnerability. Examples of such techniques are incorporating malware into the custodian environment via targeted email to the custodian operators, generating and using private signature keys from outside the system, allowing remote access to the system.

Unintended behaviours arising from implementations: The system behaves unexpectedly irrespective of the intention or malice of the operation; for example, a signature key leaks due to a bug in the custodian key management system.

It is assumed that theft and fraudulent use in general are regarded as threats that can only be caused by explicit malicious factors. Taking these factors into account the possible risks related to the private signature key are collected in Table 4.

Table 4 — List of risks related the management of signature keys

Risks	Factors of risks	Loss	Leakage	Theft	Fraudulent use
Unauthorized operation (with legitimate path)	End-user's / customer's malice	×	×	×	×
	Custodian operator's malice	×	×	×	×
	Spoofing of end users / customers	×	×	×	×
	Internal frauds (spoofing of operators)	×	×	×	×
Intrusion from the outside	Intrusion into the transaction signing modules	×	×	×	×
	Intrusion into the incoming transaction management function (implementation)	×	×	×	×
	Intrusion into the customer asset management function (implementation)	×	×	×	×
	Intrusion into the exchange operation modules	×	×	×	×
Risk of system unintended behaviours (not depending on human operations)	Unintended behaviours of the transaction signing modules	×	×	○	○
	Unintended behaviours of the incoming transaction management function (implementation)	×	×	○	○
	Unintended behaviours of the customer asset management function (implementation)	×	×	○	○
	Unintended behaviours of the exchange operation modules	×	×	○	○
Human errors	Error of end user	×	×	○	○
	Error of operator	×	×	○	○
Key					
○ risks does not exist					
× risk exists					

8.2.2.3 to 8.2.2.6 describe each risk, while their security controls are shown in 9.3.

8.2.2.3 Risks of loss of signature key

Table 4 describes a list of events in which there is a possibility of causing the loss of a signature key. Loss of a signature key can be the result of deleting the digital entry representing the key or losing access to the key (e.g. losing the hardware wallet containing the key or losing a decryption key associated to an encrypted storage of the signature key). A typical example of loss of a signature key is an erroneous operation by a system administrator.

8.2.2.4 Risk of leakage and theft of signature key

An intentional malicious action is a key example, but leakage can be caused also by negligence without necessarily intent. For this reason, leakage risk and theft risk are considered as separate risks. The leakage risk shown in Table 4 lists events that have the possibility of causing leakage including negligence. Typically, internal fraud, unintentional behaviour, hacks, etc. can be considered events which can lead to leakage.

Instead, the theft risk enumerates only events that occur due to malicious intentions. There are two main types of theft, either by an internal user (i.e. internal fraud), or through unauthorized intrusion from the outside (i.e. hack).

Both leakage and theft risks are similar in the outcome, as sensitive information is compromised, therefore the control measures are common, which are described in 9.3.2.

8.2.2.5 Risk of unauthorized use of signature key

The risks associated with unauthorized use shown in Table 4 are events which are caused by the unauthorized use of a signature key by a malicious person. Examples of such events are spoofing of an authorized person or intrusion into the system.

The unauthorized use of a signature key could also be caused by an unauthorized operation of pre-processing of an unsigned transaction in addition to the direct unauthorized use of the signature key by an individual.

The following examples show unauthorized use of signature keys at an early stage of the process.

— A destination address for digital asset transfer or the amount of assets to be transferred is manipulated due to software tampering in the transaction signing function module. For example, the tampering can disable the validation processes in the transaction signing function module.

— A destination address for a digital asset transfer or the amount of assets to be transferred is manipulated due to tampering of the unsigned transaction, which is generated by the transaction generator module. The unsigned transaction is then normally sent to the transaction signing function module.

— A destination address for digital asset transfer or the amount of assets to be transferred is manipulated due to software tampering in the transaction generator module. An unsigned transaction is generated due to an unauthorized direct operation on the transaction generator module.

— An incorrect amount or incorrect destination address for digital assets is transmitted from the custodian operation function module to the transaction generator module due to internal fraud, a human error, or by spoofing the identity of the administrator.

— The assets database is tampered with in a case where the operation/order of the transaction generator module refers to the assets database. See 8.2.2.

These examples show how an attacker would be able to obtain digital assets without attacking the signature key directly. Particular countermeasures are necessary in cases where the system automates even just a part of its processes.

Security control measures are necessary to protect the signature key. Moreover, security control measures of the entire custodian's system are necessary in order to mitigate these complex risks. Security control measures are discussed in Clause 9.

