



DPC: 25/30478659 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 29 August 2025

Origin: International

Latest date for receipt of comments: 22 October 2025

Project No. 2023/01880

Responsible committee: IST/12 Financial services

Interested committees:

Title: Draft BS ISO/IEC 13133 BS ISO 13133 Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM-DCHW).

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 22 October 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 13133

Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM- DCHW)

ICS: 35.240.40

ISO/TC 68/SC 2

Secretariat: **BSI**

Voting begins on:
2025-08-29

Voting terminates on:
2025-11-21

This document has not been edited by the ISO Central Secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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.

Reference number
ISO/DIS 13133:2025(en)

Full document details: 25/30478659 DC

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	5
5 Taxonomy	6
6 Reference model	7
6.1 DC life cycle	7
6.1.1 General	7
6.1.2 DC states	8
6.1.3 DC state changes	8
6.2 DCHW life cycle	9
6.2.1 General	9
6.2.2 DCHW states	9
6.2.3 DCHW state changes	9
6.3 Participants	10
6.3.1 General	10
6.3.2 Issuing entity	10
6.3.3 Intermediary	10
6.3.4 End user	10
6.3.5 Technology service provider	10
6.4 Conceptual model of a DC system	10
6.4.1 General	10
6.4.2 Issuing entity component	11
6.4.3 Intermediary component	11
6.4.4 DCHW component	12
6.4.5 Acceptance device component	12
6.5 Target of evaluation	12
6.5.1 Mobile device	13
6.5.2 ICC	14
6.6 TOE environment	14
7 Considerations for the design of the security framework	14
8 Security problem definition	15
8.1 Assets to be protected	15
8.1.1 TSF hardware and software	15
8.1.2 User data	15
8.1.3 TSF data	16
8.2 Assumptions	16
8.2.1 User technical literacy	16
8.2.2 User security awareness	16
8.2.3 User security help	16
8.2.4 Attacker factor	16
8.2.5 Competence&responsibility	16
8.2.6 System backend security	16
8.2.7 DC life cycle	16
8.2.8 DC recovery	17
8.2.9 Security logging	17
8.3 Threat actors	17
8.3.1 Swindler/Fraudsters	17
8.3.2 Hacker	17
8.3.3 Saboteur/Terrorist	17

8.3.4	Organised crime group.....	17
8.3.5	State-level attack.....	17
8.3.6	Insider.....	17
8.4	Threats.....	17
8.4.1	Threat to DC.....	17
8.4.2	Transaction threat.....	17
8.4.3	Cryptography threat.....	18
8.4.4	Authentication threat.....	18
8.4.5	Hardware and software threat.....	18
8.4.6	Communication threat.....	19
8.4.7	Emergency response threat.....	19
8.4.8	Risk management threat.....	19
8.4.9	User privacy threat.....	20
8.4.10	Supply chain security threat.....	20
8.5	Organizational security policies.....	20
8.5.1	Detection.....	20
8.5.2	Reaction.....	20
8.5.3	Log.....	20
8.5.4	Cryptography.....	20
8.5.5	Communication.....	20
8.5.6	Qualification.....	20
8.5.7	Validation.....	21
8.5.8	Verification.....	21
8.5.9	Maintenance.....	21
9	Security objectives.....	21
9.1	General.....	21
9.2	Security objectives for the TOE.....	21
9.2.1	DC security objective.....	21
9.2.2	Transaction security objective.....	22
9.2.3	Cryptography security objective.....	23
9.2.4	Communication security objective.....	24
9.2.5	Authentication security objective.....	25
9.2.6	Privacy security objective.....	25
9.2.7	Hardware and software security objectives.....	25
9.2.8	Risk management security objective.....	26
9.2.9	Emergency response security objective.....	27
9.2.10	Monitor security objective.....	27
	Annex A (informative) Example Models for Secure Implementation of DCHW on Mobile Devices.....	28
	Annex B (informative) Examples of layered digital wallets.....	31
	Bibliography.....	32

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, Financial Services, Subcommittee SC 2, Security.

