ISO/PRF TS 23526

ISO/TC 68/SC 02/WG 17 2

Secretariat: BSI

Date: YYYY-MM-DD2023-07-19

Security Aspectsaspects for Digital Currenciesdigital currencies

FDIS stage

~~**Warning for WDs and CDs**~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

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

Published in Switzerland

Contents

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/~~TC68~~TC 68, *Financial* ~~Services~~*services*, Subcommittee SC 2, ~~Information Security, Working group WG 17, Security aspects of digital currencies~~*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

~~The~~There is a need for the international financial community ~~should recognise~~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 ~~the financial services~~ digital currencies ~~surfaces~~reveals a need to adjust and to add new capabilities ~~that include~~, 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 ~~that has caused~~, causing a re-examination of ~~what has been~~traditional security technologies ~~that have years of use~~, while ~~the~~ digital applications are constantly changing. Adding ~~an additional~~another digital dimension for secure payments and secure transactions with a digital currency pushes the security paradigms and ~~adding~~adds a mix of threats that become real for every level of the financial ecosystem.

A security framework and assurance ~~should~~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.

~~To build~~Building a digital currency model can require a security framework that is not identified in this document~~. An example of a security framework that~~ and is ~~not included in this document is~~yet to be determined.

Security ~~Aspects~~aspects for ~~Digital Currencies~~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 ~~is intended to propose~~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~~(en),~~ 3.13]

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

[SOURCE: ISO 22739:2020~~(en),~~ 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~~(en),~~ 3.20]

3.5
digital currency
digital representation of monetary value

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

[SOURCE: ISO 22739:2020~~(en),~~ 3.~~60~~]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~~(en),~~ 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

~~An international standard regarding~~ This document establishes the foundation for a security ~~and its aspects for a digital currency should be aligned with an effort to have a common reference model~~ framework for ~~multiple independent digital currency representations.~~

~~Coupled to the security criteria, there is a need for a standard security model for the management of~~ digital currencies ~~which can take advantage~~, in anticipation of the future development of an International Standard.

A standard security~~, ideally,~~ model is required to manage digital currencies that can utilize global security practices and ~~of~~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 ~~pre-defined~~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.

Security frameworks with their security technologies and components are anticipated. AThe security framework is needed thatcan be customizable by international financial markets can select and adapt to meet their own needs and not treat the subjectindividual requirements, instead of treating security aspects as a one design for -size-fits-all frameworkssolution. 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:

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

— Thethe roles required to manage a digital currency system;

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

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

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

— Thethe 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;

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

— Functionalfunctional engineering considerations: Availabilityavailability of infrastructures and of 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 currenciescurrency (digital assetsasset) security framework

The internationalInternational financial services have expanded athe role for aof virtual currencycurrencies to account for the multiple definitions and models that have surfaced forof what can be considered as non-fiat digital currencies with awithin the context asof digital assets. Cryptography has been a major enabler for security among the non-fiat digital currencies:.

EarlyBitcoin emerged early in the formation of a virtual currency emerged Bitcoin 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 ofon cryptography. The notion of a stablecoin designation emerged as a bridging mechanism for cryptocurrency digital currency model with a stated Stablecoins were created to bridge the gap between cryptocurrencies and national monetary designation that wascurrencies without *its*their own security protection. Stablecoins with a 1:1 ration of a tokenthat were pegged to a national currency ratio without itstheir own security criteria was volatilemeasures were unstable in currency exchanges. A missing