Completed projects in ISO/ TC 307/JWG 4

ITU Workshop on DLT security, identity management and privacy

Session 2: ***DLT security and privacy***

Geneva, Switzerland, 20 February 2023

julien.bringer@kallistech.com

JWG 4 - Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: **Security, privacy and identity for Blockchain and DLT**

- Published
  - ISO/TR 23244:2020 Privacy and personally identifiable information protection considerations
  - ISO/TR 23576:2020 Security management of digital asset custodians [from WG2]

- Also worked on various studies (e.g. security of smart contracts, Security Evaluation of Consensus Models, …)

julien.bringer@kallistech.com

ISO/TR 23244: 2020

- Blockchain and distributed ledger technologies — **Privacy and personally identifiable information protection considerations**

- **Scope**

  This document provides an overview of privacy and personally identifiable information (PII) protection as applied to blockchain and distributed ledger technologies (DLT) systems.

- **Publication date: 2020-05**

ISO/TR 23244: 2020

- **1 Scope**
- **2 Normative references**
- **3 Terms and definitions**
- **4 Abbreviated terms**
- **5 Privacy framework for blockchain/DLT systems**
  - **5.1 Overview**
  - **5.2 Interactions**
  - **5.3 Recognizing PII**
  - **5.4 Privacy safeguarding requirements**
  - **5.5 Privacy policies**
  - **5.6 Privacy controls**
  - **5.7 Privacy and identity management**
- **6 Privacy impact assessment**
  - **6.1 General**
  - **6.2 Privacy impact assessment as part of the overall risk management program**
  - **6.3 Privacy threats**
  - **6.4 Privacy vulnerabilities**
  - **6.5 Privacy consequences**
  - **6.6 Privacy risk mitigation strategies**
- **7 Privacy management in blockchain and DLT**
  - **7.1 General**
  - **7.2 Personal information management systems**
  - **7.3 Change management**
  - **7.4 Monitoring, review and continuous improvement**
  - **7.5 PII principal awareness**
  - **7.6 Privacy-related complaint handling**
  - **7.7 Decommissioning**
  - **7.8 Regulatory and compliance aspects**

ISO/TR 23244: 2020

- **1 Scope**
- **2 Normative references**
- **3 Terms and definitions**
- **4 Abbreviated terms**
- **5 Privacy framework for blockchain/DLT systems**
  - **5.1 Overview**
  - **5.2 Interactions**
  - **5.3 Recognizing PII**
  - **5.4 Privacy safeguarding requirements**
  - **5.5 Privacy policies**
  - **5.6 Privacy controls**
  - **5.7 Privacy and identity management**
- **6 Privacy impact assessment**
  - **6.1 General**
  - **6.2 Privacy impact assessment as part of the overall risk management program**
  - **6.3 Privacy threats**
  - **6.4 Privacy vulnerabilities**
  - **6.5 Privacy consequences**
  - **6.6 Privacy risk mitigation strategies**
- **7 Privacy management in blockchain and DLT**
  - **7.1 General**
  - **7.2 Personal information management systems**
  - **7.3 Change management**
  - **7.4 Monitoring, review and continuous improvement**
  - **7.5 PII principal awareness**
  - **7.6 Privacy-related complaint handling**
  - **7.7 Decommissioning**
  - **7.8 Regulatory and compliance aspects**

ISO/TR 23576:2020

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

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

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

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

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

  The following is out of scope of this document:

  — core security controls of blockchain and DLT systems;

  — business risks of digital asset custodians;

  — segregation of customer's assets;