Introduction

With the popularity of electronic payment and the gradual decline in the use of cash, in order to ensure that the public can maintain access to public money, maintain the characteristics of cash-like experience, and protect the privacy of users while ensuring safety and convenience, many central banks and monetary authorities are conducting research on, experiments with and pilots of digital currencies issued by a specific entity such as a central bank, which in this case are named central bank digital currency (CBDC).

Digital currencies issued by a specific entity, such as a central bank, are not intended to replace cash, but rather to be an important complement to cash and an important backup to existing payment tools to provide emergency services in the event of payment service disruptions, poor network coverage, natural disasters, etc. They can also improve financial inclusion, allowing the underbanked, the unbanked, the elderly and others to better access financial services. They also have the potential to facilitate innovation, bringing new features and services to the ecosystem through the adoption of appropriate technologies and designs.

This document assumes a target of a digital currency wallet that will be embodied in, for example, an integrated circuit card (ICC), a commercial off the shelf (COTS) mobile device, etc. While commodity smartphones could be used as wallets, the wallet sensitive data and sensitive code itself could reside within a hardware device, which is the so-called digital currency hardware wallet (DCHW).

Assumptions

To make the context and scope clearer, and to help better understand and use this document and this security reference model for DCHW, here are some assumptions:

- This document focuses on hardware wallets for digital currencies issued by a specific entity, such as a central bank, and for primary use in retail finance;
- This document does not constrain the specific architecture of DCHW;
- This document does not constrain the specific scenarios or user cases of DCHW;
- This document does not constrain the specific model and architecture of DC, but uses a two-tier model as an example illustration, in which the central bank issues CBDC and manages the supply. Intermediaries would be responsible for distributing CBDCs to end users (individuals and businesses) and supporting CBDC payments;
- This document recommends that readers use ISO 31000 as a risk management framework reference and accordingly conduct an analysis of detailed and specific assessment of the threat impact, threat likelihood, etc.

The purpose of this document

Multiple central banks are considering the introduction of digital currencies (DCs) in digital wallets, which has led to the following requirements:

- a) The establishment of global standards to provide clear guidelines for mitigating circulatory and payment risks associated with such DCs; and
- b) These standards should be based, to the greatest extent possible, on existing financial industry security standards and best practices.

The purpose of this standard is to facilitate the secure design and implementation of digital currency hardware wallets.

The audience for this document includes organizations that develop and operate digital currency hardware wallets, such as mobile device manufacturers, chip manufacturers, and companies that provide digital currency hardware wallet solutions. Third parties that provide services to the above-mentioned stakeholders may also benefit from this standard.

Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM-DCHW)

1 Scope

This document provides taxonomy, a security reference model, consideration items for a security framework and security problem definition of digital currency hardware wallets (DCHW). Then it specifies security objective to address and counter security issues of the defined security problem.

This document addresses sovereign/ fiat digital currencies issued by a specific entity, such as a central bank.

NOTE In order to fulfil those security objectives, TC 68/SC 2/WG 13 is planning to come up with future proposed documents to specify such as security requirements for account-based architecture, security requirements for token-based architecture, security requirements for acceptance devices, etc.

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.

3.1 access control

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

[SOURCE: ISO/IEC 27000:2018, 3.1]

3.2 asset

anything (sensitive data, etc.) that has value to a stakeholder of digital currency hardware wallet, which is processed, stored, transmitted and should be protected against unauthorized disclosure, alteration, or destruction

Note 1 to entry: The boundary of the asset to be protected is the retail banking user device.

3.3 attack

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

Note 1 to entry: A form of attack could also comprise of attempts to illegitimately create assets.

[SOURCE: ISO/IEC 27002:2022, 3.1.3, added “Note 1 to entry”.]

3.4 central bank digital currency CBDC

A 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 retail payments and/or wholesale settlement

3.5

counter, verb

act on or respond to a particular threat so that the threat is eradicated or mitigated

[SOURCE: ISO/IEC 15408-1:2022, 3.28]

3.6

digital currency

DC

Digital currency is the digital version of money, which should have the basic functions of money, such as unit of account, medium of exchange, etc.