8.2.2.6 Other risks — Hardware wallet (supply chain risk)

So-called hardware wallets are products providing solutions for managing signature keys using a hardware device. Most hardware wallets connect to the management terminal (i.e. PC, laptop, etc.) via USB and are used to perform key management operations. FIPS 140-3 is one of the most common security certifications used by products which provide key management functions. Since some cryptographic algorithms used by digital assets have not been subjected to certification, unfortunately the third-party accreditation system results are inadequate for the security of hardware wallets for digital assets. For this reason, while there are hardware wallets with sufficient security on the market, it is necessary to recognize that there are also products with insufficient security. Furthermore, even when hardware wallets have a sufficient level of security, this might be impaired along the supply chain between manufacturing and distribution. For example, a hardware wallet could be loaded with malware during the distribution / sales phases. In this case, even if a purchaser generates a new signature key in the hardware wallet, the attacker through the malware could obtain or destroy the key.

8.2.3 Risks on asset data

The asset data is data which is used to manage assets such as digital assets and fiat currency held by customers and custodians. The signature key is normally not kept with the asset data (see 5.2).

As mentioned previously, since asset data varies between custodian and custodian, an abstract model will be considered in this document. Good practice is performing both a detailed threat analysis and risk assessment on the asset data managed by the actual custodian system.

The main threats to the asset data are considered to be data tampering, loss, or leakage. The factors include human error by an operator, internal fraud, spoofing of a legitimate user, being hacked, and unintended behaviour of the system. In the example of the basic model provided in 5.2, a route exists from the exchange management system, through the customer property management system, to the incoming asset determination unit. Among the different threats to the asset data, the following examples are considered incidents caused by data tampering.

— A customer asset management system referring to manipulated asset data may create an “illegal” transaction and flow through the normal process and onto the DLT / blockchain (8.2.2.5). Some examples of data which can be tampered with can be the amount of assets held for an account or the destination address for the digital asset transfer.

— Manipulation of the “meta” data that is not part of the DLT / blockchain hash, such as the block state in the consensus protocol, or the voting data on a transaction verification, can provide risk to the asset data.

— An incident in which a malicious transaction which is generated using manipulated asset data is transmitted through a legitimate process. (See 8.2.2.5)

— Tampering of the records holding the amount of assets held in accounts, which are stored in the asset data module. These assets could be related both to customers and to the custodian system. One kind of tampering is to modify the list of digital asset addresses linked to a client. This effectively results in the client losing assets, without a transaction being transmitted to the DLT / blockchain.

Risks related to the asset data may be considered the same as the risks of a traditional financial service and settlement service system. However, it is highly advisable that specific countermeasures for incidents in which transaction(s) have been transmitted to the DLT / blockchain and approved as a result of unauthorized manipulation of the asset data are considered, remembering that once a transaction is sent to the blockchain and approved it becomes irreversible.

8.2.4 Risks related to suspension of systems and operations

8.2.4.1 General

A digital asset custodian system consists of software, hardware, network, and so on. In addition, the term "operation" refers to an operation performed manually by a user, such as the operation of account opening, executing a payment instruction, wallet deposit / withdrawal operations, monitoring a switching centre system, etc. The system and related operations may be stopped or forced to stop due to various factors. Risks related to the suspension of systems and operations can be regarded as problems similar to the ones in general financial and payment systems.

However, there are also some potential differences such as the fact that digital asset custodian systems are connected to the internet all the time, are operating 24 hours a day, 365 days a year, and are often built on the public cloud infrastructure. Also, the conditions of operations of a digital asset custodian system can have a large effect on the exchange rate of digital assets, and therefore they tend to be a target of attack.

8.2.4.2 Risks related to network congestion

Digital assets custodian systems are frequently the target of denial of service attacks. Publicly available web pages, API endpoints, etc. are common targets for denial of service attacks. When a business system or operation monitoring system is reachable through the internet, these kinds of attacks are highly probable and therefore become truly relevant, even more so, if an attacker knows the system configuration.

8.2.4.3 Risk of system outage

It is possible for the data centre, the cloud infrastructure, etc. where the system is installed to go down and / or become unreachable, stopping the system and operations. Various factors could produce such an effect such as a power outage due to a natural disaster, large scale failures of cloud or telecommunications operators, failure of software releases, etc.

8.2.4.4 Risks related to operators

Even if the system itself is operational, if operations monitoring and more in general, tasks of personnel responsible for the operation of the system are hindered, the custodian service will effectively be suspended. The following are some potential reasons for such cases: regular inspections of power facilities at operation bases, disruption of transportation due to natural phenomena or strikes, protest activities and consequent mass aggregation of press reporters may hinder the entrance and exit of buildings.

In addition to the previous examples, when personnel of a custodian system are using the same transportation method or are participating to the same event, there is a risk that many of them will be involved in the same event such as traffic accident or food poisoning.

8.2.4.5 Regulatory risks

The company which runs the digital asset custodian system, will be subject to laws and regulations, based on the country and jurisdiction where it operates. There are risks associated with the possibility of not being able to operate due to receiving a business improvement order, business suspension order, deletion of registration, suspension, revocation of license, etc.

