TECHNICAL SPECIFICATION

ISO/TS 23526

First edition

Security aspects for digital currencies

PROOF/ÉPREUVE

Reference number
ISO/TS 23526:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

There is a need for the international financial community to recognize certain security measures and criteria to promote public trust in digital currencies. From a security and assurance perspective, protecting an ecosystem surrounding any type of digital currency ultimately protects and informs any future issuance goal of a fiat digital currency. Security aspects as they relate to cross-border transactions are to be compiled as well.

A look at the security horizon for digital currencies reveals a need to adjust and to add new capabilities, including a broadening of the business needs for banking and financial actions with security representing national and international uses. The financial landscape has expanded into the digital realm, causing a re-examination of traditional security technologies, while digital applications are constantly changing. Adding another digital dimension for secure payments and secure transactions with a digital currency pushes the security paradigms and adds a mix of threats that become real for every level of the financial ecosystem.

A security framework and assurance needs to recognize existing international financial ecosystems and their security components. A security framework is needed that international financial markets can select and adapt to their own needs.

Building a digital currency model can require a security framework that is not identified in this document and is yet to be determined.

Security aspects for digital currencies

1 Scope

This document specifies an acceptable security framework for the issuance and management of digital currencies using cryptographic mechanisms standardized by ISO/TC 68/SC 2 and other references.

This document proposes a framework approach based on standards for mitigating vulnerabilities for digital currency systems. The objective is that security aspects are integrated by design and not added afterwards as an extra processing layer that needs to accommodate legacy infrastructures.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
central bank digital currency
CBDC
central bank digital money
digital representation of cash, issued by the central bank and a claim on the central bank

3.2
crypto asset
digital asset (3.4) implemented using cryptographic techniques

[SOURCE: ISO 22739:2020, 3.13]

3.3
cryptocurrency
crypto-asset (3.2) designed to work as a medium of value exchange

[SOURCE: ISO 22739:2020, 3.14, modified — Note 1 to entry removed.]

3.4
digital asset
asset that exists only in digital form or which is the digital representation of another asset

[SOURCE: ISO 22739:2020, 3.20]

3.5
digital currency
digital representation of monetary value

3.6
distributed ledger
ledger that is shared across a set of distributed ledger technology nodes and synchronized between the distributed ledger technology nodes using a consensus mechanism

[SOURCE: ISO 22739:2020, 3.22, modified — Note 1 to entry removed.]

3.7
distributed ledger technology
DLT
technology that enables the operation and use of distributed ledgers

[SOURCE: ISO 22739:2020, 3.23]

3.8
fiat digital currency
digital currency model representing a debt of a central bank that can be redeemed with fiat money and mutually exclusive to non-fiat digital currency

3.9
non-fiat digital currency
digital currency model governed by a business contractual relationship between the user and the issuer of the digital currency, whose value is not guaranteed by a central bank and is mutually exclusive to fiat digital currency

3.10
identity-security
identity capabilities which can be used for associating an action or an individual to an event which performs some security access protection

3.11
envelope security
secure encapsulated access control capability with cryptography and additional security features

3.12
security framework
framework which defines policies and procedures for establishing and maintaining security

4 Considerations on security framework for digital

4.1 General

This document establishes the foundation for a security framework for digital currencies, in anticipation of the future development of an International Standard.

A standard security model is required to manage digital currencies that can utilize global security practices and adapt to local regulations. The security model can be designed as a series of interacting modules implementing security controls under the responsibility of entities playing a predefined role. This security model could be extended to encompass and to protect existing financial applications using digital currencies, either fiat or non-fiat. As a framework, the security model offers interoperability of information exchange as well as support for multiple currency objects, each supporting their own security process.

The international financial community has undertaken many existing infrastructure investments in which the introduction of security has historically been a major burden and easily deferred. However, international financial organisations have experienced a growth in digital threats to payments, to transactions and to other forms of financial exchanges.

The security framework can be customizable by international financial markets to meet their individual requirements, instead of treating security as a one-size-fits-all solution. The goal is to establish an

international trusted financial infrastructure based on a collection of national financial architectures to include all stakeholder members.

4.2 Security considerations for processing digital currencies

Security considerations for processing digital currencies include:

— the need to agree on the security objectives for digital currency systems;

— the roles required to manage a digital currency system;

— the provision of controlled access to repositories of digital currencies, such as wallets;

— the conflicts between confidentiality and anonymity for users of digital currencies and the desire of regulators to control transactions;

— the integrity or assurance of non-alteration of digital currency units;

— the nature of the personal security credentials or attributes (e.g. cryptographic keys, authentication elements and certificates) used to generate evidence of a particular operation involving digital currencies;

— risk impact assessment of different alternatives to process digital currencies;

— functional engineering considerations: availability of infrastructures and appropriate personal devices to load and pay with digital currencies in a convenient way, including transaction speed and the portability of digital currency unit aspects.

4.3 Variations of security frameworks

4.3.1 Non-fiat digital currency (digital asset) security framework

International financial services have expanded the role of virtual currencies to account for the multiple definitions and models that have surfaced of what can be considered as non-fiat digital currencies within the context of digital assets. Cryptography has been a major enabler for security among the non-fiat digital currencies.

Bitcoin emerged early in the formation of virtual currencies with a commercial generation of its currency aspect (i.e. a commercial monetary infrastructure as a potential cryptocurrency).

