Workgroup: Network Working Group
Internet-Draft:
draft-vcgtf-crypto-assets-security-considerations-07
Published: 16 December 2020
Intended Status: Informational
Expires: 19 June 2021
Authors: M. Sato (SECOM IS Lab.), M. Shimaoka (SECOM IS Lab.), H. Nakajima, Ed. (Mercari)

General Security Considerations for Cryptoassets Custodians

Abstract

This document discusses the technical and operational risks of cryptoassets custodians and its security controls to avoid the unintended transactions for its customers.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/cgtf/draft-crypto-assets-security-considerations.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document gives guidance as to what security measure should the cryptoassets custodians consider and implement to protect the asset of its customers. The management of the signature key for cryptoassets especially has different aspects than other types of information systems and requires special attention.

This document reports especially on the appropriate management of the signature key by the cryptoassets custodians to avoid the unintended transactions for its customers.

The document organizes recommendations for considering security as a purpose of protecting users' assets by operators of cryptoassets custodians. Among the assets to be protected, in particular, the signature key of the cryptoassets has a different characteristic from the conventional information system and needs attention. Particular emphasis is given to points that should be kept in mind for the cryptoassets custodians to properly manage the signature key and to prevent illegal transactions that the customer does not intend.

The basic model of the cryptoassets custodians system covered in this document is shown in Section 5. A system in a form different from this basic model, for example, a system where an operator manages a signature key provided by a user (e.g. online wallet), is handled in another complementary document or later revision of this document.

2. Scope of this document

An operator covered by this document is a cryptoassets custodian that manages the signature key used in the cryptoassets. Including the case where the management of the signature key is entrusted to another custodians operator. In that case, even for operators entrusted with the management of signature key, a considerable part of the recommendation indicated in this document is considered to apply.

This document includes considerations on threats and risks for the following subjects.

* A cryptoassets custodians system that provides cryptoassets custodians work to customers (consumers and other exchanges)

* Assets information managed by the cryptoassets custodians system (including the signature key of the cryptoassets)

* The social impact which can be exerted by imperfect security measures of the cryptoassets custodians system

This document does not focus on the following items.

* Security measures for information systems used by daily operations by custodians operators

* Security measures against blockchains that provide the mechanism of cryptoassets and distributed ledger itself

* Operator's own management risk

* Specific requirements on separation of assets of customers and custodians/exchanges

3. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Terminology

Terms used in this document are defined in [I-D.nakajima-crypto-asset-terminology]

5. Basic description of a model system of a cryptoassets custodian

5.1. General

In this section, a model of a cryptoassets custodians system that is used to explain the concepts and provisions in this document are explained.

5.2. A basic model of cryptoassets custodians system and its functional components

Followings are the basic model of a crypto assets custodian that this document deals with. A basic model of cryptoassets custodians system is shown on Figure 1.

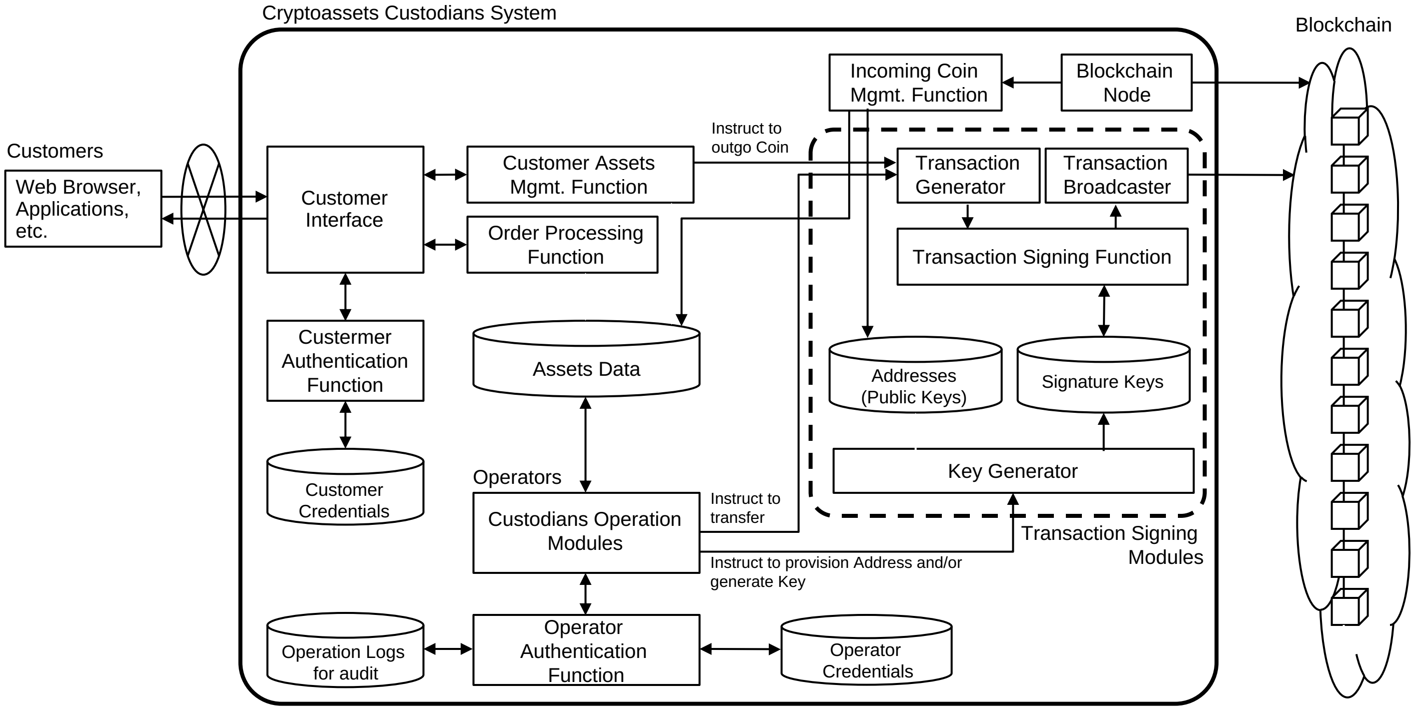

Figure 1: Basic Model of Cryptoassets Custodians system

*Interface (Web Application, APIs) Provides screen and input functions such as login process, account management (deposit/ withdrawal instruction etc.) and trade instruction for the customers(users). Web application, API, etc.

*Customer Authentication Function Performs user authentication process for login to the cryptoassets custodians.

*Customer Credentials Manages required IDs for login and verification information related to user authentication process (e.g. password verification info.).

*Customer Assets Management Function A group of functions to manage customer accounts. Receive instructions for deposit or withdrawal (outgoing coins) and perform processing according to the user instructions. Retrieve or update assets data.

*Blockchain Node Connects to another blockchain nodes to retrieve blockchain data.

*Incoming Coin management Function Checks transaction stored in blockchain and confirm whether incoming coins are involved in the specified addresses. Update an assets database according to the transaction from blockchain.

*Order processing function A group of functions that receives orders from customers and performs processing related to trading of cryptoassets. Retrieves and updates assets data based on the orders.

*Assets Database Manages holdings of fiat currencies and cryptoassets. The database does not include the private keys for transaction signature. Assets are managed separately from the assets of the custodian for each customer.

*Transaction Singing Function

- -Transaction Generator Generates transactions to be sent to the blockchain based on instructions from the customer asset management function or the custodians operation function.

- -Transaction Broadcaster Broadcasts the signed transaction to the blockchain. Connects to other nodes on the blockchain.

- -Transaction Signing Function Generates digital signatures based on the instructed transaction contents and the signature key (or its IDs and its addresses).

- -Address Management Manages public keys with related to the signature keys, or addresses (such as values calculated from the public keys).

- -Signature Key Management Function Manages the signature keys of the cryptoassets (keys used for signing the transaction). Sometimes signature keys are separately stored into the cold-wallet as security countermeasure.

- Signature key generator Generates signature keys. The generated keys are registered in the signature key management function, and the public keys and addresses are registered in the address management function.

* Custodians Operation Modules A group of functions for custodians' operators or administrators. Based on operations from administrators, the module instructs generating new signature keys or transferring cryptoassets.

* Operator Authentication Function Authenticates the administrators.

* Operator Audit Database Manages auditing data related to the authentication of the administrators.

We defined each functional element to distinguish functions logically, and do not show the actual arrangement on the actual system. For example, in our actual system, the address management unit may be managed by an integrated database. Also, there are implementations with multiple functions packaged together. For example, each functional element of the transaction signature system may be integrated with the customer property management system, or the transaction signature system may be operating as another system.

When using existing implementations such as bitcoin wallet, bitcoin wallet is thought to provide the functions of the transaction signature system as just one implementation as a whole. It is also conceivable that some functions are provided by a remote subcontractor as in a form in which the function of the transaction signature system is provided by a remote server.

5.3. The flow leading to the sending of the transaction

* Deposit Phase

1. Customers send fiat to custodian's bank account.

2. Custodians shall confirm to receive fiat, and shall update assets database to reflect customer asset information.

* Input coin phase

1. Customer transfer cryptoassets to the address instructed by custodians. The transfer shall be made by cryptoassets wallet for the customer such as tools or services (other custodians or Web wallet)

2. Custodians shall confirm cryptoassets has been transferred to the address instructed and shall update the asset database to reflect asset information of the customer.

*Trading phase

1. Customer access to interfaces to make instructions.

2. Instructions to transfer shall be processed by custodians operations functions. The result of trade processed by custodians operations functions shall be updated into the asset database.

*Instructions to output coins from customers

1. Customers access to interface and instruct it to transfer its cryptoassets to other address. (Instruct to output coins)

2. Instructions to output coins shall be processed by customer assets management functions. Transaction generator shall make transaction messages based on instructions such as receive address or amount of cryptoassets.

3. Transaction messages shall be added a digital signature by transaction signing functions.

4. Transaction messages with a digital signature shall be delivered to all nodes on blockchain by transaction broadcaster.

*Instruction to transfer from Customer Assets Management Function

1. Administrator instructs to send cryptoassets to address through the interface of Management Functions. For Example, it may send between address managed inside custodians.

2. Instructions to transfer shall be processed on Management Function, and shall be processed as described 2 to 4 on "output coin". Transactions with digital signature shall be delivered to all nodes on blockchain.