8.3 Risks from external factors

8.3.1 General

This subclause illustrates the cases in which the systems and operations of the digital asset custodians are working correctly, but either the DLT / blockchain system or the network in which the digital asset

operates and the internet infrastructure supporting the connection between the nodes are attacked. In such a case, the service provided by the custodian system cannot be provided or at least the transactions cannot be handled properly.

8.3.2 Risks related to the internet infrastructure and authentication infrastructure

8.3.2.1 Internet routing and name resolution attacks

Possible risks in this area include the possibility of an attacker interfering with the routing of the internet and DNS, hindering the reachability of the digital asset custodian system, and potentially redirecting users to a fake custodian service and / or DLT or blockchain system. It is also possible to intentionally cause a DLT / blockchain branch by hindering synchronization between nodes. These types of attacks can be carried out not only by a malicious attacker, but also from an ISP (or similar provider) based on instructions from a government.

8.3.2.2 Attacks on web PKI

Most digital asset custodian systems provide service through the web. TLS and server certificates are used for the encryption of sites and the verification of authenticity of the web site by the users. Due to an attack on a certification authority which issues server certificates it may be possible to impersonate the original custodian site. Alternatively, server certificates can be revoked and therefore the service cannot be provided as browsers would not allow the user to reach the custodian (or at least warn the user).

8.3.2.3 Attacks on messaging systems

Attackers can target email, SMS, or other equivalent messaging systems, in order to block or intercept messages for users, like for example one-time passwords used for authentication and authorization. An attacker can use these kinds of attacks and impersonate a user, and for example login and change the password.

8.3.3 Risks inherent to digital asset DLT systems / blockchains

8.3.3.1 Split or fork of a DLT / blockchain

A DLT / blockchain might be forked due to specification changes which have not reached consensus amongst the developer community. When a fork occurs there are two cases that can arise: the first is that the last transaction before the fork is executed and recorded in both ledgers after the fork; the second is that the last transaction before the fork is executed and recorded in only one ledger.

8.3.3.2 DLT / blockchain reorganisation caused by 51 % attack or selfish mining

When a block or ledger record which is committed in the past is discarded, the transaction included in the discarded block or ledger record might be rolled back. The transaction included in the discarded block or ledger record is disabled, and digital assets or fiat money paid in compensation for the transaction might be swindled.

8.3.3.3 Compromising cryptographic algorithms and hash functions

The continuous advances in computing and / or the discovery of an effective attack might allow to compromise the cryptographic algorithms and hash functions which are at the base of blockchains and DLT systems.

8.3.3.4 Inadequate DLT / blockchain specifications and implementations

Attacks can be carried out by exploiting specific vulnerabilities which can be found in some implementation of blockchain and DLT. These attacks usually are only specific to one implementation. The following are some real uses cases of attacks carried out on live systems.

One example of exploit leveraged bug in the consensus algorithm of the blockchain, which made it possible to send fake transaction information (e.g. fraudulent timestamps) to specific nodes, which allowed to mine a lot of digital assets "illegally". A real-life example of this exploit was the so-called "timewarp" attack carried out on the Verge network in 2018, which leveraged a timestamping related vulnerability in the PoW algorithm used.

Another example of exploit, focused more on disrupting a network, is the one carried out on the Lisk blockchain. In this case the implementation allowed to specify a timestamp with a numeric value which was out of the range permitted by the internal database of the system. Nodes receiving these transactions could not process them, which effectively meant that block generation stopped [3]. This issue was fixed in several hours, by updating the client software, and the network recovered. However, the blockchain was not able to process transactions for several hours.

Exploits leveraging inadequate implementations of smart contracts are also a risk factor. An example of this was the case of the ERC20 Ethereum-based Beauty Chain Token (BEC), which led to the collapse of value of the token. The exploit leveraged a vulnerability caused by an overflow in the smart contact that regulates the token, which allowed to generate a number of tokens which greatly exceeded its upper limit, making its value collapse[4].

8.3.3.5 Rapid change in hash rate

When the hash rate increases or decreases rapidly in a blockchain, it might take a very long time to generate new blocks using the remaining nodes.

8.3.4 Risks arising from external reputation databases and anti-money-laundering regulations

8.3.4.1 Establishment, elimination, and deactivation of bank accounts

Due to AML / CFT regulations, in some jurisdictions there are cases in which banks refuse to open bank accounts related to the activity of a digital asset custodian. Even when an account has been opened, it is subject to the risk of being deactivated or eliminated, due to instructions from the regulatory authorities. In the event of an account deactivation or suspension it will not be possible for users to deposit or withdraw fiat currency through the digital asset custody system.

8.3.4.2 Digital asset addresses

Due to AML / CFT regulations, when a user of a digital asset custodian system transfers assets to another digital asset address, in some cases checks are performed on the destination address, to assess if it is a high-risk transaction. In the case in which the destination address is registered as a "problematic" address, it is highly unlikely that the transaction will be performed smoothly. Since it is common practice for criminals to use known addresses to try to launder / hide stolen assets, it may happen that an address at a digital asset custodian system is classified as high-risk by mistake.

