AS ISO 13491.2:2019
ISO 13491-2:2017

AS ISO 13491.2:2019

Australian STANDARD

Financial services—Secure cryptographic devices (retail)

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

STANDARDS Australia

AS ISO 13491.2:2019

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 23 January 2019.

This Standard was published on 12 March 2019.

The following are represented on Committee IT-005:

Australian Payments Network
EFTPOS Payments Australia

Additional Interests

ANZ Banking Group
Coles Group
Diebold Nixdorf
FIS Global
Gemalto
National Australia Bank
Sundial
SWIFT
Thales e-Security
Woolworths

This Standard was issued in draft form for comment as DR AS ISO 13491.2:2018.

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 76072 369 9

Australian STANDARD

Financial services—Secure cryptographic devices (retail)

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

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

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.14.2—2009, *Electronic funds transfer — Requirements for interfaces —Part 14.2: Secure cryptographic devices (retail) — Security compliance checklists for devices used in financial transactions.*

The objective of this Standard 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 16609, AS 2805.6.1.1 (identical adoption of ISO 11568-1), AS 2805.6.1.2 (identical adoption of ISO 11568-2), and AS 2805.6.1.4 (identical adoption of ISO 11568-4), 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 Standard is identical with, and has been reproduced from, ISO 13491-2:2017, *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 Standard, a full point substitutes for a comma 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 annexes to which they apply. A "normative" annex is an integral part of a Standard, whereas an "informative" annex is only for information and guidance.

Contents

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 on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This fourth edition cancels and replaces the third edition (ISO 13491-2:2016), of which it constitutes a minor revision with the following changes:

— references made to H.5 have been replaced with ISO 9564-1;

— editorially revised.

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

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, etc.) 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.

It is to be ensured that the risk of financial loss is 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 may be appropriate for formal security evaluations (e.g. ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 19790) and 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.

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, ISO 11568-1, ISO 11568-2, and ISO 11568-4 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 does not address issues arising from the denial of service of an SCD.

In the checklists given in Annex A to Annex H, the term "not feasible" is intended to convey the notion that although a particular attack might be technically possible, it would not be economically viable since carrying out the attack would cost more than any benefits obtained from a successful attack. In addition to attacks for purely economic gain, malicious attacks directed toward loss of reputation need to be considered.

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 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

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 terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
auditor
person who has the appropriate skills to check, assess, review, and evaluate compliance with an informal evaluation on behalf of the sponsor or audit review body