5.4. Types of keys that are used for signature and encryption

5.4.1. Type of keys

Types	Description
Signature Key	A private key for signing transactions (asymmetric key cryptography)

Types	Description
Verification Key	A public key for verification of transactions (asymmetric key cryptography). Recipient address of transactions are the unique value calculated from verification key
Encryption/ decryption key for signature key	Secret key used to keep signature key (symmetric key cryptography) confidential / protected
Master Seed	A seed, e.g. random number, to generate a signature key in deterministic wallet

Table 1: Type of keys

5.4.2. Flow for the key generation and key usage

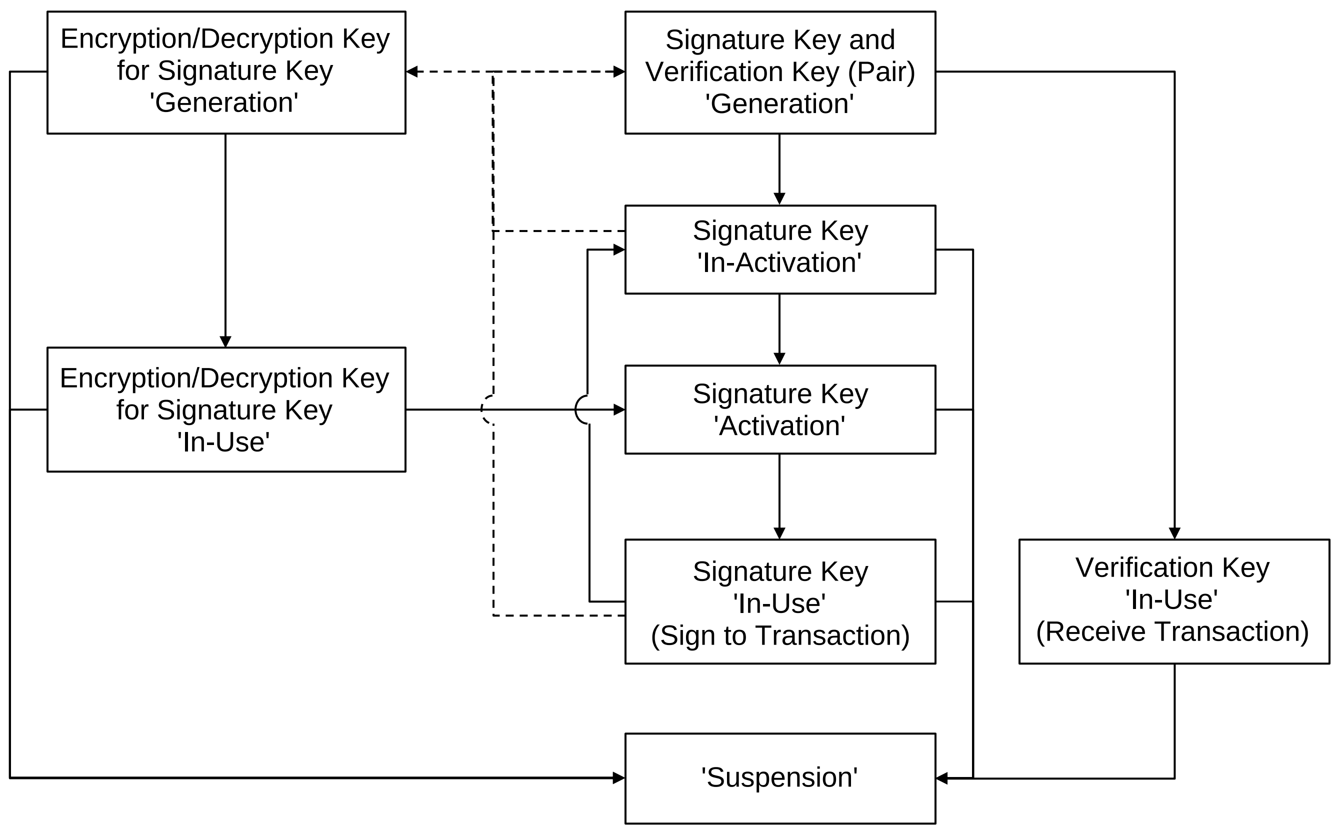

Figure 2: Lifecycle of signature key, verification key and encryption/ decryption key for signature key

After a pair of keys (signature & verification, hereafter "key pair") is generated, an addressed to receive transaction is derived from the verification key. By providing a sender of digital assets this address, the sender is able to transfer one or more assets to this address. When the recipient transfers the assets to another address, the original recipient signs the transaction data which includes the transfer order.

A signature key is considered to be in an inactive state when it is stored in a confidential manner (ie. cannot be directly used to sign), for example within the key management function in Figure 1. An example of how to set a signature key in an inactive state is to encrypt the signature key using an encryption key (ie. passphrase).

The opposite process of decrypting the signature key will return the key inactive state. The activation of a key is assumed to be executed within the transaction signing function in Figure 1.

Activation and deactivation of keys is part of the function set of certain wallets.

The signature key is not needed after its generation until a transaction has to be signed. Therefore this allows for the store and manages signature keys offline while keeping the verification key and addresses online (See: Section 7.3.6.2).

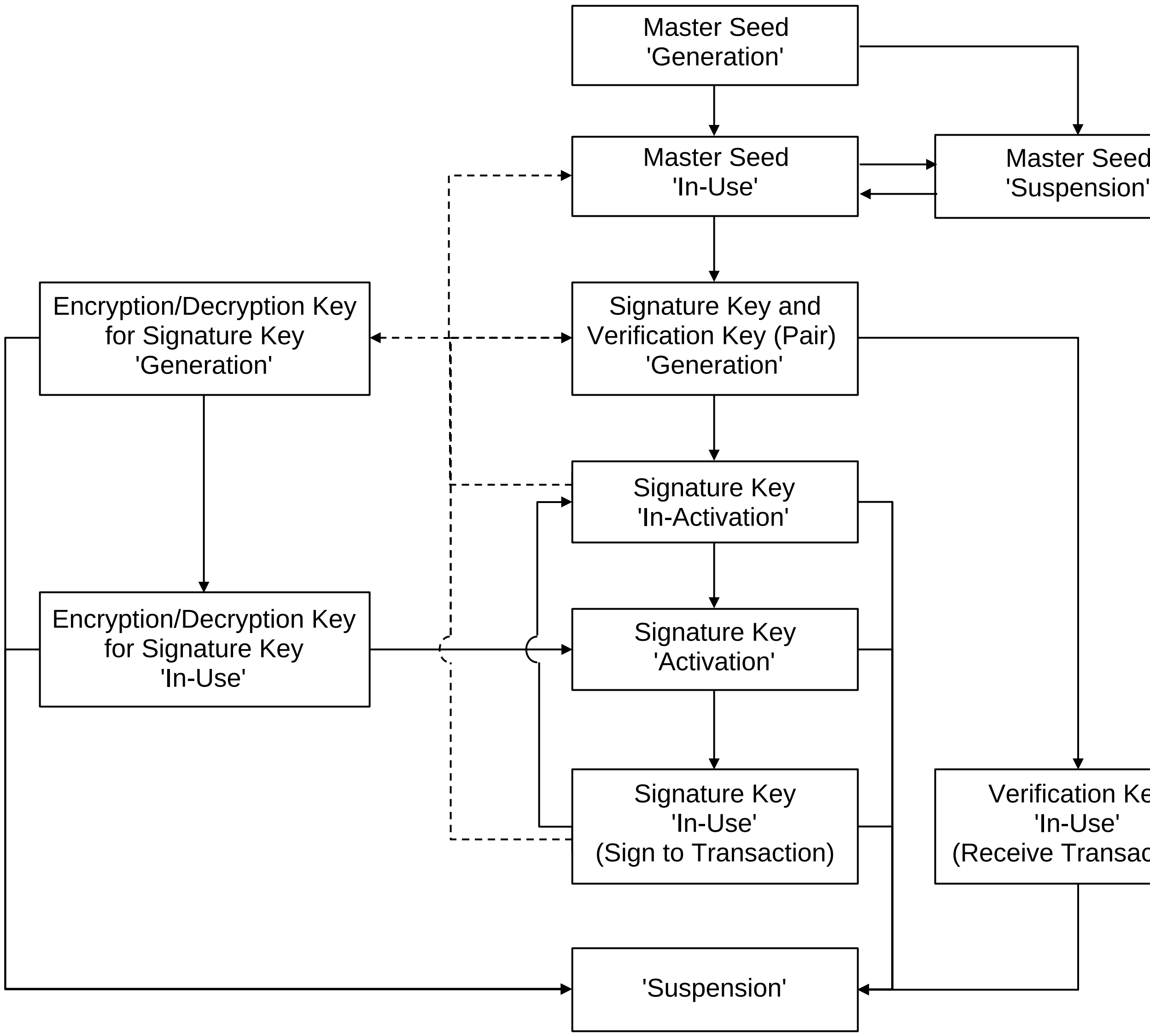

Figure 3: Lifecycle of signature key, verification key and encryption/ decryption key for signature key in case of deterministic wallet

The deterministic wallet is a mechanism that generates one master seed and generates multiple signature key pairs from that master seed. It is possible to regenerate each signature key pair from the master seed by backing up the master seed and restoring it. On the other hand, if the master seed is stolen, the crypto assets which are managed by all signature key pairs (and addresses) derived from the master seed may be stolen. Also, if the master seed is lost, all signature key pairs will not be able to be regenerated.

As an extension of the deterministic wallet, there is a hierarchical deterministic wallet (HD wallet). In the case of HD wallet, a master key pair is created from the master seed, and child key pairs are derived from the master key pair. Furthermore, descendant key pairs can be derived from the child key pairs in a hierarchical manner. Since the child key pair can be created from the parent key pair, it is not necessary to access the master seed when generating the child key pair. The implementation of hierarchical key pair generation depends on the signature algorithm, and some currencies cannot be realized in principle. Although this document refers mainly to the management of the signature keys in the security control measures, the master seed also needs security management equal to or higher than the signature keys.

