International Standard

ISO 13133

Financial services — Security reference model for digital currency hardware wallet (SRM-DCHW)

Services financiers — Modèle de référence de sécurité pour les portefeuilles matériels de monnaie numérique (SRM-DCHW)

First edition
2026-09

Reference number
ISO 13133:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

Users are stepping away from cash payments in favour of electronic payments. Many central banks and monetary authorities conduct research on and pilot digital currencies (DCs) issued by a specific entity such as a central bank [referred to as "central bank digital currencies (CBDCs)" in this document] to safely and conveniently:

— provide access to public money;

— maintain the characteristics of a cash-like experience;

— protect the privacy of users [23], [24], [25], [26].

CBDCs are not intended to replace cash, but rather to complement cash and provide a backup to existing payment tools. For example, CBDCs can be designed to maintain critical payment functionality in the event of service disruptions, poor network coverage or natural disasters. CBDCs can also improve financial inclusion, providing better access to financial services for the underbanked, unbanked, elderly and others. They can also facilitate innovation, bringing new features and services to the ecosystem through the adoption of appropriate technologies and designs.

Multiple central banks are considering introducing DCs in digital wallets. This has led to the establishment of global standards to provide clear guidelines for mitigating circulation and payment risks associated with these DCs. These standards are expected to be based, to the greatest extent possible, on existing financial industry security standards and best practices.

This document outlines a DC wallet that can be embodied in, e.g. an integrated circuit card (ICC) or a commercial off-the-shelf (COTS) mobile device. While commodity smartphones can be used as wallets, the sensitive data and code of the wallets can reside within hardware devices, known as digital currency hardware wallets (DCHWs).

This document focuses on hardware wallets for sovereign or fiat DCs issued by a specific entity, e.g. a central bank.

This document does not require a specific architecture. It uses a two-tier model as an illustrative example. In this model, the central bank issues CBDCs and manages the supply, while intermediaries are responsible for distributing CBDCs to end users and supporting CBDC payments.

The purpose of this document is to facilitate the secure design and implementation of DCHWs.

It is recommended to use ISO 31000 as a risk management framework reference and accordingly conduct a detailed and specific assessment of the threat impact, threat likelihood, etc.

Financial services — Security reference model for digital currency hardware wallet (SRM-DCHW)

1 Scope

This document provides a taxonomy, reference model, considerations for a security framework and a security problem definition for digital currency hardware wallets (DCHWs). It also specifies security objectives to address security issues related to the security problem definition.

This document is applicable to organizations that develop and operate DCHWs, e.g. mobile device manufacturers, chip manufacturers and companies that provide DCHW solutions. This document is also relevant to third parties that provide services to these stakeholders. It addresses sovereign or fiat digital currencies issued by a specific entity, e.g. a central bank.

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
access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO 27789:2021, 3.1]

3.2
asset
anything (e.g. sensitive data) that has value to a stakeholder of a digital currency hardware wallet (DCHW), which is processed, stored, transmitted and protected against unauthorized disclosure, alteration or destruction

3.3
attack
successful or unsuccessful unauthorized attempt to destroy, alter, disable or gain access to an asset or any attempt to expose, steal or make unauthorized use of an asset

Note 1 to entry: Attacks can also involve attempts to illegitimately create assets.

[SOURCE: ISO/IEC 27002:2022, 3.1.3, modified — Note 1 to entry has been added.]

3.4
central bank digital currency
CBDC
new form of central bank money in a digital format, denominated in the national unit of account, that is a direct liability of the central bank and can be used for either retail payments or wholesale settlement or both

3.5
counter, verb
act on or respond to a particular threat so that the threat is eradicated or mitigated

[SOURCE: ISO/IEC 15408-1:2026, 3.29]

3.6
digital currency
DC
digital version of money that has the basic functions of money, e.g. unit of account and medium of exchange

3.7
digital currency hardware wallet
DCHW
hardware wallet that facilitates digital currency transactions

Note 1 to entry: This document focuses on hardware wallets for sovereign or fiat digital currencies issued by a specific entity, e.g. a central bank.

3.8
hardware security module
HSM
secure cryptographic device (SCD) that provides a set of secure cryptographic services

Note 1 to entry: Secure cryptographic services can include key generation, cryptogram creation, personal identification number (PIN) translation and certificate signing.

[SOURCE: ISO 13491-1:2024, 3.12]

3.9
hardware wallet
wallet which leverages a hardware device to generate, manage, store or use cryptographic keys or cryptographic data

EXAMPLE A secure cryptographic device, a secure element or a trusted execution environment.

[SOURCE: ISO/TR 23576:2020, 3.4, modified — The example "(e.g. HSM)" has been deleted, "private and public key" has been replaced with "cryptographic keys or cryptographic data" and the EXAMPLE has been added.]

3.10
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability, can also be involved.

[SOURCE: ISO/IEC 27000:2026, 3.1, modified — Note 1 to entry has been added.]

