



Financial services—Secure cryptographic devices (retail)

Part 1: Concepts, requirements and evaluation methods



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



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.

COPYRIGHT

© ISO 2019 — All rights reserved
© Standards Australia Limited 2019

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).

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 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

Preface	ii
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	5
5 Secure cryptographic device concepts	5
5.1 General.....	5
5.2 Attack scenarios.....	6
5.2.1 General.....	6
5.2.2 Penetration.....	6
5.2.3 Monitoring.....	6
5.2.4 Manipulation.....	6
5.2.5 Modification.....	6
5.2.6 Substitution.....	6
5.3 Defence measures.....	7
5.3.1 General.....	7
5.3.2 Device characteristics.....	7
5.3.3 Device management.....	8
5.3.4 Environment.....	8
6 Requirements for device security characteristics	8
6.1 General.....	8
6.2 Physical security requirements for SCDs.....	9
6.2.1 General.....	9
6.3 Tamper evident requirements.....	9
6.3.1 General.....	9
6.4 Tamper resistant requirements.....	10
6.4.1 General.....	10
6.5 Tamper responsive requirements.....	10
6.5.1 General.....	10
6.6 Logical security requirements for SCDs.....	11
6.6.1 Dual control.....	11
6.6.2 Unique key per device.....	11
6.6.3 Assurance of genuine device.....	11
6.6.4 Design of functions.....	11
6.6.5 Use of cryptographic keys.....	12
6.6.6 Sensitive device states.....	12
6.6.7 Multiple cryptographic relationships.....	12
6.6.8 SCD software authentication.....	12
7 Requirements for device management	12
7.1 General.....	12
7.2 Life cycle phases.....	13
7.3 Life cycle protection requirements.....	14
7.3.1 General.....	14
7.3.2 Manufacturing phase.....	14
7.3.3 Post-manufacturing phase.....	15
7.3.4 Commissioning (initial financial key loading) phase.....	15
7.3.5 Inactive operational phase.....	15
7.3.6 Active operational phase (use).....	16
7.3.7 Decommissioning (post-use) phase.....	16

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-