TECHNICAL SPECIFICATION

ISO/TS 23526

First edition
2023-09

Security aspects for digital currencies

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 capability with new security paradigms, as would be associated with a cryptocurrency, will result in a value of security to the overall national objective.

5.3 Cryptocurrencies and the digital currency market challenges

Technology innovation is transforming the context of financial services and products so that currencies in a digital format are used or can be used.

Digital currency can be a representation of monetary value used for payment. The digital currency can be identified as a fiat version representing a government or central authority submission. International efforts, such as CBDC, are bringing forth various cryptocurrency choices that can be modelled for a fiat digital currency solution. The international financial markets are also exhibiting private cryptocurrency that includes their payment and transaction capabilities with their security paradigms.

This document recognizes that cryptocurrencies present significant challenges, such as:

— the presence of cryptocurrencies as non-fiat digital currencies;

— a mix of international financial central authorities surfacing with their national representations through CBDC efforts;

— continuous, additional threat and fraud from digital ecosystem platforms;

— an advancement by a national body to shift the current monetary market position;

— the potential for a digital currency basket, in which multiple national bodies include currencies to offer consumers an assortment of digital currency choices;

— a financial market that envisions technology innovations as an avenue for less costly transactions with expanded business opportunities, while addressing these challenges;

— an established fiat financial architecture that sees the advantage of an additional digital cryptocurrency application for supplemental economic gain.

5.4 Cryptocurrencies and financial market formats

Cryptocurrencies can include various financial market formats. A stablecoin can be considered a crypto asset which seeks to stabilize a price with a "coin", a "token" or an "account", by linking value to that of a pool of assets and/or with a national currency, which can serve as a means of payment and store of value. It could be viewed as a different business case version of a payment vehicle that can have a fee associated with the stablecoin reference beyond an application service fee. As an example, Bitcoin has been present for a longer period and can represent a commercial value proposition associated with only their coin and no linkage with any national entity.

The national currency can be represented by digital cash, as detailed in 6.1. The digital cash is the store of value identified by the stablecoin. Stablecoin could cite the specific digital assets which can be included as an accounting entity with security enforcement to ensure equity among transactions with national recognition for a monetary representation in a digital format.

Other financial market formats can be seen with CBDC. Documents from the Bank of England and other central banks have been published that could provide households and business with suggestions for central bank money (fiat). Moving to advanced digital applications for financial application usage can establish a parallel digital form for making financial payments and financial transactions. The intent is to have a digital form of money that can parallel a reserve currency of a national entity and include security capabilities that can be the basis for trust from the central authority through a financial ecosystem to the consumer. A CBDC design would include potential capabilities for a digital wallet as a digital means of payment and transactions and, in short, take advantage of new digital financial offerings with a means of fulfilling a central bank's role within a financial ecosystem. Security measures need to be incorporated to support the evolving digital capabilities or security must be considered as a protective layer for CBDC capabilities that align with the security paradigm of the current financial ecosystem.

Another financial market data and messaging format in use by financial entities is the ISO 20022 series. ISO 20022 digital messages are integrated with digital financial applications. The ISO 20022 series covers electronic data interchange between financial stakeholders. It describes a metadata repository containing descriptions of messages and business processes and a maintenance process for the repository content. The international financial community has been advancing ISO 20022 messaging among national bodies to extend a common means of exchanging financial messaging. It can be viewed as an important step to establish a common interoperability to have cross-border payments and transactions. To complement the advancements cited in this document, the International Telecommunications Union (ITU) is advancing their standard security work for digital currencies. Security can be exhibited directly with the ISO 20022 exchanges with cryptography for designated access control and data protection. In summary, ISO standards could define specific security criteria for use with ISO 20022 messages.

Security is integral to all banking financial transactions. The advent of new digital formats will still require security. It has been said that security in digital formats offers a greater degree of assurance for protection and faith in existing and future capabilities. In discussions regarding cryptocurrencies, questions always arise that involve trade-offs where security can be a distinguishing factor. A cryptocurrency with its associated security can be recognized by a central authority based on its security framework, along with other factors. Does the business case for security technologies and security techniques apply to a central authority’s goals? Existing ISO banking standards, and potentially additional standards, need to be considered. Trust in a currency depends on security and associated standards.

5.5 Cryptocurrencies and banking regulation – stablecoin example

An assortment of commercial and national bodies are advancing efforts to qualify cryptocurrency with regulatory guidance which can imply a level of security is needed to result in trust. In the background are world monies as currencies identified in ISO 4217 and their national body supporting physical currency infrastructures. There is a desire to include digital currencies in ISO 4217 to gain international trust and acceptance across borders. Security aspects are available with the digital currency representation that can be included in ISO 4217 to parallel the analogue ISO 4217 currency versions.