8.3.4.3 Filtering and blocking for web sites

There is a risk that the URL of the digital asset custodian is filtered by the network or blocked by the ISP making it unreachable for users. Also, if it is erroneously recognized as a malware distribution site or similar, there is a risk that it will not be displayed as a search result or it will be impossible to browse from the browser.

8.3.4.4 Email

As a measure against spam emails, most email servers provide mail rejection based on reputation and classification of incoming emails. If the email delivered by the exchange is judged as spam, it may be impossible to contact the user.

8.3.4.5 Appraisal of a smartphone application

Depending on the app platform used and jurisdiction, there are cases in which handling digital assets in an app is restricted. Also, if the smartphone application is not approved by the platform, the user may not be able to download it and may be therefore unable to use the service.

8.3.4.6 ID theft

A common type of attack is impersonating a legitimate user (spoofing). This is usually done by list-based attacks, which allow the theft of IDs, passwords, or other credentials such as API access tokens, or by malware infection or social engineering.

The main purposes of spoofing attacks are theft of fiat currency or digital assets by means of unauthorized withdrawals, money laundering by means of cashing digital assets with an account in someone else's name, and profit shifting by means of market manipulation obtained with unauthorized purchases and / or sales of digital assets.

9 Consideration on security controls of digital asset custodians

9.1 General

This clause describes considerations from an ISMS viewpoint on implementing security controls for digital asset custodians, related to the risks highlighted in Clause 8.

Building on the best information security practices, all the security controls in this clause follow the guidance provided in ISO/IEC 27001:2013 and ISO/IEC 27002:2013. The main area of focus for custodian systems is on strong controls for the management of signature keys for digital assets.

Other relevant security controls are mostly like the ones in the traditional financial sector, for example, to name one, storage of PII. ISO/IEC 27001:2013 and ISO/IEC 27002:2013 indicate that security controls are to include concrete content from the results of risk analysis and vulnerability diagnosis. Cyber security threats are always changing, therefore constant reviews of security controls, according to situations, are important.

9.2 and 9.3 contain considerations on the security controls, which include references to the appropriate existing ISO standards (ISO/IEC 27001:2013 and ISO/IEC 27002:2013) and how they relate to these standards. Issues caused by the specific characteristics of digital assets managed by a blockchain or distributed ledger are included.

9.2 Basis for considerations about security management

Standards on requirements for information security already exist, namely ISO/IEC 27001:2013 and ISO/IEC 27002:2013. Digital asset custodian systems can refer to the requirements and / or guidance in these standards and can consider which security controls are needed.

Based on the referenced standard, it is good practice for custodians to establish, implement, maintain, and continually improve their security management.

Digital asset custodians hold data related to customer's assets, their own assets, customer's information, and signature keys.

Security management best practices suggest that all this data should be protected from leakage, loss, tampering and misuse.

Additionally, the risks associated with loss of assets due to foreign factors such as DLT systems / blockchains or networks, due to suspension of the system or of its operation become relevant factors. The following are the main areas of consideration for security management for a digital asset custodian.

— Interested parties (from ISO/IEC 27001:2013, Clause 4): Protect the assets of the custodian's users. Segregation of duties for the digital asset custodian's operators, especially for the management of signature keys. Impacts on the business due to regulatory issues such as money laundering are also to be considered.

- Policy (from ISO/IEC 27001:2013, Clause 5): ISO/IEC 27001:2013 mandates digital asset custodian to establish an information security policy which includes information security objectives and controls. The information security policy could be made public so that users are able to read it.
- Continual improvement and risk assessment (from ISO/IEC 27001:2013, Clauses 6, 8, 9 and 10): As described in 8.3.2, a large number of digital assets have been developed to date, and the speed at which these digital assets evolve is very rapid. The referenced standards mandate that digital asset custodians monitor security risks which are specific to digital assets in addition to the general information security management. Therefore, reviewing and improving security controls periodically and / or according to a specific situation, are considered good practices for a digital asset custodian.

9.3 Considerations about security controls on digital asset custodians

9.3.1 Guidelines for the information security management

Objectives for security management for a digital asset custodian contain protection of customers' assets, compliance to business requirements, abiding to laws and regulations, and realization of social responsibility. The security policies and execution statements derived from such objectives are recommended to be made publicly available for consumers, business partners, auditors, and regulators.

Security objectives and controls are typically based on the aspects listed below:

— risk management options to counter the loss, theft, leakage and misuse of signature keys, customer data and customer assets;

— compliance with business;

— legal and contractual compliance.

In 9.2 there are some considerations about security controls based on system risks for a digital asset custodian system. ISO/IEC 27002:2013 contains guidance on security controls, and therefore digital asset custodian systems can refer to it to design and / or identify their security controls. 9.3.2 to 9.3.14 refer to ISO/IEC 27002:2013 and describe items which are considered particularly relevant for a digital asset custodian system.

