AS ISO 13491.1:2019
ISO 13491-1:2016

AS ISO 13491.1:2019

Australian STANDARD

Financial services—Secure cryptographic devices (retail)

Part 1: Concepts, requirements and evaluation methods

STANDARDS Australia

AS ISO 13491.1:2019

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 13491.1:2018.

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 355 2

Australian STANDARD

Financial services—Secure cryptographic devices (retail)

Part 1: Concepts, requirements and evaluation methods

Originated as AS 2805.14.2—2000.
Previous edition 2011.
Revised and redesignated as AS ISO 13491.1:2019.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede AS 2805.14.1—2011, *Electronic funds transfer — Requirements for interfaces — Part 14.1 Secure cryptographic devices (retail) — Concepts, requirements and evaluation methods.*

The objective of this Standard is to specify the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609, and ISO 11568. It is also states the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle and provides guidance for methodologies to verify compliance with those requirements.

This Standard is identical with, and has been reproduced from, ISO 13491-1:2016, *Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods.*

As this document has been reproduced from an International Standard, the following applies:

(a) In the source text "this part of ISO 13491" should read "this Australian Standard".

(b) 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This third edition cancels and replaces the second edition (ISO 13491-1:2007), which has been technically revised.

ISO 13491 consists of the following parts, under the general title *Financial services — Secure cryptographic devices (retail)*:

— *Part 1: Concepts, requirements and evaluation methods*

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

Introduction

ISO 13491 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 information used in a retail financial services environment.

This part of ISO 13491 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, and

— 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 opportunity for a breach of SCD security. This aims for a high probability of detection of any unauthorized access to sensitive or confidential data should device characteristics fail to prevent or detect the security compromise.

Australian Standard®

Financial services—Secure cryptographic devices (retail)

Part 1: Concepts, requirements and evaluation methods

1 Scope

This part of ISO 13491 specifies the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609, and ISO 11568.

This part of ISO 13491 has two primary purposes:

— to state the security characteristics concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle;

— to provide guidance for methodologies to verify compliance with those requirements. This information is contained in Annex A.

ISO 13491-2 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, ISO 11568-3, ISO 11568-4, ISO 11568-5, and ISO 11568-6 in the financial services environment.

Annex A provides an informative illustration of the concepts of security levels described in this part of ISO 13491 as being applicable to SCDs.

This part of ISO 13491 does not address issues arising from the denial of service of an SCD.

Specific requirements for the security characteristics and management of specific types of SCD functionality used in the retail financial services environment are contained in ISO 13491-2.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

accreditation authority

authority responsible for the accreditation of evaluation agencies and supervision of their work in order to guarantee the reproducibility of the evaluation results