(Draft)



Key management of centralized custody

**

# 

# Introduction

This document explains

|  |
| --- |
| Text to be provided by Governance WG. |

# 

# Table of contents

[**Introduction**](#_1je30v6slvx) **2**

[**Table of contents**](#_449nw28pn5sf) **3**

[**1. Scope**](#_wck0xj18f0a1) **4**

[**2. Normative reference**](#_k0l7gypjirp) **4**

[**3. Terms and definitions**](#_hw5re93zqy4o) **4**

[**4. Abbreviations and symbols**](#_94rx0gilt6ii) **4**

[**5. Models of cryptoasset custody system**](#_rectvz5nqq1g) **4**

[5.1 Reference Architecture](#_1ddzni1erlk9) 4

[5.2 Information assets and cryptographic keys](#_z4mk1bgoy1xt) 5

[5.2.1 List of Information assets](#_c6uylt3craj4) 5

[5.2.2 Key Lifecycle](#_uu6lmn3tnlnq) 5

[**6. Incident response**](#_mndgom9hzlu2) **5**

[6.1 Responsible entities and framework](#_jfj97ljvq2on) 5

[6.2 Process](#_mztgwx6b1907) 5

[6.3 Tracing the stolen cryptoassets](#_u0td2v4t0r7h) 5

[**7. Identity management**](#_7mid4teqa8yx) **5**

[7.1. AML requirements](#_47q2zrjhvwwf) 5

[7.2. Privacy enhancing mechanisms](#_kfnvc1f622my) 5

[**8. Security considerations**](#_i0aygael3uc4) **5**

[**9. Privacy considerations**](#_wtu5eykzl62t) **5**

[**10. Regulatory considerations**](#_9c54v8y2fg6j) **6**

[**11. Informative reference**](#_1mzntpvl6vsl) **6**

[**Appendix A – Acknowledgement**](#_yb83ibahglw7) **7**

[A.1 Editors and Co-editors](#_5m8h2u463cbi) 7

[A.2 Contributors](#_myj72dkh1kz6) 7

# 

# 1. Scope

The covered party in this document is a custodian of cryptoassets that manages the signature key used in the cryptoassets system/ecosystem (including when the management of the signature key is entrusted to another custodian). For custodians entrusted only with the management of the signature key, a considerable number of this report's recommendations would be also applicable.

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

* Model(s) of cryptoasset custodians system that provides cryptoassets custodians work for customers (consumers and other exchanges)
* A list of information assets 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
* Key lifecycle and its management
  + Status control: especially suspended (not revoke)
* Threat model
* Incident response upon data breach
* Identity management with access control (privilege management)
* AML (FATF Travel Rule)
  + Audit
  + How well current cryptographic solutions and/or protocols satisfy the requirements of FATF for cryptocurrencies, and the limitations of existing solutions to satisfy FATF
* Other regulatory requirements (e.g. Japanese regulation, European MiCA)

This document does not focus on the following items.

* General security measures for information systems used for daily operations by custodians operators
* Security measures against blockchains that provide the mechanism of cryptoassets and distributed ledger itself
* Operator's own company management risk
* Specific requirements on separation of assets of customers and custodians/exchanges

Implications to stakeholders

* Engineers
  + Requirements for key management
  + Standard key protection mechanism
    - Protocol
    - Implementation (HW/SW)
  + Identity management mechanism
* Regulators
  + Points of audit
  + A guide for incident response
* Business entities
  + Agreed key management and operation process
  + Agreed identity management process
  + A guide for incident response
* Customers
  + Criteria to evaluate business entities

# 2. Normative reference

This document has no normative reference.

# 3. Terms and definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the term.

**3.1**

**term**

shortcut of the definition

# 4. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

BGIN Blockchain Governance Initiative Network

NOTE: All the abbreviations SHALL appear in this clause.

# 5. Models of cryptoasset custody system

## 5.1 Reference Architecture

## 5.2 Information assets and cryptographic keys

### 5.2.1 List of Information assets

### 5.2.2 Key Lifecycle

# 6. Incident response

## 6.1 Responsible entities and framework

## 6.2 Process

## 6.3 Tracing the stolen cryptoassets

# 7. Identity management

## 7.1. AML requirements

## 7.2. Privacy enhancing mechanisms

# 8. Security considerations

This document has no security considerations.

# 9. Privacy considerations

Acknowledgement section contains PII of those people. Editors SHALL make sure to obtain the consent of the people to be included. Sometimes, a contributor MAY want to remain pseudonymous and just appear as an initial etc.

# 10. Regulatory considerations

# 11. Informative reference

This document has no informative reference.

# 

# Appendix A – Acknowledgement

(Informative)

## A.1 Editors and Co-editors

* Yuji Suga (Internet Initiative Japan)

## A.2 Contributors