International Standard

ISO 13491-1

Fourth edition
2024-07

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts and requirements

Services financiers — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 1: Concepts et exigences

Reference number
ISO 13491-1:2024(en)

© ISO 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024
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 Abbreviated terms **4**
5 Secure cryptographic device concepts **5**
5.1 General 5
5.2 Hardware management devices 5
5.3 Secure cryptographic device types 6
5.3.1 General types 6
5.3.2 Secure cryptographic device components 6
5.3.3 Hardware security module 7
5.3.4 Key loading devices 10
5.4 Attack scenarios 10
5.4.1 General 10
5.4.2 Penetration 10
5.4.3 Monitoring 10
5.4.4 Manipulation 11
5.4.5 Modification 11
5.4.6 Substitution 11
5.5 Defence measures 11
5.5.1 General 11
5.5.2 Device characteristics 12
5.5.3 Device management 12
5.5.4 Environment 13
6 Requirements for device security characteristics **13**
6.1 General 13
6.2 Physical security requirements for secure cryptographic devices 13
6.3 Tamper-evident requirements 14
6.3.1 General 14
6.3.2 Substitution 14
6.3.3 Penetration 14
6.3.4 Modification 14
6.3.5 Monitoring 14
6.4 Tamper-resistant requirements 14
6.4.1 General 14
6.4.2 Penetration 14
6.4.3 Modification 15
6.4.4 Monitoring 15
6.4.5 Substitution or removal 15
6.5 Tamper-responsive requirements 15
6.5.1 General 15
6.5.2 Penetration 15
6.5.3 Modification 15
6.6 Logical security requirements for SCDs and HMDs 16
6.6.1 General 16
6.6.2 Dual control 16
6.6.3 Unique key per device 16
6.6.4 Assurance of genuine device 16
6.6.5 Design of functions 16
6.6.6 Use of cryptographic keys 17
6.6.7 Sensitive device states 17

© ISO 2024 – All rights reserved

6.6.8 Multiple cryptographic relationships 17
6.6.9 Secure device software authentication 17

7 Requirements for device management 17
7.1 General 17
7.2 Life cycle phases 18
7.3 Life cycle protection requirements 19
7.3.1 General 19
7.3.2 Manufacturing phase 20
7.3.3 Post-manufacturing phase 20
7.3.4 Commissioning (initial financial key loading) phase 20
7.3.5 Inactive operational phase 20
7.3.6 Active operational phase (use) 21
7.3.7 Decommissioning (post-use) phase 21
7.3.8 Repair phase 21
7.3.9 Destruction phase 22
7.4 Life cycle protection methods 22
7.4.1 Manufacturing 22
7.4.2 Post-manufacturing phase 22
7.4.3 Commissioning (initial financial key loading) phase 23
7.4.4 Inactive operational phase 23
7.4.5 Active operational (use) phase 23
7.4.6 Decommissioning phase 24
7.4.7 Repair 24
7.4.8 Destruction 24
7.5 Accountability 24
7.6 Device management principles of audit and control 25

Bibliography 27

© ISO 2024 – 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 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 268, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

This fourth edition cancels and replaces the third edition (ISO 13491-1:2016), which has been technically revised.

The main changes are as follows:

— revision for classes of secure cryptographic devices (SCDs);

— updated life cycle guidance.

A list of all parts in the ISO 13491 series can be found on the ISO website.

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 2024 – All rights reserved

Introduction

The ISO 13491 series describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive data used in a retail financial services environment.

This document contains the security requirements for SCDs. ISO 13491-2 is a tool for measuring compliance against these requirements. It provides a checklist of:

— characteristics that a device has to possess;

— how devices have to be managed;

— characteristics of the operational environments.

The security of retail electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be tapped and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When personal identification numbers (PINs), message authentication codes (MACs), cryptographic keys and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. The risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner (e.g. by bugging) and that any sensitive data placed within the device (e.g. cryptographic keys) has not been subject to disclosure or change.

Absolute security is not achievable in practical terms. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunities for breaches of SCD security. The aim is for a high probability of detection of any unauthorized access to sensitive or confidential data in cases where device characteristics fail to prevent or detect the security compromise.

© ISO 2024 – All rights reserved

Financial services — Secure cryptographic devices (retail) —

Part 1:
Concepts and requirements

1 Scope

This document specifies the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes defined in the ISO 9564 series, ISO 16609 and ISO 11568.

This document states the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle.

This document does not address issues arising from the denial of service of an SCD.

This document does not address software services that use multi-party computation (MPC) to achieve some security objectives and, relying on these, offer cryptographic services.

NOTE These are sometimes called “soft” or software hardware security modules (HSMs) in common language, which is misleading and does not correspond to the definition of HSM in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 11568, *Financial services — Key management (retail)*

ISO 13491-2:2023, *Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

NIST SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

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
audit
evaluates compliance with an evaluation on behalf of an evaluation agency

© ISO 2024 – All rights reserved