9.3.2 Information security policies

The information security policies can be defined to follow ISO/IEC 27002:2013, Clause 5. The main security objectives for digital asset custodian systems are protection of the customer's assets, satisfying business requirements, compliance with legal and contractual requirements and social responsibilities. Information security policies on the other hand include policies on access control (9.3.6), cryptographic controls (9.3.7), operations security (9.3.9) and communications security (9.3.10).

9.3.3 Organization of information security

For the organization of information security, digital asset custodians can refer to ISO/IEC 27002:2013, Clause 6, where it explains how to establish a management framework to implement and operate information security. ISO/IEC 27002:2013 mandates that digital asset appoint relevant engineers and other types of staff, who have the right credentials and / or appropriate knowledge and skills, to

oversee the consideration of threats such as illegal acquisition of signature keys and illegal creation of transactions. Also, segregation of duties, mainly with respect to the management of signature keys and the creation of transactions, is another key area of relevance.

9.3.4 Human resource security

For human resource security, digital asset custodians can refer to ISO/IEC 27002:2013, Clause 7. ISO/IEC 27002:2013 suggests that in order to examine and evaluate security controls effectively, a digital asset custodian should deploy human resources with expertise not only in information security applied in general but also in digital assets and DLT / blockchain technology. ISO/IEC 27002:2013 also indicates that all employees who may handle assets, should receive appropriate education and training and regular updates in organizational policies and procedures.

9.3.5 Asset management

For asset management, digital asset custodians can refer to ISO/IEC 27002:2013, Clause 8. Digital asset custodian systems contain all the information to manage the assets they hold, and information on the users (operators, and customers), and of their assets, such as signature keys. If hardware wallets are used within the system, security controls suitable for risks related to this practice would become relevant. Also, for the protection of customers' assets, segregation of assets (customers' and custodians') is considered good practice in compliance with accounting practices. AML regulations require that the real owner of a digital asset must be identified as part of a KYC process.

9.3.6 Access control

9.3.6.1 General

For access control, digital asset custodians can refer to ISO/IEC 27002:2013, Clause 9. Users are separated into two main types: authorized operators (and administrators) and customers. Some considerations on operators and administrators are written in 9.3.6.2, while considerations on customers are written in 9.3.6.3.

9.3.6.2 Access controls for operators and administrators

There are two different kinds of operators and administrators:

— operators and administrators for the custodian system; they execute commands to create keys or accounts and / or to transfer funds by software or terminal;

— administrators which maintain hardware, OS, databases, and middleware.

Management of signature keys with operations such as activation, backup and restore are described in 9.3.7.

Digital asset custodian systems, typically, to operate correctly, assign proper authority to users and implement access control. Access control regulates authorizations and permission for users to connect to the custodian system remotely, for external services which interact with the digital asset custodian system, and for administrators who need to operate on the infrastructure, operating systems, databases, terminals, etc. Access control also defines permissions to enter and leave the facilities. Some policies may be used to restrict access such as allowing access only during office hours or in predetermined time slots, whitelist specific IP addresses for specific terminals / servers, require confirmation by operators using credentials, for connections to predetermined terminals. Roles and authority are also typically set for operators and administrators of each system. Setting access control for operators and administrators to the minimum required in order to run the permitted functions or software, and not only to access applications, is considered a best practice.

The risks and consequences of data manipulation, human errors, and malicious attacks on transferring assets or on signature keys are described in 8.2. To counter these threats multiple approvals / confirmations can be put in place, so that no operator or administrator on their own can perform

important operations such as transferring assets or managing signature keys. Therefore, duties are distributed amongst several individuals and not centralized on one.

9.3.6.3 Access control for customers (user authentication / API)

— A robust KYC process may need to be carried out when a new account is setup on all users who will be accessing the system, and credentials are sent to each user individually. For example, during KYC an official personal identification document is often collected, and communications are generally sent to a verified address (electronic and / or physical). KYC processes are influenced by relevant law, regulations, and conventions such as FATF. Manipulation of photos or data on identity documents are typical threats for personal identification / KYC. KYC processes require to verify identity documents following a dedicated process to mitigate the threats.

— Multi-factor authentication is being used increasingly within the traditional financial sector to prevent spoofing and internal fraud, also due to increasing regulatory requirements (e.g. Directive (EU) 2015/2366 – PSD2). Multi-factor authentication can protect against leakage of single credentials. Risk-based authentication can be used to highlight abnormal usage such as different IP addresses, different terminals, different time slots, etc. A common practice, for example, is to send one-time-password's, as an additional factor, to the user via SMS. Emails tend not to be used for this purpose, as they provide a higher risk of interception, re-routing, and impersonation. Also, app-based multi factor authentication is becoming increasingly popular. ISO/IEC 29115:2013 is a relevant standard for this topic.

— Multi-factor authentication and risk-based authentication are recommended when registering a customer and setting access control, to protect against spoofing fraud being carried out on the customers' funds, such as converting digital assets to fiat money and withdrawing it, or money laundering. ISO/IEC 29115:2013 is a valuable reference for this aspect.