  — governance and management issues.
- **Publication date: 2020-12**

ISO/TR 23576:2020

- digital asset custodian system

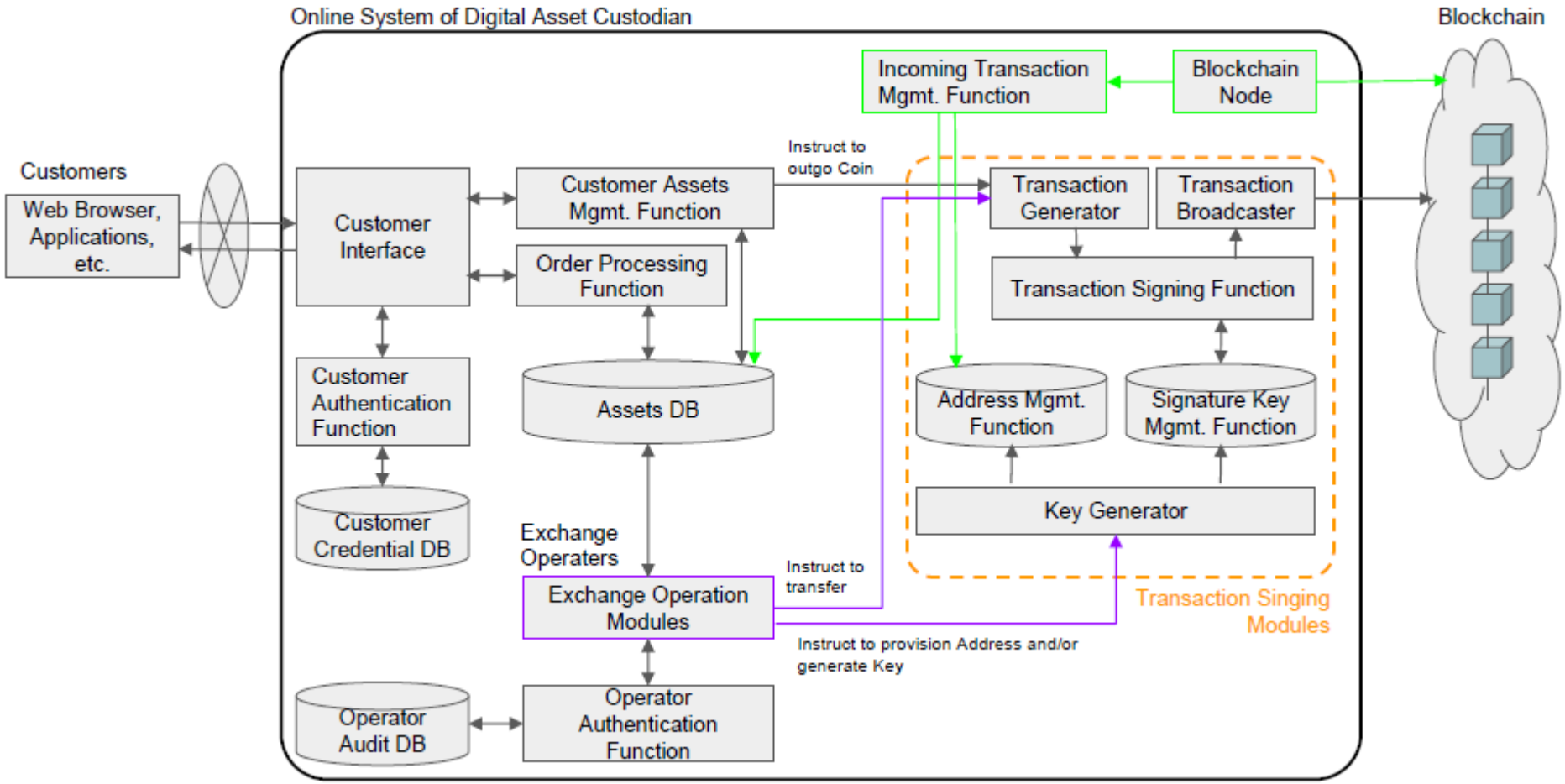
  system that holds customers' digital assets for safekeeping in order to minimize the risk of their theft or loss

- illustrates the security risks, threats, and measures which digital asset custodians consider, design, and implement in order to protect the assets of their customers,
  - based on best practices, existing standards and research.
  - For example, the management of signature keys for digital assets requires special attention

ISO/TR 23576:2020

- 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**
  - 5.5 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
    - **5.5.4 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**

julien.bringer@kallistech.com



julien.bringer@kallistech.com

ISO/TR 23576:2020

- 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
    - **8.3.3 Risks inherent to digital asset DLT systems / blockchains**
    - 8.3.4 Risks arising from external reputation databases and anti-money-laundering regulations

ISO/TR 23576:2020

- 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

ISO/TR 23576:2020

- 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

Thanks

julien.bringer@kallistech.com