Note 1 to entry: This document focuses on the digital currencies issued by a specific entity such as a central bank, which in this case are named central bank digital currency (CBDC)

3.7

evaluation assurance level

EAL

well-formed package of security assurance requirements representing a point on the pre-defined assurance scale

[SOURCE: ISO/IEC 15408-1:2022, 3.39]

3.8

hardware wallet

wallet which leverages a hardware device to generate, manage, store, or use private and public key

Note 1 to entry: An example of a hardware device is an SCD, SE or TEE.

[SOURCE: ISO/TR 23576:2020, deleted — “(e.g. HSM)”, added “Note 1 to entry”.]

3.9

digital currency hardware wallet

DCHW

hardware wallet that facilitates digital currency transactions.

3.10

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]

3.11

integrated circuit card

ICC

IC card

Card into which one or more integrated circuits have been inserted

[SOURCE: ISO 9564-4:2016, 3.7, modified — replace “ID-1 card type, as specified in ISO/IEC 7816 (all parts)” with “Card”.]

3.12

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 27000:2018, 3.28]

3.13
operating system
OS

Software that controls the execution of programs and that may 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(en), 2.12]

3.14
operational environment

environment in which the target of evaluation (TOE) is operated, consisting of everything that is outside the TOE boundary

[SOURCE: ISO/IEC 15408-1:2022, 3.63]

3.15
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 15408-1:2022, 3.65]

3.16
protection profile
PP

implementation-independent statement of security needs for a target of evaluation (TOE) type

[SOURCE: ISO/IEC 15408-1:2022, 3.68]

3.17
secure cryptographic device
SCD

device that provides physically and logically protected cryptographic services and storage (e.g. PIN entry device (PED) or HSM), and which may be integrated into a larger system, such as an automated teller machine (ATM) or point of sale (POS) terminal.

[SOURCE: ISO 13491-1:2016, 3.28]

3.18
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 —"platform in the mobile device " replaced by "component"

3.19
security functional requirement
SFR

security requirement, which contributes to fulfil the target of evaluation (TOE) security problem definition (SPD) as defined in a specific security target (ST) or in a protection profile (PP)

Note 1 to entry: A security functional requirement can be addressed directly as in the direct rationale model, or indirectly, through the security objectives for the TOE, as in the general model.

[SOURCE: ISO/IEC 15408-1:2022, 3.78]

3.20

security objective

statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

[SOURCE: ISO/IEC 15408-1:2022, 3.79]

3.21

security target

ST

implementation-dependent statement of security requirements for a target of evaluation (TOE) based on a security problem definition

[SOURCE: ISO/IEC 15408-1:2022, 3.82]

3.22

security problem

security problem definition

SPD

statement, which in a formal manner 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 15408-1:2022, 3.80]

3.23

sensitive data

sensitive information

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

EXAMPLE Status information, cryptographic key, personal identification number (PIN).

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

3.24

target of evaluation

TOE

set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

[SOURCE: ISO/IEC 15408-1:2022, 3.90]

3.25

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 (SFRs)

[SOURCE: ISO/IEC 15408-1:2022, 3.92]

3.26

TSF data

data for the operation of the TOE upon which the enforcement of the SFR relies

[SOURCE: ISO/IEC 15408-2:2022, 3.13]

3.27

trusted execution environment

TEE

aspect of the device comprising hardware and/or software which provides security services to the mobile 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, deleted — “mobile”.]

3.28

user data

data received or produced by the TOE, which is meaningful to some external entity, but which do not affect the operation of the TSF

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

[SOURCE: ISO/IEC 15408-2:2022, 3.14]

3.29

threat

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

[SOURCE: ISO/IEC 27002:2022(en), 3.1.34]

3.30

value form

a representation of value held in a wallet

Note 1 to entry: For instance, this could be a plain balance (account) or a cryptographically computed digital coin (token).

3.31

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 Symbols and abbreviated terms

APP	application
ATC	application transaction counter
BLE	bluetooth low energy
CBDC	central bank digital currency
CC	common criteria
COTS	commercial off the shelf
DC	digital currency
DCHW	digital currency hardware wallet
EAL	evaluation assurance level
eSE	embedded secure element
eSIM	embedded subscriber identity module