— Different levels of authentication can be used depending on the risk of the operation carried out, in order to find the correct balance between the safety of the services provided and the customer's convenience and user experience when using the services. For example, a low risk operation such as displaying the balance of an account, or the details of a transfer may require only single-factor authentication. On the contrary, transactions which transfer assets, or make changes to accounts or addresses might require multi-factor authentication. In addition, operations with an even higher degree of risk, such as cashing out assets, or fiat transactions might require an additional authentication and / or further confirmation by an operator. Indications found in ISO/IEC 29115:2013 are truly relevant to this aspect.

— Data preservation techniques can be used when deleting a digital asset custodian account, to allow rollback of the operation if a customer declares his account was spoofed. Therefore, a digital asset custodian can delete an account if request by the customer but can also take into account the risk that the request was illegitimate.

— It is advisable to preserve signature keys even on discontinued addresses. Therefore, a signature key linked to an address which holds no value, is not deleted. An address could receive some digital assets from outside the custodian system, and a customer may therefore want to reuse that address. Signature keys for unused accounts can be backed up so they can be restored if necessary.

— Access control is an important factor not only for accessing functions and services through the web browser but also through APIs, which could be used by an application on a smartphone or other external systems. The provided APIs might have to take into account cases in which it is difficult to obtain an explicit approval from the customer. Best practices shared in the financial industry represent a relevant guidance on risks specific to APIs, of which Financial API by OpenID Foundation is an example.

9.3.7 Security controls on signature keys

9.3.7.1 General

ISO/IEC 27002:2013, Clause 10 can be used as a reference for compliance. Some security controls for signature keys, which are an issue specific to digital asset custodians, are closely related to controls in other subclauses in this clause (e.g. 9.3.6). In some cases, it is advisable to keep digital assets stored in hot wallets to a minimum and isolate the rest to a more secure storage solution, which could be for example a cold wallet.

The minimum amount is considered to be the one which can be temporarily paid to the customer, while the rest of the assets are recovered from the secure storage. Digital asset custodians can refund the customer from the secure assets even in case of a theft or leak in the hot wallet. Research suggests that a digital asset custodian system would need to choose and use the appropriate cryptographic technology for securing signature keys, ideally, one which has been evaluated by third parties in accordance with the purpose of use, as is done in general information systems. The life cycle of signature keys is considered a key issue to address, and therefore also implementing and operating appropriate controls.

9.3.7.2 Basics of key management

In general, the following is considered fundamental for the management of signature keys:

— isolation from other informational assets in the system;

— rigorous access control;

— limitation to the minimum possible, of the number of accesses to the signature keys;

— plan for unintentional loss of a signature key.

The following are three basic security controls which illustrate how to implement the above considerations. Additional security controls, specific to digital asset custodians are described in and after 9.3.7.3.

a) State management of signature keys

As described in Figure 2, a signature key has one of multiple states, and it may be in an active or inactive state. The signature key needs to be in an active state when it is being used for signing or decryption. It is recommended to enforce the use of some secret information (i.e. passphrase), which needs to be inputted, to activate an inactive key. This technique helps to protect the signature key from abuse, as an attacker would need to know the secret in order to activate the key. Therefore, this method enhances the security of the signature key and helps prevent from its misuse by unauthorized parties. It is also recommended to minimize the time a signature key is active for, to limit the risk of abuse. Unnecessary and / or prolonged activation of the signature key increases the risk of abuse, leakage, and theft, but is more efficient from a business and customer experience point of view as it requires less frequent activation / deactivation. Therefore, it is important to consider the trade-off between the risks and business efficiency / customer experience and provide a clear key management policy to customers.

b) Administrator role separation and mutual checks-and-balances

Role separation and mutual checks-and-balances are a fundamental form of operation for a critical business process which uses signature keys to perform cryptographic operations on behalf of multiple parties, in order to prevent internal frauds and errors. For example, by setting up a process in which an operation requires multiple signatures and / or approvals to be executed, it becomes difficult for an attacker to try and perform an operation without a third-party noticing. At the same time, the enforcement of the presence of another operator / administrator is an effective security control for internal fraud and human error.

c) Backing up signature keys

The loss of a signature key makes any operation with that key impossible, therefore making a backup of a signature key is an important security control. On the other hand, risks of leakage and theft of backup keys is also a relevant point. Security best practices indicate that backup keys are to be kept in an inactive state. Another security control which can be implemented is to monitor DLT / blockchain addresses to detect illegal use of little-used addresses and unauthorized recovery of backup keys.