5.4.3. On the use of multiple keys

There are some cases to use cryptoassets where one user uses one address, one user uses multiple addresses. The number of addresses and pairs depends on the number of cryptassets and method of management. For example, cryptoassets that can contain tags related to the transaction such as Ripple and NEM, cryptoassets custodian may distinguish customers by each tag if custodian uses one address. On the other hand, cryptoassets that cannot contain any tags for transactions, custodians have to make addresses for each customer, so the number of addresses and key pairs would be increased. It is considered to use multiple addresses and key pairs by risk evaluation with not only a variety of cryptoassets (e.g., Bitcoin, Ethereum, etc.) but also management by the hot wallet and cold wallet.

It is recommended not to reuse key pair for general. But it is focussed for anonymous transactions by private use, so this is not suitable for custodians from viewpoint of efficiency and practicality. Cryptoassets custodians shall make effective controls considered by risk evaluations and control objective.

5.4.4. On the suspension of keys

Even if Figure 2 indicates operations on operations of custodian, cancellation of transaction cannot be made for cryptoassets. Also, it is difficult to revoke the signature key after suspension of using keys. For example, it may happen to input coins to the address user has suspended to use. To return coins to the sender, custodian needs a signature key for the suspended address. cryptoassets custodians shall assume those cases, and shall consider about revoking signature keys carefully.

5.5. Characteristics of cryptoassets in blockchain and distributed ledger

5.5.1. About this section

In the handling of cryptoassets using blockchain / distributed ledger, there are things to emphasize and different characteristics compared with general information systems and usages of private/encryption keys. In considering the risk assessment described in Section 6 and the security requirements and measures based thereon, it is necessary to pay attention to these characteristics.

5.5.2. Importance of signature keys

As described in Section 5.3, by signing transactions using the signature keys, it is possible to instruct the transfer of the values of cryptoassets to other addresses. Once this transaction is written to the block or ledger data and the transfer of the values of cryptoassets is approved it is difficult to revert it or to invalidate the transfer by revocation procedure etc. This property is in contrast to taking time until the remittance gets caught or the process can be canceled during remittance and be reassembled, even if it requires complicated administrative procedures in the process of remittance, and illegal remittances occur. In addition, when the private signature keys have vanished in the cryptoasset scheme, there will be a case that the cryptoasset held by the address corresponding to the signature private key is impossible to transfer to the other. In cryptoassets having such irreversible nature, it must pay attention to the theft, fraudulent use and disappearance of the signature secret key.

5.5.3. Diversity of implementations

There are various cryptoassets including Bitcoin. The specifications also vary widely from cryptoassets to cryptoassets. For example, there are differences in the using of encryption algorithms, hash functions, the methods of generating/spreading transactions, and wallet implementations to protect the signature key(s), and so on. Due to these differences in specifications, effective countermeasures for a specific cryptoasset may not be able to be carried out under the specification of another cryptoassets. And also, from the current feaver trends of the cryptoassets, the appearance of new cryptoassets and the speed of functional expansion and specification change of existing cryptoassets mechanisms are very fast.

5.5.3.1. Cryptographic algorithm of cryptoassets

There are cases that new cryptographic algorithms in cryptoassets that are not sufficiently reviewed for security may be adopted. In ordinary use cases of cryptography technology, designers often use cryptographic algorithms that are scientifically verified, mathematically proved secure, and approved by official authorities/agencies, however, cryptoassets designers are often adopting "immature and unverified" cryptographic algorithms. This means that it takes time to archive provable security for algorithms and approve by official authorities/agencies, while in the blockchain where competition and evolution are remarkable, the maturity level is low as technology, and differentiation and blocking from other cryptoassets. It must be optimized the technology specific to the chain. These algorithms are likely to have no properly reviewed implementation, or the risk of a vulnerability being discovered later and compromising (compared to mature algorithms) is high.

5.5.4. Possibility of blockchain forks

In the blockchain using Proof-of-Work and the like typified by bitcoins, a state such as a temporary fork of a chain due to specification change of software or a single chain of branched chains (re-organization) can arise. Also, as another case, due to the division of the developer community, blockchains are divided from the point of time and sometimes operated as separate cryptoassets. In the real world, there are various forks, it may be difficult to respond to all of them, and it should be consider countermeasures according to the risks.

5.5.4.1. Rolling back due to re-organization

If the chain is discarded due to a reorganization, the history of transactions contained in the discarded chain will be lost. In that case, the transaction on the block discarded within the reorganization period may not be reflected in the main-chain.

5.5.4.2. Handling forks of cryptoassets

As in the case of bitcoins and ether symbols, blockchains are divided and sometimes managed as another cryptoassets (here, called a fork coin). The fork coin is also derived from the same software as the original cryptoassets and uses the same technology and compatible technology (A description that incorporates the case where different technologies are adopted for a fork is necessary). In addition, the chain until just before splitting has exact identical data. By using its functionality, it becomes possible to attack, for example, replay attacks. A replay attack is an attack in which transactions used in the original cryptoassets are retransmitted to the sender of the transaction at the fork coin chain and the fork coin is illegally acquired as a result. In this kind of replay attacks, countermeasures such as monitoring of the transaction sender, for fork coin chain, measures to be sent before transactions that return coins to their own other address are required.

In addition, if a fork coin occurs in the cryptoassets held by the exchanger, there is also a problem that the fork coin is not returned to the user unless the fork coin is assigned to the user of the exchanger in the exchange system.

5.5.5. Risks for Unauthorized Transactions

5.5.5.1. About this section

Just by sending the transaction instructing the transfer of the coins(assets) to the node of the blockchain does not instantly reflect the cryptoassets transfer. In order for a transaction to be approved, it is stored in a block created every decided period and needs to be accepted by the majority of mining nodes. It may be difficult to confirm that the transaction has been approved for the following reasons.

5.5.5.2. Handling unapproved transactions

In a cryptasset using a distributed ledger, there are a variety of cryptoassets (such as Bitcoin, Ethereum, etc.) that the transaction sender sends transactions with a transaction fee. This transaction fee is acquired by the miner who creates the block, and the higher the transaction cost, It is easy to store in blocks (transactions are easily approved immediately). If the cost of the transaction sent from the cryptoassets custodian to the blockchain is low, it may take times to approve the transaction, or there is a possibility that the time will expire without being approved. Besides the case due to the transaction fee, the temporary chain fork as in Section 5.5.4.1 can be occurred that the transaction that should have been approved once becomes the unapproved state and the dual spend of cryptoassets. In usage scenes where cryptoassets transfer is required immediately, such as payments in real stores, it may be difficult to take time to confirm the approval of the transaction, and it is necessary to assume the risk of unauthorized transactions.

5.5.5.3. Transaction failure due to vulnerabilities from cryptoassets specifications and implementations

Although it is not exactly the case of unauthorized transactions, there was a vulnerability called transaction malleability as a past case of bitcoins. With this vulnerability, if the node relaying the transaction is malicious, it is also possible to make transactions illegally manipulate, thereby making it impossible to find the transaction stored in the block (make it impossible to search by transaction ID). There is also the possibility of an attack that makes a duplicate by requesting transmission of the cryptoassets again from the counterparty by making the approved transaction appear as not approved. This attack is performed after sending the transaction to the nodes, so it is characteristic that the sender can not take measures beforehand before sending. Regarding transaction malleability, it is now possible to avoid it by using SegWit in bitcoins. However, as a lesson from this case, effective defense measures cannot be made effective only with the cryptoassets custodian that becomes the sender or receiver of the cryptoassets with respect to faults and threats due to another vulnerability of bitcoins and other cryptoassets.

6. Risks of cryptoassets custodian

6.1. About this chapter

Below in this section, some risks custodian shall consider for the system and for foreign factor outside of control from custodian such as blockchain is described. The risks for systems in custodians are listed as a threat, factor, and actor may cause threat. The risks for foreign factor outside of control from custodian such as blockchain are listed from the incident. Some risks may be caused by property or quality described in Section 5.5.

On the other hand, there are some risks based on operations or systems implemented by each custodians. Custodians shall pick up risks to deal with control to refer these risks with understanding with system or operation of custodian. Custodians shall evaluate impacts may be affected by risks and shall decide controls and its priority.

6.2. Risks of cryptoassets custodian system

In this section, major risks regarding information asset which cryptoassets custodian system holds are listed. Among the fundamental model shown in Section 5, the signature key and asset data are focused as significant information asset to protect customers asset.

The attacker may be able to broadcast a malicious transaction to nodes of distributed-ledger after generating the transaction if the signature key and surrounding environment are not safe.

Withdrawing transaction is almost impossible once the malicious transaction has been broadcasted and built into the blockchain. Therefore, prior countermeasures to prevent generating malicious transaction are essential.

Moreover, consideration of a loss of signature key is also essential. Cryptoassets stored in the address associated with the signature key become unavailable in a case where the signature key has been lost.

Risk regarding the signature key including the signature key and surrounding environment are mentioned in Section 6.2.1 based on Figure 1.

In this document, the model is described as more abstract as the content of data, data format, management model or details of processing regarding asset data varies among custodians. Record such as client assets (both cryptoassets and fiat currency), assets of custodians(both cryptoassets and fiat currency), clients' account information, or address of cryptoassets is listed as common content of asset data subject to protection. Manipulation to those asset data caused by the attacker results in damage to client assets or affect to the custodians' operation. Risks related to assets data are discussed in Section 6.2.2.

Risks of system outage MUST be considered concerning availability which allows clients to control their assets in addition to the protection of important information such as the signature key or assets data. Risks of system control are discussed in Section 6.2.3.2.

In addition to information or risks mentioned in this section, system specific risks varied among cryptoassets custodian or risks regarding external contractor MUST be considered. Detailed risk analysis MUST be performed against the actual system of the cryptoassets custodian.

6.2.1. Risks related to signature keys

Both role and risks of signature keys are extremely large on cryptoasset exchange. Signature keys enable to transfer coins, but it comes from properties of difficulties for revocation of lost, leakage, stolen, and rollback transaction. Some risks about signature keys are listed in this section. In addition, risks about supply chain related to risks install wallets handles signature keys.

6.2.1.1. Risk analysis related to signature key

Risk analysis may depend on threats assumption, the structure of the system, and threats model, the results for each custodians shall be different. Some case studies are described in this section.

Threats for signature keys and its actors are assumed as listed below. And actors are assumed as the input of signature key in Figure 1.