Other digital currency models evolved that relate to a digital form of a national currency with an emphasis on cryptography. Stablecoins were created to bridge the gap between cryptocurrencies and national currencies without their own security protection. Stablecoins that were pegged to a national currency without their own security measures were unstable in currency exchanges. To improve the security of stablecoins and address the risk and liability for national currencies, security features outlined herein are required. Once security considerations are addressed, stablecoins can evolve into a digital version of physical cash, with security measures provided by a central authority.

International banks are examining and developing their own digital currency methodologies, which can include cryptocurrencies with security and stablecoins. A collective body of banks and financial institutions are included in central bank digital currency (CBDC) efforts.

4.3.2 Creating a national digital currency with an anonymity security framework

Before the digital format was available, physical money based on ISO 4217 as a national designation was the primary means of financial exchange. The Central Authority as a Central Bank minted the money and included various analogue security technologies and techniques with the intent of preventing fraud. The advent of the digital format has shifted the focus to alternative usages, which in turn has created new security paradigms. Security can be directed towards the digital representation of currency or towards a digital use case that involves currency representation. Digital currency can be seen as digital

cash with security properties resulting in anonymity, either for one counterparty to a transaction (e.g. the consumer) or for both counterparties to a transaction. The degree of anonymity associated with digital currency, and which counterparties have anonymity, can have legal and liability implications wherein security can play a role.

4.3.3 Secure digital cash as digital currency with consumer identity security framework

Identity security can be extended beyond the digital currency boundary to include a consumer or equivalent that would be a party to a payment or a transaction. Digital currency can be digital cash that includes inherent security features and a separate layer of identity security, perhaps for the digital application associated with a financial payment or to link the transaction and the consumer.

The security framework can serve as the basis for an international trusted financial infrastructure based on a collection of securely integrated national financial architectures that includes all stakeholders.

4.4 Overview of security frameworks

4.4.1 General

A security framework should include the current security best practices of technologies and advancements within standards to address:

— the business model leveraging digital currencies for commercial banks;

— agreed consensus for a security and assurance architecture to cross international borders with digital currencies;

— a security paradigm which can deliver security for a whole dimension of the IT/security international digital currency architectures.

4.4.2 Standards as a basis for security frameworks

The realm of digital currencies and their security aspects is contained in banking security standards which are identified in ISO standards. Other standards bodies exist which could be used by central authorities to complement ISO standards where the additional security capabilities are sought.

5 The emergence of currency in digital formats

5.1 Digital cash representing money as a basis for financial usage with security

Digital cash (also cited as central bank digital money) can be viewed as an emulation of a current physical national currency, such as dollars, euros or yuan, with their security (and, optionally, identity-security references) present with usage. Legal aspects and rules associated with financial practices can be the basis for putting digital cash into practice. Like a reserve currency, digital cash can have an integrity-security envelope for itself that can index a digital relationship with identity-security to extend the digital cash into digital applications and to add digital asset value. Technologies are available to offer security for different environments from a currency-only environment to currency with differing digital application environments that can include the individual. A national body establishes direction for defining digital cash as currency and to establish security technologies with digital platforms. The result of a digital cash architecture and its associated security is to create trust acceptance in practice.

Before the digital format was available, physical money was the primary means of financial exchange. The central authority as a central bank minted the money and included various analogue security technologies and techniques with the intent of preventing fraud. The advent of the digital format has shifted the focus to alternative usages, which in turn has created new decisions for the use of security paradigms. The extent of security technologies can have a limited role, focusing on privacy and security, or a broader role, with a fiat digital representation of currency. With either representation, security can

be included without the consumer or an equivalent being identified. Security can be the focus of an internal anti-fraud role within a digital form of money. In the case of digital representation of money, security focuses on the digital currency entity and not any application using the digital currency. Digital currency can be seen as digital cash with a potential level of containment-security protection, while maintaining anonymity. The anonymity associated with digital currency can have legal liability boundaries. Minting of this digital currency and its distribution is outside the scope of this document.

User-linked digital cash as digital currency with identity can be extended beyond the digital currency boundary to include a consumer or equivalent that would be a party to a payment or a transaction. Digital currency can be digital cash that includes inherent security that a separate layer of security is included for the digital application associated with a financial payment or a financial transaction.

Existing security tools and techniques can be applied to digital cash without consumer identity.

The following documents describe existing standards and security technologies that are relevant to digital currencies:

— the ISO 13491 series;

— ISO/TR 13569;

— ISO/TR 14742;

— the ISO/IEC 15408 series;

— ISO 16609;

— ISO/IEC 17799;

— ISO/IEC 18028;

— the ISO/IEC 18033 series;

— ISO/IEC 18045;

— ISO 19092;

— the ISO/IEC 19989 series;

— ISO 20038;

— ISO/TR 24374.

5.2 Cryptocurrencies as a digital entity for financial usage

For several years, private cryptocurrencies have been emerging in both national and international financial markets. They are the result of central bank authorities exploring the feasibility for a digital currency role in their financial ecosystem. The history of the subject has been constantly evolving.

It needs to be recognized that the subject of digital currency can be complex, with various definitions and differing security directions from international central authorities and commercial bodies.

The choice of including a cryptocurrency requires consideration of the value of security to the policy and the legal boundaries that exist. A security profile needs a relationship to a financial business model which is trusted and accepted by the international community. The following overview is an introduction to the role(s) for cryptocurrency, with an intent to present an international input with security for a fiat digital currency or a private digital currency solution with its security. To begin, technology is influencing direction for advancing a digital currency solution. Within the international financial markets, there are established financial ecosystems. In parallel, there are new or nearly new financial entities which are advancing. Existing financial entities have established policies, technologies and ecosystems that represent an economic capability and investment. Changes to their economic