3.11
integrated circuit card
ICC
IC card
card into which one or more integrated circuits have been inserted

3.12
operating system
OS
software that controls the execution of programs and that can provide services such as resource allocation, scheduling, input-output control and data management

Note 1 to entry: Although operating systems are predominantly software, partial hardware implementations are possible.

[SOURCE: ISO/IEC TR 13066-6:2014, 2.12]

3.13
organizational security policy
OSP
set of security rules, procedures or guidelines for an organization

Note 1 to entry: A policy can pertain to a specific operational environment.

[SOURCE: ISO/IEC 15408-1:2026, 3.68]

3.14
private key
key in an asymmetric key pair which is known only by that entity

[SOURCE: ISO 11568:2023, 3.69]

3.15
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage and which can be integrated into a larger system, such as an automated teller machine or point of sale terminal

EXAMPLE Personal identification number entry device or hardware security module.

[SOURCE: ISO 13491-1:2024, 3.18]

3.16
secure element
SE
tamper-resistant component capable of securely hosting and executing applications and associated confidential and cryptographic data (e.g. key management)

[SOURCE: ISO 5201:2024, 3.20, modified — The term "platform in the mobile device" has been replaced by "component".]

3.17
security objective
statement of an intent to either counter identified threats or satisfy identified organization security policies or assumptions, or both

[SOURCE: ISO/IEC 15408-1:2026, 3.82]

3.18
security problem definition
SPD
statement that defines the nature and scope of the security that the target of evaluation (TOE) is intended to address

Note 1 to entry: This statement consists of a combination of: threats to be countered by the TOE and its operational environment, the organizational security policies (OSPs) enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.

Note 2 to entry: SPD elements include threats, OSPs and assumptions.

[SOURCE: ISO/IEC 15408-1:2026, 3.83]

3.19
sensitive data
sensitive information
data which need to be protected against unauthorized disclosure, alteration or destruction

EXAMPLE Status information, cryptographic key, personal identification number.

[SOURCE: ISO 13491-1:2024, 3.20]

3.20
target of evaluation
TOE
set of software, firmware, hardware, or a combination of these, possibly accompanied by guidance, which is the subject of an evaluation

[SOURCE: ISO/IEC 15408-1:2026, 3.93]

3.21
TOE security functionality
TSF
combined functionality of all hardware, software and firmware of a target of evaluation (TOE) that is relied upon for the correct enforcement of the security functional requirements

[SOURCE: ISO/IEC 15408-1:2026, 3.95]

3.22
TSF data
data for the operation of the target of evaluation upon which the enforcement of the security functional requirements relies

[SOURCE: ISO/IEC 15408-2:2026, 3.13]

3.23
threat
potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27032:2023, 3.21]

3.24
transaction key
key used to cryptographically protect the transaction data elements between nodes

Note 1 to entry: If more than one key is used for different cryptographic functions, each key can be a variant or derivative of the transaction key.

Note 2 to entry: A transaction key is sometimes referred to as a data key, communications key, session key or working key.

[SOURCE: ISO 11568:2023, 3.85]

3.25
trusted execution environment
TEE
aspect of the device comprising either hardware or software or both which provides security services to the device computing environment, protects data against general software attacks and isolates hardware and software security resources from the operating system

[SOURCE: ISO 5201:2024, 3.21, modified — The wording "mobile" has been deleted, "and/" has been deleted, "either" and "or both" have been added.]

3.26
user data
data received or produced by the target of evaluation (TOE), which are meaningful to some external entity, but which do not affect the operation of the TOE security functionality (TSF)

Note 1 to entry: Depending on the concept, this definition assumes that the same data created by users that have an actual impact on the operation of the TSF can be regarded as the TSF data.

[SOURCE: ISO/IEC 15408-2:2026, 3.14]

3.27
value form
representation of value held in a wallet

EXAMPLE A value form can be a plain balance (account) or a cryptographically computed digital coin (token).

3.28
vulnerability
weakness of an asset or control that can be exploited by one or more threats

[SOURCE: ISO/IEC 27002:2022, 3.1.38]

4 Abbreviated terms

AML	anti-money laundering
ATC	application transaction counter
ATE	anti-tax evasion
ATM	automated teller machine
CBDC	central bank digital currency
CC	common criteria
CFT	counter terrorist financing
COTS	commercial off-the-shelf
DC	digital currency
DCHW	digital currency hardware wallet
eSE	embedded secure element
eSIM	embedded subscriber identity module
HAL	hardware abstraction layer
HSM	hardware security module
ICC	integrated circuit card
ISMS	information security management system
KYC	know your customer
MNO	mobile network operator
NFC	near field communication

OS	operating system
OSP	organizational security policy
P2P	person to person
PCI	payment card industry
PIN	personal identification number
PII	personally identifiable information
POI	point of interaction
POS	point of sale
PSP	payment service provider
SCD	secure cryptographic device
SDK	software development kit
SE	secure element
SIM	subscriber identity module
SPD	security problem definition
TEE	trusted execution environment
TOE	target of evaluation
TSF	TOE security functionality
TSM	trusted service manager
TSP	technology service provider
TUI	trusted user interface