*Threats:

-Loss

-Leakage, Theft

-Unauthorized Use

*Factors of Threats:

-Error in operation

-Maliciousness (of legitimate person)

-Spoofing (for legitimate person))

-Malicious intentions of outsiders

-Unintended behavior (system)

*Actors:

-Custodians operation modules

-Transaction Signing modules

-Customer assets management function

-Incoming Coin management function

Factors of threats are organized as follow.

Error in operation: A human error caused by an authorized user (including an administrator) during operation of the system. For example, the expected operation was to withdraw coin equivalent to 100,000 JPY. But, the actual operation is withdrawing coin equivalent to 1,000,000 JPY.

Malicious acts by authorized person: An act committed with malice by an authorized person (including an administrator). For example, theft or unauthorized use of the signature key by the insider. Purpose or incentive of the act is not concerned.

Spoofing(of authorized person): Impersonation with a stolen credential of an authorized person. For example, the order to sell/buy/transfer cryptoassets by an external attacker impersonating a client; the malicious order of transfer or generation/signing of a transaction through access to the system with the legitimate operator/administrator credential by an unauthorized insider. Especially, theft and abuse of credential upon an account registration by impersonating a legitimate user MUST be considered. Note: Impersonation which is not caused by theft of legitimate user/authorized person's credential (e.g., Privilege escalation) are mentioned in "malicious acts by outsiders."

Malicious acts by outsiders: Access or operation to the system by outsiders with malicious purpose excluding spoofing. (e.g., external unauthorized access by exploiting a vulnerability; remote access to the system which enables outsiders to operate to the signature key or generate a transaction by a targetted attack to an administrator of the custodians' system.)

Unintended behavior: An unintended behavior of the system regardless of intention or malice. (e.g., leakage of the signature key caused by bugs of the system, generation of a transaction including an incorrect amount of assets regardless of operation.)

Theft and unauthorized use are threats that can only be caused by a clear malicious factor. Risks to be considered as a result of threats are listed in Table 2. Please note that theft and unauthorized use could happen in a case where multiple factors such as an error in operation or unintended behavior have occurred. (e.g., insertion of backdoor that transmits a signature key or tampers a signing order to the transaction in conjunction with a specific legitimate operation.) This case can be covered in countermeasures of theft or unauthorized use.

Risk	**Factor**	**Loss**	**Leakage**	**Theft**	**Unauthorized Use**
Illegal operation(Route is legitimate)	End user's malicious operation	Y	Y	Y	Y
	Malicious operation by the administrator of customer assets management function	Y	Y	Y	Y
	Impersonation to end users	Y	Y	Y	Y
	Insider impersonating an administrator	Y	Y	Y	Y
Intrusion from outside	Intrusion into Tx signing function	Y	Y	Y	Y
	Intrusion into incoming coin management function	Y	Y	Y	Y

Risk	Factor	Loss	Leakage	Theft	Unauthorized Use
	Intrusion into customer asset management function	Y	Y	Y	Y
	Intrusion into custodian operation function	Y	Y	Y	Y
Incorrect behavior is different from operation instruction	Unintended behaviors of Tx signing function	Y	Y	-	-
	Unintended behaviors of incoming coin management function	Y	Y	-	-
	Unintended behaviors of customer asset management function	Y	Y	-	-
	Unintended behaviors of custodian operation function	Y	Y	-	-
Human error	Error in operation by end user	Y	Y	-	-
	Error in operation by administrator of customer asset management function	Y	Y	-	-

Table 2: List of possible risks for the signature key, Y means applicable risk exists, - means no applicable risk exists

The following sections outline each risk. The control measures corresponding to each risk are shown in Section 7.3.

6.2.1.2. Risk of loss of signature key

Risks listed below are an event which causes loss of the signature key from a viewpoint of input to the signature key such as order or operation.

As a typical event, the loss of the signature key caused by human error in operation by the administrator of the custodians' system may be considered.

6.2.1.3. Leakage and theft risk of signature key

In most case, theft is caused by the operation of a malicious person. By contrast, leakage could happen by error or fault not requiring the malice. Therefore, the risk of theft and the risk of leakage MUST be separately considered.

The risks of leakage shown in Table 2 are lists of the event which potentially causes leakage of the signature key including the leakage caused by error/fault regarding the input to the signature key such as an order or an operation. For example, an internal criminal, unintentional behavior of the system and intrusion to the system.

Likewise, the risks of theft are lists of the event which potentially causes the theft of the signature key by a malicious person. For example, an internal criminal and intrusion to the system.

Regarding the leakage of sensitive information to the outside, both leakage and theft are similar, and the countermeasures are the same. The countermeasures are discussed in Section 7.3.6.

6.2.1.4. Risks of unauthorized use of the signature key

The risks of unauthorized use shown in Table 2 are lists of the event which causes unauthorized use by a malicious person. For example, spoofing of the authorized person and intrusion to the system.

Unauthorized use of the signature key could be caused by unauthorized operation of pre-processes of an unsigned transaction at transaction signing function in addition to the direct unauthorized use of the signature key. Following example shows unauthorized use at an early stage of the process.

*A destination address of cryptoassets or amount of assets is manipulated due to tampering of software at transaction signing function. The tamper disables designed validation process at the transaction signing function.

* A destination address of cryptoassets or amount of assets is manipulated due to tampering of the unsigned transaction generated by transaction generator. Besides, an unauthorized transaction has generated and given to the transaction signing function.

* A destination address of cryptoassets or amount of assets is manipulated due to tampering of software at transaction generator. An unsigned transaction has generated with an unauthorized direct operation to transaction generator.

* An incorrect amount or incorrect destination address of cryptoassets has transmitted from custodian operation function through transaction generator due to an internal crime, error in operation, or spoofing of the identity by the administrator.

* Assets database has tampered in a case where the operation/order to transaction generator refers to the assets database. (See: Section 6.2.2)

As shown in the above example, the attacker is able to obtain cryptoassets without attacking to the signature key illicitly. In particular, countermeasures MUST be considered in a case where the system automates each process.

Security control measures to the signature key MUST be performed. Moreover, security control measures to the entire custodian's system MUST be performed against these complex risks. Security control measures are discussed in Section 7.

6.2.1.5. Other risks

6.2.1.5.1. Supply chain risk of hardware wallet

Hardware-wallet is known to have a function to manage signature keys. In most hardware-wallet, key administration is done on an administrative terminal connecting via USB such as PC.

Cryptographic module validation program for products having a cryptographic key management function such as FIPS 140-2 are provided. However, most of the cryptographic algorithms used in cryptoassets are not covered by those validation programs. Therefore, third-party safety validation program subject to hardware-wallet for cryptoassets is not well provided. For this reason, the users of hardware-wallet MUST understand that safety level of the hardware-wallet available at a market differs among the product.

Furthermore, the safety could be threatened by tampering the product during distribution channel even though the product has a certain level of safety in the factory. For example, hardware-wallet tampered in a distribution channel to have a malware enables the attacker to restore the signature key generated by a legitimate owner without acquiring the hardware-wallet.

6.2.2. Risks related to assets data

Assets data is data to manage an amount of cryptoassets/fiat currencies held by clients or custodian itself. The signature key for transaction signing is not recorded in the assets data. (See: Section 5.2)

As mentioned earlier, assets data differs among the custodians, an abstracted model is used in this section. In this section, a brief thought is given since detailed threat assessment and risk analysis MUST be performed against assets data of the actual custodians' system.

Major threats to the assets data are unauthorized manipulation, loss, and leakage. The factors are an error in operation by the administrator, malicious acts by the authorized person, spoofing of the authorized person, malicious acts by outsiders, and unintended behavior of the system.

In a case of the basic model shown in Section 5.2, attack surfaces are custodian operation function, assets database, and incoming coin management function.

Following example shows the incidents caused by unauthorized manipulation among the risks to assets data.

* An incident that the malicious transaction generated by assets database which refers manipulated assets data has broadcasted through a legitimate process. (See: Section 6.2.1.4)

* Unauthorized manipulation to a number of assets stored in asset data between clients and/or between clients and custodians by tampering a list of cryptoassets address linked to clients. This enables losing assets of clients or custodians without broadcasting the transaction to the blockchain.

Risks of assets data may be considered as risks of system in financial service and settlement service. However, countermeasures to the incident that transaction(s) has merged into blockchain as a result of unauthorized manipulation to the assets data MUST be considered with an understanding that transaction broadcast to the network is irreversible.

6.2.3. Risks of suspension on system and operation

Cryptoassets custodians' systems are composed of software, hardware, networks. Operations are classified as monitoring, opening an account, an order of transfer, deposit/withdrawal of (crypto/fiat) assets from the wallet, and any operations by the operator. The system may be suspended due to various factors.

Cryptoassets custodians' system tends to be a subject to the attack due to following: the systems are connected to the Internet for 24 hours 365 days, not by the leased line, many of the systems are deployed on cloud services, prices of cryptoassets are effected from operating condition of the cryptoassets custodians. Therefore, countermeasures to the attack MUST be considered.

6.2.3.1. Risks related to network congestion

Cryptoassets custodians may be attacked by DoS and traffic flooding. In general, targets of attack are a top page of the Website, API endpoint, etc., but operation and monitoring system deployed on the Internet may be a target of DoS attack in a case where the attacker acquired the information of the system beforehand.

6.2.3.2. Risks of system suspension due to infrastructure

System and operation may be suspended in a case data center or cloud infrastructure where custodian's system is deployed are suspended. The system may be suspended due to various factors such as blackout and disruption of communication due to acts of nature, due to operation failure by cloud or infrastructure, and failure of software release.

6.2.3.3. Risks of system suspension due to the operator

Even if the system is in operation, there is a possibility that the service may be suspended if operation monitoring and the activities of the operator in charge of work are hindered. For example, there is a possibility that business would be suspended due to various factors such as periodic inspection of power supply facilities at operational sites, disruption of transportation by disaster, strikes, and obstruction of building access by protest activities and rush of reporters. There are also risks that many personnel cannot operate due to the same reasons, such as using the same transportation method, participating in the same event, or traffic accident or food poisoning.

6.2.3.4. Regulatory risks

In countries where the cryptoassets custodian is defined by law and should be licensed or registered, operations may be suspended by order of business improvement, operation suspends, deletion of license or registration issued by the authority.