9.3.7.3 Detailed control in terms of backup

Backup is considered to be the most fundamental and effective measure against the loss of the signature key. On the other hand, there are risks of leakage and loss related to backup devices. These risks depend on the kind of backup device used, thus also the security controls will depend on which device is used. Also, issues deriving from long-term storage of backups, are a relevant topic for consideration. The following are some examples of leakage/theft risks associated with typical backup devices and mechanisms:

— Cloning to tamper-resistant key management device

If a signing key is managed by a tamper-resistant key management device (device X) and X has a cloning function, cloning the key to another device Y is a good practice for the backup of the key. Cloning is a technique to copy the key, from X to Y, whilst keeping the key confidential from any other device. It is recommended that the implementation of the cloning function be evaluated/ certified by certification program like CMVP or FIPS 140. Note that, the cryptographic algorithms supported by such tamper-resistant key management devices are limited and not all digital asset systems support them, but it is one of the most secure ways of performing a backup.

— Backup to storage for digital data

It is assumed that storage for digital data are storage devices such as USB memory sticks or optical media such DVD, or hard drives. There are two main types of backup operations in this context; the first involves the data to be backed up on a movable device which is offline (i.e. USB stick), the second involves the data to be backed up on a device which is available online (i.e. backup server). If the device is easily movable, the possibility of theft and loss increases, thus, according to best practices, it would ideally be kept in a cabinet or a vault with a key, and the access to such cabinet / vault would be restricted. If the backup storage is online, the risks of leakage and theft are the same as the ones in the key management function module inside the digital asset custodian system. Therefore, in general the same security control is applicable for the backup storage. If there are some additional layers of security, such as the fact that the backup device is not active except for when a restore operation is being executed, the security controls may be modified with respect to the actual operating environment. In situations where it cannot be avoided that the raw key data is kept outside of the key management function module in the custodian system, the fact that it is possible to recover data from magnetic storage devices even if it has been deleted, is another risk to take into consideration.

— Backup to non-digital medium

Signature keys can be backed up offline on non-digital mediums. For example, keys can be printed to paper as a QR code or other machine-readable mechanism. Paper is moved more easily compared to traditional storage for digital data and is easy to identify. This method introduces other risks of leakage and theft, like for example the possibility of taking a photo of the piece of paper with the QR code.

— Secret sharing scheme

Signature keys can be backed up by dividing them into multiple parts, then managing them with multiple isolated systems. To be reconstructed, all parts of the key need to be re-united. Secret sharing is used also on the actual keys themselves not only for backups as described in 9.3.7.5.

9.3.7.4 Offline key management

There is a type of offline key management (known as "cold wallet") which isolates signature keys from the system network to prevent leakage and theft caused by intrusion.

