AS ISO 13491.2:2025
ISO 13491-2:2023

Australian STANDARD®

STANDARDS Australia

Financial services — Secure cryptographic devices (retail)

Part 2: Security compliance checklists for devices used in financial transactions



AS ISO 13491.2:2025

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 03 April 2025.

This Standard was published on 2 May 2025.

The following are represented on Committee IT-005:

ANZ Banking Group
Australian Payments Network
Australian Securities and Investments Commission
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
EFTPOS Payments Australia
National Australia Bank
New Payments Platform Australia
Pacific Research
SWIFT
Thales Australia
Triton Systems of Delaware
UL Transaction Security
Verisec International

This Standard was issued in draft form for comment as DR AS ISO 13491.2:2025.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76175 145 5

AS ISO 13491.2:2025
ISO 13491-2:2023

Financial services — Secure cryptographic devices (retail)

Part 2: Security compliance checklists for devices used in financial transactions

Originated as AS 2805.14.2—2003.
Second edition 2009.
Revised and redesignated as AS ISO 13491.2:2019.
Second edition 2025.

COPYRIGHT

© ISO 2025 — All rights reserved
© Standards Australia Limited 2025

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

How to read this Standard

This page explains the meaning of the language and structure of this Standard.

Refer to Standards Australia's Standardisation Guide 006 for more details about drafting rules.

Australian and Australian/New Zealand Standards are voluntary unless they are referenced in legislation or called up in contracts.

Requirements

To conform to a Standard, all requirements in the Standard need to be met.

A requirement is any statement in the Standard which uses the word "shall".

Recommendations, permissions and possibilities

The following words are commonly used in Standards, but statements using them do not have to be followed to conform to the Standard:

(a) "should" means that something is recommended.

(b) "may" means that something is permitted.

(c) "can" means that something is possible.

Structure of Standards

A Standard always has the following parts:

(i) The Preface states who developed the Standard, what the Standard is aiming to do, and how it relates to other documents.

(ii) The Scope states what the Standard is about, what it covers and what it does not cover.

(iii) The Normative references clause lists other documents that are referenced in the Standard as part of requirements.

(iv) The Terms and definitions clause defines important terms to help with understanding the Standard.

A Standard may also include other parts, such as the following:

(1) A normative appendix sets additional requirements that need to be conformed to.

(2) An informative appendix provides additional information or guidance. They usually do not contain requirements. If an informative appendix does contain requirements, the Standard will explain when those requirements apply

(3) A Bibliography lists documents referenced in the Standard but not as part of requirements.

Many Standards include notes. Notes provide recommendations and/or guidance only. They never contain requirements.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS ISO 13491.2:2019.

The objective of this document is to specify checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in ISO 9564-1, ISO 9564-2, ISO AS 16609, and AS ISO 11568 in the financial services environment. Integrated circuit (IC) payment cards are subject to the requirements identified in this document up until the time of issue, after which they are to be regarded as a "personal" device and outside of the scope of this document.

This document is identical to, and has been reproduced from, ISO 13491-2:2023, *Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*.

As this document has been reproduced from an international document, a comma is to be read as a full point when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms "normative" and "informative" are used in Standards to define the application of the appendices or annexes to which they apply. A "normative" appendix or annex is an integral part of a Standard, whereas an "informative" appendix or annex is only for information and guidance.

© Standards Australia Limited 2025

Contents

Preface ... **iii**
Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Use of security compliance checklists ... **2**
Annex A (normative) **Physical, logical and device-management characteristics common to all secure cryptographic devices** ... **3**
Annex B (normative) **Devices with PIN entry functionality** ... **11**
Annex C (normative) **Devices with PIN management functionality** ... **17**
Annex D (normative) **Devices with message authentication functionality** ... **20**
Annex E (normative) **Devices with key generation functionality** ... **22**
Annex F (normative) **Devices with key transfer and loading functionality** ... **26**
Annex G (normative) **Devices with digital signature functionality** ... **31**
Annex H (normative) **Categorization of environments** ... **33**
Bibliography ... **38**

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*.

This fifth edition cancels and replaces the fourth edition (ISO 13491-2:2017), which has been technically revised.

The main changes are as follows:

— an additional subclause, H.5, is added to Annex H and the entire Annex H is reordered for clarity;

— editorially revised.

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.

© Standards Australia Limited 2025

Introduction

This document specifies both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys and other sensitive information used in a retail financial services environment.

The security of retail financial services is largely dependent upon the security of these cryptographic devices.

Security requirements are based upon the premise that computer files can be accessed and manipulated, communication lines can be "tapped" and authorized data or control inputs in a system device can be replaced with unauthorized inputs. While certain cryptographic devices (e.g., host security modules) reside in relatively high-security processing centres, a large proportion of cryptographic devices used in retail financial services (e.g., PIN entry devices) now reside in non-secure environments. Therefore, when PINs, MACs, cryptographic keys and other sensitive data are processed in these devices, there is a risk that the devices can be tampered with or otherwise compromised to disclose or modify such data.

The risk of financial loss can be reduced through the appropriate use of cryptographic devices that have proper physical and logical security characteristics and are properly managed. To ensure that SCDs have the proper physical and logical security, they require evaluation.

This document provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and can be appropriate for formal security evaluations (e.g., ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 and ISO/IEC 19790) but are outside the scope of this document.

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) have not been subject to disclosure or change.

Absolute security is not practically achievable. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate device management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These measures aim for a high probability of detection of any illicit access to sensitive or confidential data in the event that device characteristics fail to prevent or detect the security compromise.

© Standards Australia Limited 2025

Australian Standard®

Financial services — Secure cryptographic devices (retail)

Part 2: Security compliance checklists for devices used in financial transactions

1 Scope

This document specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in ISO 9564-1, ISO 9564-2, ISO 16609, and ISO 11568 in the financial services environment. Integrated circuit (IC) payment cards are subject to the requirements identified in this document up until the time of issue, after which they are to be regarded as a "personal" device and outside of the scope of 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 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

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

ISO 13491-1, *Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13491-1 and the following 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
auditor
person or organization approved as an auditor by an approval authority

[SOURCE: ISO 9000:2015, 3.13.15]

3.2
data integrity
assurance that data has not been altered or destroyed in an unauthorized manner

3.3
dual control
process of utilizing two or more entities (usually persons) operating in concert to protect sensitive functions or information whereby no single entity is able to access or use the materials

Note 1 to entry: A cryptographic key is an example of the type of material to be accessed or utilized.

© Standards Australia Limited 2025