6.3. Risks from external factors

Even if a cryptoassets custodian performs its operation appropriately, the cryptoassets custodian could not continue the service or might not execute transactions when encountering attack to the blockchain network and/or the network infrastructure connecting each node.

6.3.1. Risks related to the Internet, Web PKI, and users environment

6.3.1.1. Attack to Internet routing and DNS

Attackers can lower the reachability to cryptoassets custodians, lure a user into the fake cryptoassets custodian, or fork deliberately by preventing the synchronization of the blockchain, through the intervention in routing or DNS, such as BGP hijacking. These methods might be used by not only malicious attackers, ISPs acting governments order.

6.3.1.2. Attack to Web PKI

Most cryptoassets custodians provide their services on the Web and use TLS and server certificates for authenticity and confidentiality of their website. When the certification authority issuing their certificates encounter an attack, it yields to enable to spoofing the cryptoassets custodians' website. When the certificate is revoked, the cryptoassets custodian might not be able to provide own service.

6.3.1.3. Attack to messaging systems

Attackers can swindle or block the e-mail and SMS using for delivering One-Time Password, through the intervention in messaging systems such as SMS or e-mail. When a users message is swindled, attackers can log in as the spoofed user or reset the password.

6.3.1.4. Risks related to users environment infection

When a user's environment such as PC and smartphone is infected by malware, any secrets such as credentials in the environment might be swindled.

6.3.2. Risks related to cryptocurrency blockchain

6.3.2.1. Split or fork of blockchain

A distributed ledger might be forked by specification changes without consensus in the developers community. There are two cases around the fork; one is that the transaction before the fork is executed and recorded in both ledgers after the fork, another one is that the transaction before the fork is executed and recorded in only one ledger.

6.3.2.2. Blockchain Re-organization caused by 51% attack or selfish mining

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

6.3.2.3. Compromising cryptographic algorithm and hash function

Improvement of performance of computing power and the discovery of effective attack might cause being compromisation of the cryptographic algorithm and hash function.

6.3.2.4. Inadequate blockchain specification and implementation

In the cryptoassets Lisk, there were implementations in which the timestamp value of the transaction allowed implementation of numerical value input in a range not permitted by the internal database so that each node could not process the transaction and block generation stopped[LISK-ISSUE_2088]. This issue was fixed within several hours after the problem occurred and the node updated the client software, and the network was sequentially recovered. However, the transactions could not be processed in the blockchain for a certain period.

There are cases that token value collapses due to inadequate implementations of smart contract. In Beautychain Token (BEC) of ERC20 token issued on Ethereum, there is a vulnerability that causes overflow in the smart contract, so there is an attack which derives greatly exceeded tokens over the upper limit, then the worth of BEC was collapsed. [CVE-2018-10299]

6.3.2.5. Rapid changes in the hashrate

When the hash rate increases or decreases rapidly, it might take a very long time for generating blocks using the remaining node.

6.3.3. Risks from external reputation

6.3.3.1. Bank account frozen

Banks might freeze an account of cryptoassets custodians operation, by the guidance of regulatory as a countermeasure for AML/CFT, or by some accidents/incidents. This freeze results in a suspending a deposit/withdraw operation of clients fiat assets.

6.3.3.2. Address of cryptocurency

As countermeasures for AML/CFT, other cryptoassets custodian Y might assess whether the destination address of cryptoassets custodian X have a high deal risk when a user of Y transfers some assets to the address of X. If an address of X is blacklisted, the transaction between X and Y might not be executed smoothly.

Since criminals often transfer the stolen "cryptoassets" to unmalicious third party's address for disrupting investigation, the address might be involuntarily categorized as high-risk.

6.3.3.3. Filtering or blocking website

Users might not be able to access cryptoassets custodian when its URL is filtered out by network operators or is blocked by ISPs. When a cryptoassets custodian's website is recognized as used for malware distribution, its URL might not be appeared in search results or not be able to browse in the browser.

6.3.3.4. Email

Most mail servers provide a filtering service or a classifying service based on reputation, as countermeasures for spam mail. If the e-mail from the cryptoassets custodian is recognized as spam mail, the custodian might not be able to contact the user.

6.3.3.5. Appraisal of a smartphone application

Application delivery platform might limit applications from handling cryptoassets. When the application provided by a cryptoassets custodian could not be approved by the platforms, a user cannot download the application for access to the custodian, and cannot use the services.

6.3.3.6. ID theft

There is some case where the attacker acts malicious instruction spoofing as a user, for example: - list based attack, - theft of ID, password or other credentials, by a malware infection, and - theft of API access token.

The distinctive purposes of spoofing are: - theft of fiat currency or cryptoassets by unauthorized withdrawals, - money laundering by cashing cryptoassets with an account in the name of other people, and - profit shifting by market manipulation by unauthorized buy and sell cryptoassets.

7. Considerations of security controls on Cryptoassets Custodians

7.1. General

Below is a basis of security controls about risks written in Section 6.

To promote understanding and coverage, all security controls in this chapter are followed by below: [ISO.27001_2013] , [ISO.27002_2013]. There are some specific considerations for Cryptoassets Custodians to follow ISOs. Especially, the organization shall consider for strong controls to manage signature keys for cryptoassets backed by assets.

Other security controls are expected to be referred to similar operations by the financial sector. Security controls should be included concrete content from results of risk analysis and vulnerability diagnosis. Threats of cybersecurity are changing, reviews of security controls according to situations are important. Articles below are expected to describe contents by references and completion of description.

7.2. Basis for consideration about security management

There are some standards of requirement for information security, [ISO.27001_2013] and [ISO.27002_2013]. Cryptoassets Custodians shall refer the requirement or guidance of these standards and consider security controls needed and shall establish, implement, maintain and continually improve security management. Cryptoassets Custodians has data of customers asset, self asset, customer information, signature keys. Those shall be protected from leakage, loss, tampering, and misuse. Cryptoassets Custodians shall consider about risks of lost assets by foreign factors such as blockchains or network, suspension of system, and shall act properly. Cryptoassets Custodians shall mainly consider about security management described below:

*Interested parties (from "4. Context of organization", [ISO. 27001_2013]) To protect assets of cryptoassets custodian's customer. Division of responsibility between outsourced and cryptoassets custodians such as management of signature keys for cryptoassets. Impact of business such as money laundering shall be considered from another viewpoint.

*Policy (from "5. Leadership", [ISO.27001_2013]) Cryptoassets custodians shall establish an information security policy that includes information security objectives and controls. Information security policy shall be disclosed so that customers can browse.

*Continual improvement and risk assessment (from "6. Planning", "8. Operation", "9. Performance evaluation", and "10.Improvement", [ISO.27001_2013]) As described in Section 6.3.2, numbers of cryptoassets have been developed and its speed of evolving is rapid, Cryptoassets Custodians shall monitor security risks about cryptoassets in addition to information security management applied in general. Cryptoassets Custodians shall review and improve security controls according to the situation.

7.3. Considerations about security controls on Cryptoassets custodians

Cryptoassets Custodians shall determine information security objectives and controls from the viewpoint listed below:

*Risk treatment options to prevent from loss, steal, leakage, misuse of secret keys used for cryptoassets, customer data, and customer asset.

*Compliance with business

*Compliance with legal and contractual requirements

There are some considerations described in Section 7.2 about security controls based on system risks at Cryptoassets Custodians. There is a guidance for security controls as [ISO.27002_2013], Cryptoassets Custodians shall refer it to design and / or identify security controls. Section 7.3.1 to Section 7.3.13 below are followed to [ISO.27002_2013] and describe items to be especially noted in the virtual currency exchange system.

7.3.1. Information security policies

Information security policies shall be defined to follow Section 5 on [ISO.27002_2013]. Information security objectives on Cryptoassets Custodians shall include conservation of customer's asset, requirements of the business, compliance with legal and contractual requirements, social responsibilities. Information security policies shall contain policies about access controls (on Section 7.3.5), cryptographic controls (on Section 7.3.6), operations security (on Section 7.3.8), and communications security (on Section 7.3.9) .

7.3.2. Organization of information security

Cryptoassets custodians shall follow "6. Organization of information security" on [ISO.27002_2013], and shall establish a management framework to implement and operate information security. Cryptoassets custodians shall consider about threats such as an illegal acquisition of signature keys or illegal creation of transaction carefully. Segregation of duties shall be fully examined to manage signature keys for signing or to permit create transactions.

7.3.3. Human resource security

Cryptoassets custodians shall follow section "7. Human resource security" on [ISO.27002_2013]. To examine and evaluate security controls, cryptoassets custodians shall deploy human resources with expertise not only in information security applied in general but also in cryptoassets and blockchain technology. All employees may handle assets and shall receive appropriate education and training and regular updates in organizational policies and procedures.

7.3.4. Asset management

Cryptoassets custodians shall follow section "8. Asset management" on [ISO.27002_2013]. Cryptoassets custodians shall contain any pieces of information to manage assets, and information and asset of the customer such as the signature key. Cryptoassets custodians shall determine controls suitable for risks to follow this section if cryptoassets custodians operate hardware wallets. To protect assets of customers, cryptoassets custodians shall separate assets into customers and custodians to follow compliances with accounting.

7.3.5. Access control

Cryptoassets Custodians shall follow section "9. Access Controls" on [ISO.27002_2013].

Users are separated into 2 parties; Permitted operators and administrators within outsourced, and customers. Some considerations for operators and administrators are written in Section 7.3.5.1, and for customer is written in Section 7.3.5.2

7.3.5.1. Access controls for operators and administrators

There are some cases for operators and administrators.

* Operators and administrators for custodians system. They will command to create keys or to transfer funds by software or terminal.

*Administrators to maintain hardware, OS, databases, and middleware.

Management measures of signature keys such as activate, backup, restore are described on Section 7.3.6. Cryptoassets custodian shall be carried out to assign authority to operate properly and shall set access control. Access controls shall be include authorize and permit to connect custodians system from remote, authorize for external service if using as functions for cryptoasset custodians, authorize as a user for OS and databases, permit to enter and leave facilities systems or terminals installed. There are some factors to permit access: Only office hours or predetermined hours, Only IP addresses assigned for specific terminals, Confirm by credentials to connect from operators or terminals predetermined. Cryptoassets custodians shall consider for access control policies by roles or authorities of operators and administrators for each system. Access control shall be set the minimum to run functions or software permitted for operators or administrators, not only for applications.