In a broad context, ISO standards are included in various security aspects which can be identified with access control, identity, authentication, authorization and other IT capabilities related to security operations. Each identified security framework can have a role with its security aspects.

The following is an example of a stablecoin module for digital cash with its security aspects:

ISO 4217 currency three-character designation/ISO 4217 digital currency one-character symbol identified by a central authority/one or more identity-security designations for counter-fraud, for example, to identify the transaction recipient.

Additional identity security aspects and security techniques associated with cryptocurrencies and digital cash are included in the following documents:

- ISO/TR 24374;
- the ISO 17442 series;
- ISO 6166;
- the ISO 24165 series

Other security technologies and techniques with their standards from the Bibliography can be used.

A stablecoin module that includes security tools that execute digital functions for encryption and additional identity verification and authentication is available. A financial payment or financial transaction would include the encrypted payment or transaction with a prearranged stablecoin representation. The resultant coded exchange would contain the necessary information to do decryption from the cryptography and authenticate with the security capability so that a central authority can execute at a known security profile. Within authorization, the stablecoin with its security module can represent a fungible digital currency form for digital cash money, a digital coin or token for money, or a digital account payment or transaction for money.

5.6 Security criteria representing security aspects

5.6.1 Security objects

A digital currency will require an internationally agreed identifier that parallels the kind specified in ISO 4217.

A digital currency framework for a central authority or distributed authority should include an external identity reference. The identity reference can parallel designations that are identified in ISO 4217, such as USD for United States dollar, and be represented in a digital format. Furthermore, in addition to the code designation for a country, a designation is needed for a fiat digital currency, such as a 4217 symbol with a '$' representing a digital form of a virtual currency representation. The symbol, in addition to a 4217 national code designation, is identified in ISO 4217.

Security standards exist to provide an international representation for digital assets in various identities. A central management is needed to maintain continuity and current business case linkages within a stablecoin usage.

Object-based cryptography establishes the security boundaries and security functions necessary for protection and access control to data associated with the security framework.

5.6.2 Key management

A digital currency can be considered a retail action in which principles of key management identified in an SC2 retail bank security standard ISO 11568 is suggested in the formation of implementing cryptography in the digital currency framework. Other ISO security mechanism standards are to be evaluated by a central authority to determine a use for their specific national effort.

5.6.3 Hiding and steganography techniques

Security techniques that are not cited in ISO standards should be assessed in parallel with cryptography and other security mechanisms. Hiding and steganography techniques which can be found in physical-analogue money as currencies may be included in a binary representation to complement cryptography in a digital form.

5.6.4 Digital representation

A digital currency can be an abstract representation of currency in binary code. A digital representation should be established to make it useful for all who want to apply their digital currency in digital applications.

5.6.5 Digital model

A digital platform for a digital currency can include a form of hardware representation with complementary security. In a financial ecosystem, the smart phone, smart tokens and other digital containers are put forth. It is necessary to have a digital currency model which can be applied to all or most of these platforms to offer a universal digital model that can be used by a variety of personal use cases. Another technology that should also be examined for a digital currency platform is a QR code with its security functionality representation. The QR code could be associated with a hardware platform.

5.6.6 Security countermeasures

Security countermeasures are needed for the digital platform to prevent threats to gain access to the digital representation hosted by the digital platform. A secondary countermeasure level should be considered to provide additional protection for the selected countermeasure platform, in addition to countermeasures associated with the digital currency itself.

5.6.7 Legal and regulatory requirements

The protection associated with the selected platform needs to consider abstract and legal requirements such as privacy and liability. Both privacy and liability are essential to an international acceptance of a future digital currency and its associated security, which can be used across national borders. The selection of the discussed security aspects can impact policy associated with both privacy and liability. Security aspects required by law must be incorporated into the security framework.

5.6.8 Trust

Trust is essential for a central authority to implement a national effort for a digital currency. Security is a necessary ingredient to have that trust. The selection of security aspects and its binding to everyday uses will visibly demonstrate to the national citizens that the economic basis for security is important.

5.6.9 Chaining security processes

Trust can be viewed as a measurable event and a concept of chaining security processes can have advantages. Chaining security processes can ensure that steps found in executing security include a validated model to counter threats. Instead of individual security pieces representing a security aspect, a chained or bound set of security pieces can make a more formidable shield for a future digital currency.

