PD ISO/TS 23526:2023



BSI Standards Publication

Security aspects for digital currencies

bsi.

National foreword

This Published Document is the UK implementation of ISO/TS 23526:2023.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 02413 5

ICS 35.240.40; 03.060

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2023.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 23526:2023

TECHNICAL SPECIFICATION

ISO/TS 23526

First edition
2023-09

Security aspects for digital currencies

Reference number
ISO/TS 23526:2023(E)

© ISO 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

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

© ISO 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Considerations on security framework for digital ... **2**
4.1 General ... 2
4.2 Security considerations for processing digital currencies ... 3
4.3 Variations of security frameworks ... 3
4.3.1 Non-fiat digital currency (digital asset) security framework ... 3
4.3.2 Creating a national digital currency with an anonymity security framework ... 3
4.3.3 Secure digital cash as digital currency with consumer identity security framework ... 4
4.4 Overview of security frameworks ... 4
4.4.1 General ... 4
4.4.2 Standards as a basis for security frameworks ... 4
5 The emergence of currency in digital formats ... **4**
5.1 Digital cash representing money as a basis for financial usage with security ... 4
5.2 Cryptocurrencies as a digital entity for financial usage ... 5
5.3 Cryptocurrencies and the digital currency market challenges ... 6
5.4 Cryptocurrencies and financial market formats ... 6
5.5 Cryptocurrencies and banking regulation – stablecoin example ... 7
5.6 Security criteria representing security aspects ... 8
5.6.1 Security objects ... 8
5.6.2 Key management ... 8
5.6.3 Hiding and steganography techniques ... 8
5.6.4 Digital representation ... 8
5.6.5 Digital model ... 8
5.6.6 Security countermeasures ... 9
5.6.7 Legal and regulatory requirements ... 9
5.6.8 Trust ... 9
5.6.9 Chaining security processes ... 9
5.6.10 Security framework implementation ... 9
5.6.11 Platform independence ... 9
5.6.12 Existing good practices ... 9
5.6.13 Digital interfaces ... 9
6 Critical areas for security to establish trust, acceptance and risk ... **10**
6.1 Digital wallets ... 10
6.2 Specific security considerations ... 11
6.3 Digital currency financial security framework considerations ... 11
7 Fraud and threat considerations ... **11**
Bibliography ... **13**

© ISO 2023 – All rights reserved

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.

© ISO 2023 – All rights reserved

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.

© ISO 2023 – All rights reserved

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

© ISO 2023 – All rights reserved