Any damage may be happened by miss or injustice operations on transferring assets or managing signature keys as described Section 6.2. To deter these threats, Confirmation of or approval by multiple operators or multiple administrators shall be needed on important operations such as transferring assets and operations for the signature key. Cryptoassets custodians shall not concentrate duties for one operator or administrator, decentralize of duties for multiple operators or administrators shall be needed.

7.3.5.2. Access control for customers (user authentication / API)

*Strict personal identification on setup account The account shall be set up by strict personal identification, and account information shall be sent to the person itself. For example, personal identification shall be operated by an identification document issued by the public organization and shall be sent a letter to the address without forwarding. Personal identification shall be carried out in accordance with relevant laws, regulations, treaty such as FATF. Replacement of pictures on an identification document or falsification of attribute information is typical treats for personal identification. In order to operate personal identification strictly, it shall be carried out to verify by software or visual check and verify by an electric method such as signature that is hard to falsification.

*Managing credential and multi-factor authentication For user authentication, it is expected to prevent from spoofing and internal injustice by installing risk-based authentication on not normal access (such as a characteristic of terminal or route, and different time slot from usual) and multi factor authentication on spoofing by leakage of single credential. It is NOT recommended to deliver one-time-password by unprotected transmission line as email because there is a risk of impersonation or fraud on the transfer route. Confirming telephone number by SMS was valid for verifying owner and reachability, but that has been RESTRICTED by NIST, so personal authentication technology such as possession identification and transaction authentication technology should be applied. SMS may be one factor used to recovery account, but not measure to confirm the existence and authenticate.

*Multi-factor authentication, risk-based authentication It shall be carried out to register customer and set access controls strictly to avoid defraud customer funds, changing to fiat and money laundering by spoofing customers.

*Confirmation of intention according to the risk of operation To be consistent with the convenience of customers and safety of service, It shall be considered to make a different level to authenticate by risks of customer's operation. For example, low-risk operations such as display balance of account or details of trade may be allowed by single-factor authentication, but update transactions such as trading coins or changing address or account shall be authenticated by an additional factor. In addition, operations it may cause damages such as output coin or order of fiat transaction shall be ordered to confirm by additional authenticate or to confirm intention by an operator.

*Data preservation on deleting an account Cryptoassets custodians shall implement system be able to rollback after erasing for a certain period if customer stated spoofed or unauthorized access. Cryptoassets custodians shall delete the account if requested from a customer, but they also shall consider about risks that attacker spoofed to customer requests to delete the account.

*Signature key preservation on discontinue addresses Signature keys linked to an account shall not be deleted even if the address of cryptoassets has no value. On a prediction for the general cryptoassets customer is allowed to send assets for any addresses and not technically prevented to send, signature keys for wallet stopped to use shall be taken back up for reuse because the possibility of receive coins to the address exists.

*Consideration for supplying APIs To set access control for operations by a customer, it shall be considered about not only operations of dialogue operations on the web but also APIs connecting from the application by smartphone and from external systems. For providing APIs, It shall be implemented to consider cases that are difficult to get explicit approval from customer. It shall comply with best practices shared in the industry based on the attack risk peculiar to API. For reference, it may be followed to Financial API by OpenID Foundation.

7.3.6. Security controls on signature keys

It SHALL conform to Section 10 "Cipher" of [ISO.27002_2013].

Particularly, some security controls for the signature key, an issue specific to cryptoassets custodians, are closely related to the controls in other sub-sections in this section (e.g., Section 7.3.5).

Amount of cryptoassets in Hot Wallet MUST be limited to a minimum amount and isolate their remain assets to another secure place, e.g., Cold wallet. The minimum amount means the amount which can be temporarily paid within the time it takes to withdraw the assets from the secure place. Custodian can be refunded to the customers from the remain assets even if the assets in Hot Wallet leaks.

Custodians MUST choose an appropriate cryptographic technology that has been evaluated its security by the third party in accordance with the purpose of use, as with general information systems. Also, they MUST decide the life cycle of a signature key and MUST implement and operate appropriate controls.

7.3.6.1. Basics of Signature Key Management

In general, followings are required in the management of private keys including signature keys.

* They should be isolated from other informational assets. Rigorous access control is mandatory.

* Limit the number of access to signature keys as minimum as possible.

* Be prepared for unintentional lost of signature keys.

Followings are three basic security control to realize above. Additional security controls specific to crypto assets custodians are described in and after sub-sections Section 7.3.6.2.

1. State management of signature keys As described in Figure 2, a signature key has one of the multiple states generally, and it may be an active or inactive state in its operation. The signature key MUST be in an active state when it is used for signing (or decryption). It is recommended to enforce to input some secret information to activate from the inactive signature

key. This makes keeping the inactive signature key away from abuse if the adversary does not have the secret information. This method ensures also the security of the signature key against leakage and lost. It is also recommended to minimize the term of activation to limit the risk of abuse as minimum as possible. Unnecessary activation of the signature key increases the risk of abuse, leakage, and theft, though keeping the activation state is efficient from a business viewpoint. On the other hand, frequent activation/inactivation may give impact to business efficiency. It is important to consider the trade-off between the risk and business efficiency and provide clear key management policy to customers.

2. Administrator role separation and two-person rule It is a fundamental form of operation of a critical business process which uses the signature key to perform cryptographic operations by multiple parties to prevent internal frauds and errors. For example, by setting separated privilege on digitally signing and approval to go into the area of signing operation, it becomes difficult for the single adversary to give a malicious digital signature without known by the third party. Additionally, the enforcement of the two-person rule is effective security control to internal frauds and misoperations.

3. Backup of a signature key Lost of the signature key makes signing operations (by using the key) impossible any more. Thus backup of the signature key is an important security control. Since lost of the signature key makes signing operations impossible any more, backup of the signature key is an important security control. On the other hand, risks of leakage and theft of backup keys MUST be considered. It is needed to inactivate the backup keys. Additionally, monitoring the blockchain whether to perform the outgoing-coin from that address to detect the inappropriate backup and the illegal-use of little-used address.

7.3.6.2. Offline Key Management

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

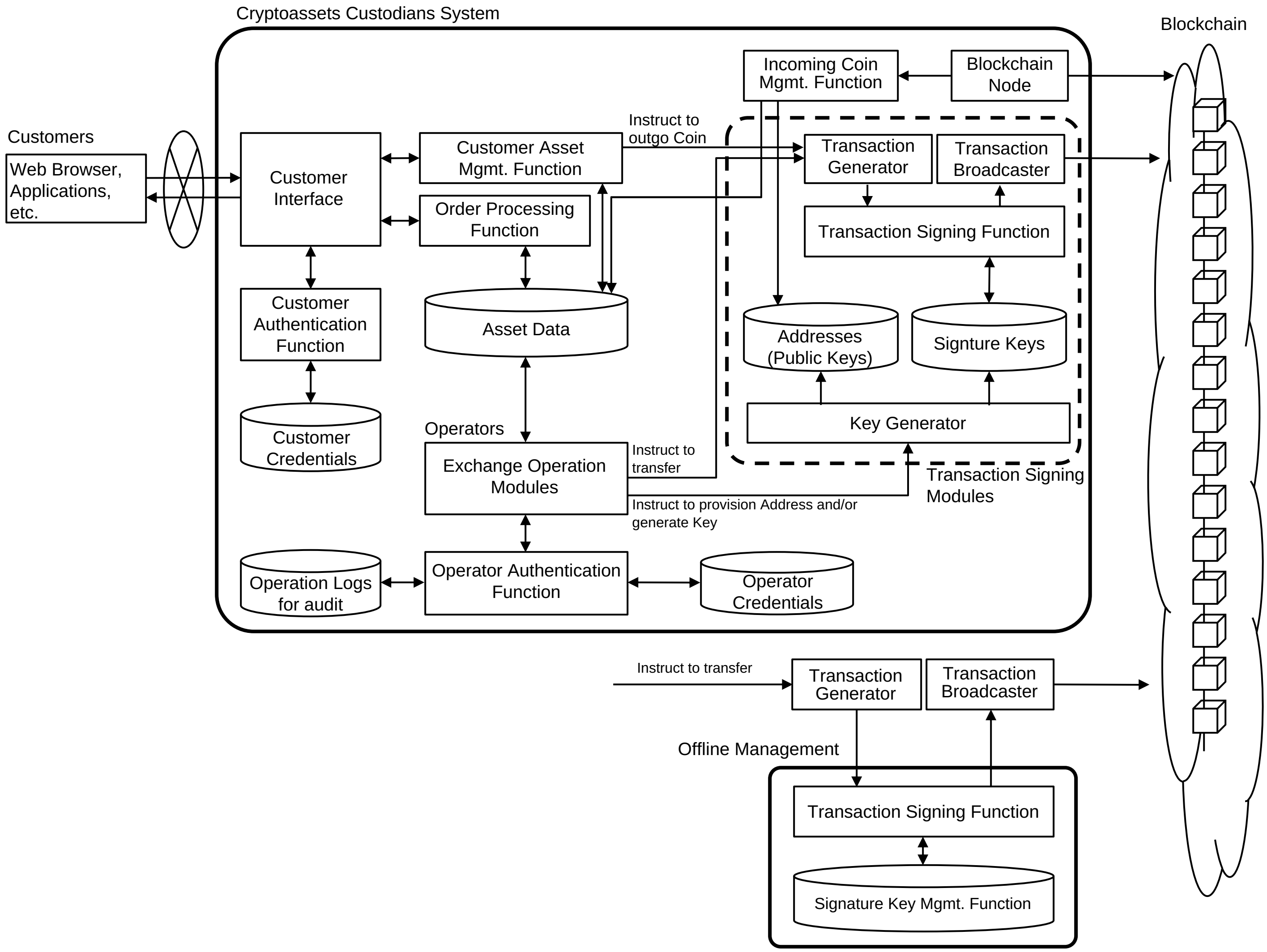

Figure 4: Example of offline signature key management

In this case, it REQUIREs some kind of offline operations to make the system use the signature key.

