General Security Considerations for Crypto Assets Exchange
draft-vcgtf-crypto-assets-security-considerations-00

Abstract

This document discusses the threat, risk, and controls on the followings; Online system of crypto assets exchange that provides the exchange service to its customer (consumers and trade partners); assets information (including the private key of the crypto assets) that the online system of a crypto assets exchange manages; Social impact that can arise from the discrepancy in the security measures that are implemented in the online system of a crypto assets exchange.

This document is applicable to the crypto assets exchanges that manages the private key that corresponds to the crypto assets. It includes the organizations that outsources the key management to another organization. In such a case, the certain recommendations applies to those outsourcers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 9, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Scope of this document ....................................... 3
3. Conventions and Definitions ................................. 3
4. Terminology .................................................... 3
5. Basic description of a model online system of a crypto assets exchange ............................................... 3
   5.1. General .................................................... 3
   5.2. A basic model of online system of a crypto assets exchange and its functional components ............................. 3
5.3. The flow leading to the sending of the transaction ....... 4
5.4. Types of keys that are used for signature and encryption
   5.4.1. Type of keys ............................................. 4
   5.4.2. A flow for the key generation and the key usage ...... 4
   5.4.3. On the usage of multiple keys ......................... 4
   5.4.4. On the suspension of keys ............................. 4
5.5. On the characteristics of crypto assets on Blockchain and distributed ledger technologies ....................... 4
   5.5.1. General .................................................... 4
   5.5.2. The importance of the private key used for signing 4
   5.5.3. Diversity of implementations ........................... 4
   5.5.4. Risk on the unapproved transactions .................. 4
6. Basic objectives for the security management of crypto assets exchanges ............................................. 4
7. Approaches to basic security controls ........................ 4
8. Sector specific security management controls for crypto assets exchanges ............................................. 5
   8.1. General .................................................... 5
   8.2. On the direction of the information security management 5
   8.3. On the controls for key recovery .......................... 5
   8.4. On the controls against theft and leakage of the private key for signing .............................................. 5
   8.5. On the illegal operation of the private key for signing 5
   8.6. On the illegal operation against the assets data .......... 5
   8.7. On the user authentication .................................. 5
   8.8. On the withdrawal of the coins ........................... 5
   8.9. On the transfer of the crypto assets to an unused address 5
9. Remaining issues ........................................ 5
10. Security Considerations ............................... 5
11. IANA Considerations .................................. 5
12. Normative References ................................. 5
Appendix A. Contributors ................................. 5
Author’s Address ........................................ 6

1. Introduction

TODO Introduction

2. Scope of this document

In this document, crypto assets exchange operators which hold a private key of crypto assets.

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

- Wallet
- Fork of blockchain

5. Basic description of a model online system of a crypto assets exchange

5.1. General

In this clause, a model online system of a crypto assets exchange that is used to explain the concepts and provisions in this document are explained.

5.2. A basic model of online system of a crypto assets exchange and its functional components

Followings are the basic model of a crypto assets exchange that this document deals with.
5.3. The flow leading to the sending of the transaction

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

5.4.1. Type of keys

5.4.2. A flow for the key generation and the key usage

5.4.3. On the usage of multiple keys

5.4.4. On the suspension of keys

5.5. On the characteristics of crypto assets on Blockchain and distributed ledger technologies

5.5.1. General

5.5.2. The importance of the private key used for signing

5.5.3. Diversity of implementations

5.5.3.1. On the cryptographic algorithms used by crypto assets

5.5.3.2. On the possibility of the forking of the Blockchain

5.5.3.3. Rollback by reorganization

5.5.3.4. The treatment of the forked crypto assets

5.5.4. Risk on the unapproved transactions

5.5.4.1. General

5.5.4.2. The handling of the unapproved transactions

5.5.4.3. Transaction failures caused by the vulnerabilities of the implementation or the specification of the crypto assets

6. Basic objectives for the security management of crypto assets exchanges

7. Approaches to basic security controls
8. Sector specific security management controls for crypto assets exchanges

8.1. General

8.2. On the direction of the information security management

8.3. On the controls for key recovery

8.4. On the controls against theft and leakage of the private key for signing

8.5. On the illegal operation of the private key for signing

8.6. On the illegal operation against the assets data

8.7. On the user authentication

8.8. On the withdrawal of the coins

8.9. On the transfer of the crypto assets to an unused address

9. Remaining issues

10. Security Considerations

    TODO Security

11. IANA Considerations

    This document has no IANA actions.

12. Normative References


Appendix A. Contributors
Author’s Address

Hirotaka Nakajima
Mercari, Inc.

Email: hiro@awa.sfc.keio.ac.jp