5.6.10 Security framework implementation

The security framework is to be executed in digital hardware platforms in the form of software or hardware. The hardware platform needs to ensure the operation of an application and to ensure that the operation can be independent of the security components associated with the application.

5.6.11 Platform independence

The hardware platforms (e.g. mobile) should ensure that operation of the application associated with a digital transaction is independent of the security components that can be provided by the currency format itself.

5.6.12 Existing good practices

An ENISA report cites various good security practices[29] that are associated with key management, cryptography, privacy, denial of service, scalability, governance controls and interoperability. International standards bodies such as ISO and ITU have various standards that include specifics for good practice. Also, national standards bodies such as ANSI and NIST include various standards that include specifics for good practices.

5.6.13 Digital interfaces

A digital currency might need to interface with potential digital applications that can employ security to use a digital currency for financial services and other currency needs. The digital interface(s) can be software or firmware based, and the framework process can operate indifferently to the digital financial currency representation. Other security technologies and techniques with their standards from the Bibliography may be used.

6 Critical areas for security to establish trust, acceptance and risk

6.1 Digital wallets

A digital wallet, also known as an e-wallet, refers to an electronic device or online service that allows an individual to make electronic transactions. This can include e-commerce transactions via the internet or point-of-sale purchases made using a physical device. Wallets can be custodial, for example, linked to a user's bank account, or non-custodial, provided by the user and to which money can be deposited prior to any transactions. Non-custodial wallets can be anonymous if the user of the wallet is not identified. The security credentials can be passed to a merchant's terminal wirelessly via near field communication (NFC).

Many usages for digital wallets require security: hosted or non-hosted, native or third-party, mobile, desktop or online. The digital wallet should offer the assurance of dependable operation and the application or currency medium should support its own security, independent of the wallet environment.

Digital wallets capabilities:

- enable input and storage of cryptographic keys to ensure that the keys are always under the control of the owner of the assets;
- perform error or format checks;
- generate encryption keys for a payment or transaction action.

Threats to the digital wallet security profile:

- complexity of wallet options;
- malware (e.g. a browser extension);
- loss of security cryptographic signing key or cryptographic encryption secret key;
- hosted service crashes;
- Trojan wallets deploying command and control;
- ledger malware enabling redirection of funds through address spoofing;
- out-of-date firmware;
- user and password problems;
- denial of service attack.

Trust-related considerations for digital currency consumers or users:

- have necessary knowledge;
- establish a secure digital wallet;
- create and securely store cryptographic secret keys for accessing financial funds;
- enable multi-factor and federated authentication as a consumer;
- a hardware security module may be used.

Potential threats to consumer digital platforms:

- fraud;
- poor identity and authentication;
- technical attacks;

- social engineering to exploit human faults;
- bad code;
- phishing schemes, social engineering, trolling to obtain secret keys by hackers.

6.2 Specific security considerations

Digital currency security requirements for merchant processors:

- maintain a cryptographically secure platform with supporting application programming interfaces (APIs);
- consumer identity security and merchant authentication.

Potential security technologies and standards that may be used for a digital wallet security profile are provided in Reference [37].

6.3 Digital currency financial security framework considerations

The following is a list of items related to alternative security frameworks that can support financial ecosystems, which includes the use of digital cash with security support, a collection of framework items, envelope security, cross-border financial payments with digital currency security and unique security levels based on ISO or other standards.

- Addition of alternative security frameworks to support financial ecosystems.
- Currency in the form of digital cash with security support.
- Collection of framework items with one or more security frameworks. This can include consumers with identity security, non-custodial digital wallets, anonymous digital wallets, secure digital wallets, secure digital devices, merchant processing, digital currency exchange, ATMs for exchanging digital currency, banks, financial institutions or computing networks.
- Envelope security that can align digital objects of digital wallets and other digital financial capability with security needs.
- Cross-border financial payments and transactions with digital currency security frameworks.
- Level of security can be considered unique to a secure financial implementation based on ISO or other accepted standards.

7 Fraud and threat considerations

Criminals are becoming more sophisticated in their use of malware to command online banking logins via telephones, tablets and computers, using stolen bank account details to make fraudulent payments. In additional to malware, criminals are using ransomware as identified with its techniques in financial articles. Potential threats to security frameworks include:

- creation of new units of digital currency without any underlying value or backing, commonly referred to as “out of nothing” (ex-nihilo);
- modification of the value transferred using digital currency units;
- modification of the structure of digital currency unit making it unacceptable;
- double spending of digital currency units;
- theft of stored digital currency units;