Examples are a) it requires to move a signature key from the vault and to connect to the online system, b) input/output between online system and offline (key management) system does perform through a kind of storage, such a USB Flash Drive.

If there is not an explicit approval process for the signature key used in the offline operation, anyone cannot stop the malicious transaction. That is, for achieving this solution can prevent abuse, loss, and theft of signature keys, an explicit approval process is needed for this solution.

7.3.6.3. Privilege separation of signature keys (Authorization process)

Both privilege separation and two-person control of signature key management are effective as shown in Section 7.3.6. In addition, there is multi-signature as a typical scheme for blockchain[BIP-0010][BIP-0011]. Multi-signature REQUIREs an authorization process with multi-stakeholders, and it is achieved by signing with the signature keys managed by each stakeholder. Each stakeholder MUST verify other signatures technically if exists, and MUST validate the practical consistency of the transaction.

Authorization process with multiple stakeholders can expect for a general countermeasure for malicious generation of a transaction. Note, however, that security controls for the leakage and/or loss of the signature key are still needed.

Since a multi-signature scheme is provided by software, its logic and implementations are varied with some blockchain. e.g., multi-signature in Ethereum is implemented on smart contract, so that there are various implementations with each wallet software. Also, some blockchains might not support multi-signature, therefore some cryptoassets could not adopt multi-signature.

Also, there is another similar scheme "Secret Sharing Scheme" which is applicable to privilege separation. This is a management technology in a distributed environment which has divided secret respectively, and one of the countermeasures for leakage and/or lost of signature key. However, this scheme is rather a technology for single stakeholder with multi-location operation than multi-stakeholders, because it REQUIREs a validation scheme separately for the transaction to each stakeholder and management of the divided secret is rather depend to implementation than the signature key.

7.3.6.4. Backup for Signature Key

Backup is the most fundamental and effective measure against lost of signature key. On the other hand, there are risks of leakage and loss of the backup device.

These risks depend on the kind backup device, thus security controls on such devices MUST be considered independently. Followings describe typical backup devices and leakage/theft risks associated with them.

* Cloning to the tamper-resistant cryptographic key management device If a signature key is managed by a tamper-resistant key management device (device X) and X has cloning function, cloning the key to another device Y is the most secure way to back up the key, where the cloning function is the technique to copy the key

with keeping confidentiality to other devices than X and Y For example, cloning via PC does not meet this requirement when the signature key is read into memory on the PC in the cloning.. The implementation of the function is recommended to be evaluated/ certified by certification programs like CMVP or FIPS 140. Note that, the cryptographic algorithms supported by such tamper-resistant key management devices are limited and all crypto assets systems can utilize it, but it is one of the most secure ways of backup.

* Backup to storage for digital data Here, it is assumed to backup keys to storage like USB memory and DVD. There are two types of operations; one is backup data is stored in movable devices in an offline manner, the other is backup data is stored in an online accessible manner. If the device is movable, the possibility of steal and lost increases, thus the device MUST be kept in a cabinet or a vault with the key, and the access control to such cabinet/vault MUST be restricted. Of the backup storage is online, risks of leakage and theft MUST be assumed as same as the key management function implementation inside the cryptoassets custodian. In general, the same security control is recommended to such backup storage. If there is some additional operation, for example, the backup device is inactivated except for the time of restore, the security control may be modified with considering the operating environment. When it is not avoided the raw key data is outside of the key management function implementation, the custodian MUST deal with the problem of remained magnetics.

* Backup to paper There is a way to backup keys in an offline manner, to print them to papers as a QR code or other machine readable ways. It is movable than storage for digital data and easy to identify. There remains some risk of leakage and theft by taking a photo by smartphone and so on.

* Redundant with Sharing secret scheme Dividing of signature key to multiple parts, then managing them by 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 to implement this control based on a certain level of security evaluation like a secret sharing scheme. In that case, secure coding and mounting penetration test are REQUIRED to eliminate the implementation vulnerabilities. This method is also effective for backup devices.

7.3.6.5. Procurement of hardware wallet

When introducing a wallet, it is RECOMMEND to use a product whose technical security is guaranteed like HSM which is originally used for existing PKI service etc. However, some products may not be applicable currently because they often do not support a kind of cryptographic algorithm used by crypto assets. Therefore, if introducing a wallet, it is RECOMMEND to operate in mind the following points with accepting the technical insufficiency:

* MUST not use hardware obtained through the untrusted procurement route.

* MUST apply the latest firmware and patches provided by the manufacturer.

* Initialization and key generation MUST do themselves, SHOULD NOT use default settings without careful considerations.

* MUST consider trustworthy of software instructing a sign to hardware wallet, especially whether it supports multi-signature or signing at the offline environment.

Additionally, when custodian uses only hardware wallets in the marketplace, they MUST manage it according to section Section 7.3.4.

On the other hand, hardware wallets MUST be subject to the third-party or independent certification scheme for security. If introducing a software wallet from outside, it MUST consider the potentiality of containing malicious code, vulnerability, and bugs.

7.3.7. Physical and environmental security

Cryptoassets custodians system MUST follow section "11. Physical and environmental security" on [ISO.27002_2013].

Cryptoassets custodians system MUST consider strict physical security protections for the following elements.

* Media containing a signature key. (Signature key management shown in Figure 1)

* Media containing a signature key for cold wallet environment. (Signature key management for offline management shown in Figure 4.)

* Media containing a backup data of signature key

If the signature key mentioned above is stored in the deactivated state, and also key encryption key to activate the signature key is controlled separately, the media containing the key encryption key MUST be strictly managed.

The security control to these signature key MUST be separated from the security control of the crypto assets custodian system. In addition to this control, access to facilities and environments which store media containing a signature key or information required to operate the signature key MUST be restricted. (See: Section 7.3.6)

Furthermore, countermeasures to loss or theft for the operational device MUST be taken place if the administration or operation is executed from a remote place such as out of a facility.

7.3.8. Operations security

Crypto Assets Custodian systems MUST follow section "12. Operations security" on [ISO.27002_2013]. In addition to the standard, cryptoassets custodian systems SHALL comply with the security controls mentioned following sections.

7.3.8.1. Protections from malicious software (Related to ISO. 27002:2013 12.2)

Detection and recovery measures of malware MUST be appropriately taken place according to configurations, the environment of cryptoassets custodian systems and confidentiality and importance of information handled in the systems.

In general, one of the prevention measures for malware is applying security patches to operating systems, middlewares of cryptoassets custodian systems. However, those patches MUST be applied upon sufficient confirmation based on the importance and urgency of a patch. Moreover, testing and deployment procedure of security patch MUST be considered beforehand just in case attacks against the vulnerability have already confirmed.

7.3.8.2. Backup (Related to ISO.27002:2013 12.3)

Upon making a backup of systems, strict security controls to important data which suffered severe damage by leakages such as the signature key or master seed MUST be applied same as data subject to backup (e.g., an appropriate selection for storage, and enforcement of strict access controls.) Security controls such as distributed storage mentioned in Section 7.3.6), proper privilege separation on backup and restore between operators and people making an authorization, and operation with multiple parties are also important.

7.3.8.3. Logging and monitoring (Related to ISO.27002:2013 12.4)

Crypto asset custodians systems MUST obtain/monitor/record logs properly (not limited to but include following logs).

*Logs on the environment where the cryptoassets custodian system Collecting and monitoring of event log outputted from the system components such as middleware, operating systems, and computers detects an abnormal state of environment where the system runs. Collected logs are used to investigate a cause in the case of the incident.

*Logs on the processing of components of crypto assets custodians system Collecting and monitoring of the processing logs from each component detects an abnormal state of crypto assets custodians system. Collecting proper logs are used as a proof of proper processing inside the crypto assets custodians system, and also used to investigate a cause in a case of the incident.

*Access log of signature key Information such as date, a source terminal, an operator(not a role but information to identify an operator) MUST be obtained and recorded in a case of operations such as activation and deactivation of the signature key, access to the activated signature key and backup/restore. Those records MUST be validated against the records such as operational procedures, operating hours, on a periodical inspection such as weekly inspection. Moreover, in a case where the signature key is managed online, operational log such as the creation of a transaction signature by operator MUST be recorded and validated as well.

*Operational Log of a wallet managed by custodians Logs on remittance MUST be monitored real-time against the attempt of outgoing coin transfer in a case where the signature key and backup are unexpectedly leaked. In a case where an unexpected remittance has occurred in one of the wallets, monitoring logs help timely detecting the incidents, suspending all signing operations, rechecking on other existing wallets, and migrating to other wallets using a different signature key.

*Access log of administration remote terminal If a remote access to cryptoassets custodian system is permitted, audit information such as date, source IP address, terminal information(e.g. terminal ID, latest result of security evaluation if it's possible) and destination IP address (or hostname) MUST be obtained and recorded for auditing which checks the accesses are from/in authorized range.

* Traffic log between the inside and the outside (e.g., the Internet) As mentioned in Section 7.3.9.1, Inbound traffic to cryotoassets custodian systems such as traffic from the Internet MUST be restricted to a permitted external network or permitted protocol. Inbound traffic from disallowed network and traffic using disallowed protocol are denied at the firewall and other middleboxes. Logs from that equipment are effective to protect customers from malicious access in terms of not only cryptoassets custodian system but also the information security. Usually, outbound traffic from protected assets such as cryptoassets custodian systems to the Internet and other systems is not a subject to logging. However, those logs are useful in cases such as investigations on incidents (e.g., malicious usage of the signature key, theft of signature key) and detection of the incident, so entire traffic or network flow are RECOMMENDED to be acquired according to protocols/destinations.

* Customers access log Customers access log MUST be obtained since those logs are used to detect malicious login or request. Also, those logs are used as evidence in a case of incidents. In a case of malicious login, custodians MUST notify its customer.

  - Provide information about the malicious activity to customers Providing a feature to allow a customer to confirm login history, source IP address, region, and terminal information, and login notification by a push-notification or an e-mail are effective to detect malicious access after the incident. Feature protecting an account and alerting to a user in cases when detecting login from unknown source address or terminal, or detecting consecutive login to multiple accounts from the same source IP address, are effective to protect a user from malicious access.