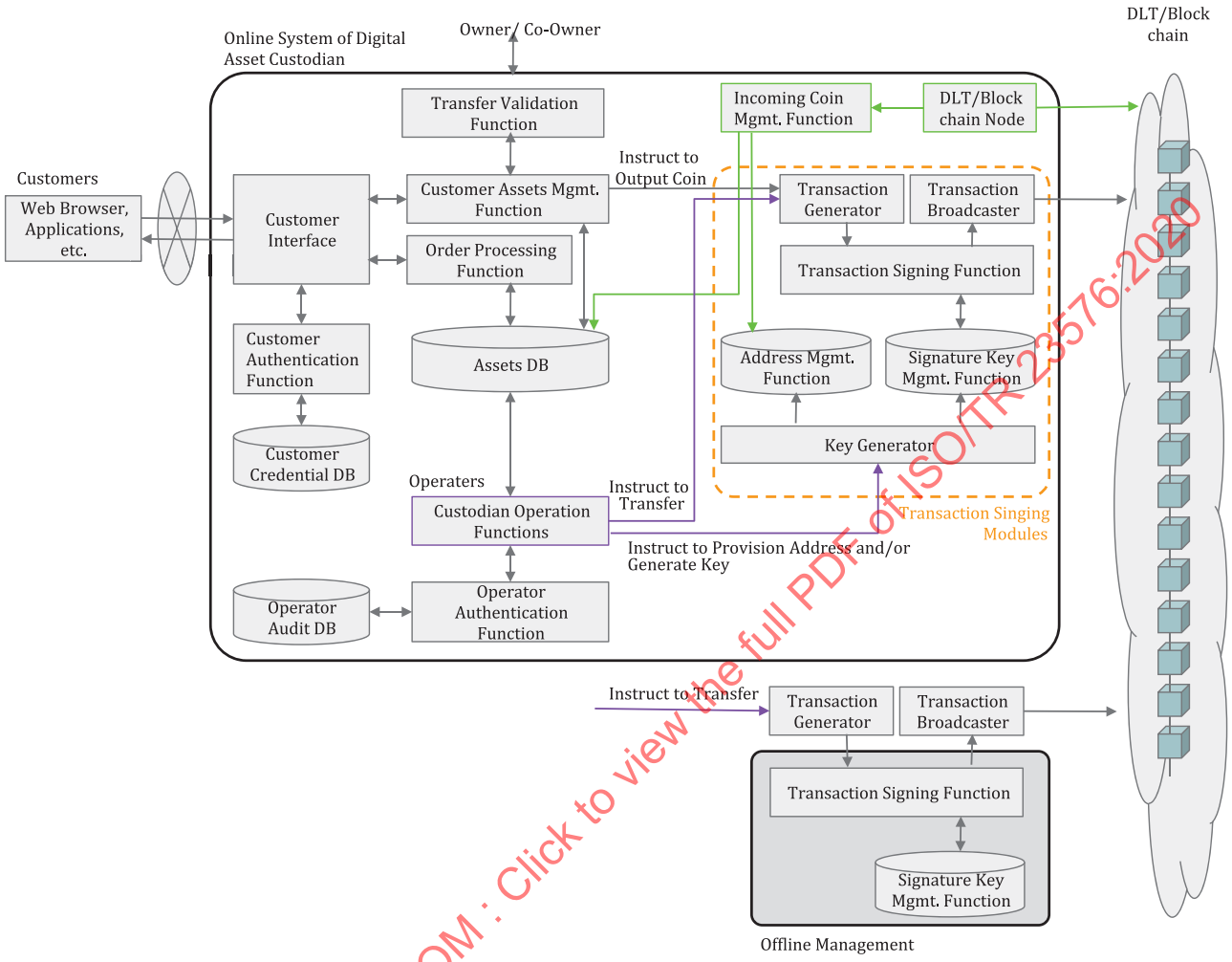

Figure 4 — Example of offline management of signature key

In this scenario, an offline interaction is needed to allow the system to use the key. For example, the keys can be stored in a "vault" within a secure USB device, which will be connected to the system only when needed. The USB channel is used to transport data between the online and offline system. Without an explicit approval process of the offline operation of the key management, it is not possible to avoid malicious transactions. Offline management can prevent loss and theft, but an explicit approval process is needed to prevent abuse of keys.

9.3.7.5 Key sharing and multisignatures

It is also good practice for security control to distribute the right to use a signature key or account to multiple entities. The following are some examples:

— Secret sharing

  Dividing the signature key into multiple parts, then managing them with multiple isolated systems is an effective measure to protect the keys against leakage and theft. This document does not recommend a specific technique but recommends implementing this control based on a certain level of security, like the one provided by a secret sharing scheme. In this case, secure coding,

penetration tests and vulnerability assessments are required to eliminate the vulnerabilities related to the implementation.

— Multisignature

Multisignature (known as multisig) is a signature scheme which requires multiple isolated signing keys to sign a message for it to be valid. Normally so-called N of M schemes are used where at least N out of M possible signers have to sign. This is an effective method of protecting each key, which is held by a different entity, as each key cannot be used on its own. There are many different implementations of multisig mechanisms, and they vary between different digital assets systems. Therefore, if a digital asset custodian service supports multiple different digital assets, the system will have to deal with complexities of supporting multiple implementations which interact with each other.

— Threshold signature scheme (TSS)

Threshold cryptography is cryptographic primitive for the generation, management and use of distributed keys, which leverages multi-party computation concepts. In a TSS a number of signers M is defined, and a threshold N smaller than M. For a threshold signature to be valid, at least N signers must sign a transaction with their signature key. TSS is an off-chain mechanism, like secret sharing, but one main difference is that there is no single signature key which needs to re-assembled. Each actor has his own TSS signature key and only the sum of N of M signatures will produce a valid signed transaction. The fact that it is managed off-chain, means it can be used also in distributed ledger systems and blockchains which do not have a native support for multisig. TSS is a relatively recent technique, therefore has not had as much testing and peer review as older more consolidated ones but is gaining a lot of popularity in the sector.

9.3.7.6 Procurement of hardware wallet

If using a hardware wallet as part of the digital asset custodian system, it is recommended to use a product whose technical security is guaranteed. An example of such a product is an HSM, which is a specialized hardware component commonly used for existing PKI services. However, some of these products may not be usable in a digital asset custodian system, as they might not support the kind of cryptographic algorithms used by a digital asset.

Therefore, when using a hardware wallet, it is important to pay attention to the following considerations, to mitigate the potential technical deficiency:

— obtaining hardware wallets from trusted suppliers;

— always applying the latest firmware and patches provided by the manufacturer;

— it is not recommended to use the default settings without careful consideration;

— initializing and generating keys autonomously if possible.

— it is recommended that users receive best practice guidance in the use of the hardware they are provided, as incorrect use can result in vulnerabilities being exposed;

— making sure the software which interacts with the wallet for signing is trustworthy, especially if multisig or offline signatures are supported.

Additionally, if the custodian only uses hardware wallets available in the marketplace, it is generally advisable to manage them according to 9.3.5. To minimize the risk of hardware wallets containing malicious code, vulnerabilities, or bugs, it is considered best practice to ensure they are subjected to third-party or independent security certification schemes. If introducing software wallets from a third party (i.e. integrating a third-party software wallet), they also could contain malicious code, vulnerabilities, or bugs, therefore a similar approach to the one used for hardware wallets is commonly adopted.