ISO/TR 23576:2020 (E)

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

Contents

Foreword

Introduction

1 Scope

2 Normative reference

3 Terms and definitions

4 Abbreviated terms

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

5.1 General
5.2 Example of a system for digital asset custodians and its functional components
5.3 Examples of transactions
5.4 Description of keys used for signature and encryption
5.4.1 Type of keys
5.4.2 Flow for key generation and key usage
5.4.3 Using multiple keys
5.4.4 Suspension of keys
5.5 Characteristics of digital assets held in DLT / blockchain systems
5.5.1 General
5.5.2 Importance of signature keys
5.5.3 Diversity of implementations
5.5.3.1 General
5.5.3.2 Cryptographic algorithms of digital assets
5.5.4 Possibility of blockchain forks
5.5.4.1 General
5.5.4.2 Rolling back due to reorganisation
5.5.4.3 Handling forks of digital assets
5.5.5 Risks for unapproved transactions
5.5.5.1 General
5.5.5.2 Handling unapproved transactions
5.5.5.3 Transaction failure due to vulnerabilities from digital assets specifications and implementations

6 Basic objectives of security management for digital asset custodians

7 Approaches to basic security controls

8 Digital asset custodians' risks

8.1 General
8.2 Risks related to the system / platform of the digital asset custodian
8.2.1 General
8.2.2 Signature key risks
8.2.2.1 General
8.2.2.2 Risk analysis on signature keys
8.2.2.3 Risks of loss of signature key
8.2.2.4 Risk of leakage and theft of signature key
8.2.2.5 Risk of unauthorized use of signature key
8.2.2.6 Other risks — Hardware wallet (supply chain risk)
8.2.3 Risks on asset data

8.2.4 Risks related to suspension of systems and operations
8.2.4.1 General
8.2.4.2 Risks related to network congestion
8.2.4.3 Risk of system outage
8.2.4.4 Risks related to operators
8.2.4.5 Regulatory risks
8.3 Risks from external factors
8.3.1 General
8.3.2 Risks related to the internet infrastructure and authentication infrastructure
8.3.2.1 Internet routing and name resolution attacks
8.3.2.2 Attacks on web PKI
8.3.2.3 Attacks on messaging systems
8.3.3 Risks inherent to digital asset DLT systems / blockchains
8.3.3.1 Split or fork of a DLT / blockchain
8.3.3.2 DLT / blockchain reorganisation caused by 51 % attack or selfish mining
8.3.3.3 Compromising cryptographic algorithms and hash functions
8.3.3.4 Inadequate DLT / blockchain specifications and implementations
8.3.3.5 Rapid change in hash rate
8.3.4 Risks arising from external reputation databases and anti-money-laundering regulations
8.3.4.1 Establishment, elimination, and deactivation of bank accounts
8.3.4.2 Digital asset addresses
8.3.4.3 Filtering and blocking for web sites
8.3.4.4 Email
8.3.4.5 Appraisal of a smartphone application
8.3.4.6 ID theft

9 Consideration on security controls of digital asset custodians

9.1 General
9.2 Basis for considerations about security management
9.3 Considerations about security controls on digital asset custodians
9.3.1 Guidelines for the information security management
9.3.2 Information security policies
9.3.3 Organization of information security
9.3.4 Human resource security
9.3.5 Asset management
9.3.6 Access control
9.3.6.1 General
9.3.6.2 Access controls for operators and administrators
9.3.6.3 Access control for customers (user authentication / API)
9.3.7 Security controls on signature keys
9.3.7.1 General
9.3.7.2 Basics of key management
9.3.7.3 Detailed control in terms of backup
9.3.7.4 Offline key management
9.3.7.5 Key sharing and multisignatures
9.3.7.6 Procurement of hardware wallet
9.3.8 Physical and environmental security
9.3.9 Operations security
9.3.9.1 General
9.3.9.2 Protection from malicious software (related to ISO/IEC 27002:2013, 12.2)
9.3.9.3 Backup (related to ISO/IEC 27002:2013, 12.3)
9.3.9.4 Logging and monitoring (related to ISO/IEC 27002:2013, 12.4)
9.3.10 Communications security
9.3.10.1 General
9.3.10.2 Network security management (related to ISO/IEC 27002:2013, 13.1.1)
9.3.10.3 Network segmentation (related to ISO/IEC 27002:2013, 13.1.3)
9.3.10.4 System acquisition, development, and maintenance
9.3.11 Supplier relationships
9.3.12 Information security incident management
9.3.13 Information security aspect of business continuity management
9.3.13.1 General
9.3.13.2 Maintaining availability of the system
9.3.14 Compliance

9.4 Other digital asset custodian system specific issues — Advance notice to user for maintenance

Page count: 35