* Images/videos recorded by a surveillance camera and entry/exit records Storing images/videos recorded by the surveillance camera and entry/exit records for proper period enables validating if physical safety control measures work properly after the incident.

Detecting a malicious process execution (e.g., malware), malicious access, an abnormal state of cryptoassets custodians system by monitoring logs mentioned above comprehensively is important. Moreover, storing this evidence is important to prevent internal fraud and exonerate person involved from the charge. Security Operation Center (SOC) may help to monitor the system. Outsourcing to trusted operators about detection and notification of threats in the operation of SOC may be helpful.

7.3.9. Communications security

Cryptoassets custodians system MUST follow section "13. Communications security" on [ISO.27002_2013].

Since assets are managed in a state accessible from the Internet on cryptoassets custodians system, preventive measures, detection measures, countermeasures and recovery measures as measures to prevent information leakage, MUST be considered according to the risk.

7.3.9.1. Network security management (Related to ISO.27002:2013 clause 13.1.1)

As same as security control measures to general systems, measures such as a definition of a boundary to the external network, restriction of connection to a network system(e.g., firewall), stop unnecessary services or close unnecessary ports, obtaining and monitoring logs and malicious access detection MUST be considered and performed.

For logs, logs of internal systems MUST be monitored to detect internal malicious access, as well as monitoring of boundary to the external network. (See: Section 7.3.8.3)

Secure communication with proper mutual authentication such as TLS(Transport Layer Security) MUST be used to protect from attacks to communication between modules such as eavesdropping and manipulation in a case where modules of cryptoassets custodians systems are remotely located.

7.3.9.2. Network segmentation (Related to ISO.27002:2013 13.1.3)

It is important to limit a connection between cryptoassets custodians systems and other systems/the Internet as minimum as possible to reduce the risk of exposing against attacks through a network. Measures as follow such as network segmentation and limitation to connection MUST be considered.

* Network isolation between custodians systems and other information systems

  - Objectives: Preventing a connection to custodians systems through information systems used in daily operations, which has been compromised due to malware infections caused by external attacks such as targeted attack.

  - Countermeasures: Isolate a network between information systems used in daily operations and custodians system by segmentation of network or limiting access.

*Network isolation at the boundary to the Internet

-Objective: Preventing access to critical information such as a signature key from attack through the Internet by minimizing and isolating modules which connect to the Internet.

-Countermeasures: Features which connects external services on the Internet to achieve the functionality of custodians system, transmit transactions or obtain blockchain data MUST be packaged as a module as minimum as possible or be isolated from other systems such as locating on DMZ. Moreover, if modules are connecting to external services, access controls to those services MUST be adequately performed.

*Limitation on a terminal used in custodians system administration

-Objective: Preventing a malicious operation due to a hijacking of terminal used in custodians system administration.

-Countermeasures: Limiting a terminal which can connect to custodians system, such as a terminal to manage a custodians system administration function and a terminal running an administrative tool to order operation to custodians system.

7.3.9.3. System acquisition, development and maintenance

Cryptoassets custodians system MUST follow section "14. System acquisition, development, and maintenance" on [ISO.27002_2013].

Cryptoassets handled by cryptoassets custodians ranges from high liquidity cryptoassets dealt with by multiple custodians to emerging cryptoassets. It is important to reduce a risk regarding system acquisition, development and maintenance in addition to [ISO.27002_2013] as characteristics of blockchain network used by those cryptoassets varies. For example, the following countermeasures are effective.

*Software development method Secure software development method such as secure coding and code review MUST be used in the software development of the custodian system. Code review not only with the development team but also with an operational team is effective to detect a vulnerability from the viewpoint of operation.

*Penetration test Conducting a penetration test helps to detect a known vulnerability at systems and results in obviating the attacking risk by the attacker in advance.

*Integration test with blockchain network Test MUST be performed not only with the test network of blockchain but also with the production network of the blockchain. Risk assessment MUST be taken with an understanding of the limitation of test on the production network such as high-load test.

*Privilege separation on the operation Privilege separation such as limiting code reviewed software deployment to the production environment to the system operating team is effective to prevent tampering attacks from internal.

*Prohibiting using default (factory-configured) values Any factory-configured authentication information such as password MUST NOT be used regardless of hardware/software, development environment or production environment.

7.3.10. Supplier relationships

Cryptoassets custodians system MUST follow section "15. Supplier relationships" on [ISO.27002_2013].

Outsourcing wallet-related services may be a reasonable choice in a case technical security of those services has been secured.

Administrative measures according to [ISO.27002_2013] MUST be taken in terms of outsourcing contractors or security controls of cloud service providers in cases where signature key in multi-signature is delegated to contractors or custodians system is implemented on cloud services.

7.3.11. Information security incident management

Cryptoassets custodians system MUST follow section "16. Information security incident management" on [ISO.27002_2013].

Since cyber attacks got complex, cyber security incidents unprecedented in the past could occur, especially in cryptoassets custodians. In addition to security control measures as a preparation to expected threat in advance, Emergency response framework MUST be prepared in a case of incidents caused by an unknown threat. For example, the establishment of internal CSIRT(Computer Security Incident Response Team) and building a relationship with external organizations.

7.3.12. Information security aspect of business continuity management

Cryptoassets custodians system MUST follow section "17. Information security aspect of business continuity management" on [ISO.27002_2013].

Requirements, Processes, Procedures and control measures to secure information security for the cryptoassets custodian in a case of the severe situation(such as disaster or crisis) MUST be established, documented, performed and maintained. In this case, administrative measures in a case where countermeasures have performed or in a period of a severe situation MUST be verified periodically. Moreover, operators MUST consider to shut down the system situationally.

*In a case where facilities (including facilities used as an office) are unavailable

-Power outage

-Damages of building

-An act of nature (e.g., earthquakes, fires (including sprayed water for neighborhoods fire), water outage, flood)

-Other reasons (e.g., facilities are unavailable, or access to the facilities are prohibited by law/regulations/authorities.)

*In a case where it's difficult to continue the system

-In a case of becoming difficult to continue running an emergency electric generator.

-Long suspension of public transportation services, a pandemic of disease, lack of human resources by an act of nature.

-Failure of a communication network

-Failure of equipment

-Failure of the system (regardless of reasons such as failure of a program or cyber attacks)

-Loss of paper wallet or hardware wallet.

-Suspension of outsourcing contractor's business

-Leakage or loss of signature key

*In the case of becoming difficult to continue business

-Business-suspension order by law/regulations.

7.3.12.1. Maintaining availability of the system

Cryptoassets custodians system MUST be designed and implemented to have enough scalability and redundancy for users with consideration of a number of users, peak date/time of transactions, system response time, maintenance period/frequency and securing a human resource for operation. Moreover, consideration for increasing the capacity of the system MUST be performed in advance with enough threshold (e.g., number of transactions or memory usage during a peak period).

7.3.13. Compliance

Cryptoassets custodians MUST respect the guidelines or laws of the region or country. (See Appendix 3 for a country of Japan)

7.4. Other cryptoassets custodians system specific issues

7.4.1. Advance notice to user for maintenance

Cryptoassets custodians are RECOMMENDED to publish a notice of maintenance schedule in advance in a case where periodical schedule especially service suspension is planned in a night. Also, Cryptoassets custodians are RECOMMENDED to provide information regarding the failure of the system at other FQDN/IP addresses to avert high volume traffic to the web server in addition to usual way of notice such as by e-mail or on the website, in a case of emergency maintenance.

Moreover, cryptoassets custodians are RECOMMENDED to put forth an effort to minimize an affected area from a viewpoint of user protection in a case of service suspension caused by immediate issues such as attacks from external.

8. Future work

Discussion of distributed exchange (DEX) is currently out-of-the-scope of this document.

9. Security Considerations

Security Considerations are included in the main section of this document.

10. IANA Considerations

None.

11. References

11.1. Normative References

[ISO.27001_2013] International Organization for Standardization, "Information technology -- Security techniques -- Information security management systems -- Requirements", ISO/IEC 27001:2013, October 2013, <https://www.iso.org/standard/54534.html>.

[ISO.27002_2013] International Organization for Standardization, "Information technology -- Security techniques -- Code of practice for information security controls", ISO/IEC 27002:2013, October 2013, <https://www.iso.org/standard/54533.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

[BIP-0010] Reiner, A., "Multi-Sig Transaction Distribution", BIP 10, 28 October 2011, <https://github.com/bitcoin/bips/blob/master/bip-0010.mediawiki>.

[BIP-0011] Andresen, G., "M-of-N Standard Transactions", BIP 10, 18 October 2011, <https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>.

[CVE-2018-10299] MITRE Corporation, "CVE-2018-10299", CVE 2018-10299, 22 April 2018, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10299>.

[I-D.nakajima-crypto-asset-terminology] Nakajima, H., Kusunoki, M., Hida, K., Suga, Y., and T. Hayashi, "Terminology for Cryptoassets", Work in Progress, Internet-Draft, draft-nakajima-crypto-asset-terminology-04, 2 July 2020, <http://www.ietf.org/internet-drafts/draft-nakajima-crypto-asset-terminology-04.txt>.

[LISK-ISSUE_2088] MaciejBaj, ., "Check INT_32 range for transaction timestamps", June 2018, <https://github.com/LiskHQ/lisk/issues/2088>.

Acknowledgements

Thanks to Masanori Kusunoki, Yasushi Matsumoto, Natsuhiko Sakimura, Yuji Suga, Tatsuya Hayashi, Keiichi Hida, Kenichi Sugawara, Naochika Hanamura, and other members of the Security Working Group of CryptoAssets Governance Task Force.

Authors' Addresses

Masashi Sato
SECOM Co., Ltd. Intelligent System Laboratory
Shimorenjaku 8-10-16
SECOM SC Center, Tokyo, Mitaka
181-8528
Japan

Email: satomasa756@gmail.com

Masaki Shimaoka
SECOM Co., Ltd. Intelligent System Laboratory
Shimorenjaku 8-10-16
SECOM SC Center, Tokyo, Mitaka
181-8528
Japan

Email: m-shimaoka@secom.co.jp

Hirotaka Nakajima (editor)
Mercari, Inc.
Roppongi 6-10-1
Roppongi Hills Mori Tower 18F, Tokyo, Minato
106-6118
Japan

Email: nunnun@mercari.com