AS ISO 11568:2025
ISO 11568:2023

Australian STANDARD®

STANDARDS Australia

Financial services — Key management (retail)



AS ISO 11568:2025

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 15 April 2025.

This Standard was published on 30 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 LLC
UL Transaction Security
Verisec International

This Standard was issued in draft form for comment as DR AS ISO 11568:2025.

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 171 4

Financial services — Key management (retail)

First published as AS ISO 11568:2025 to replace AS 2805.6.1.1—2009, AS 2805.6.1.2—2009 and AS 2805.6.1.4—2009.

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 —

(a) AS 2805.6.1.1:2009, *Electronic funds transfer—Requirements for interfaces, Part 6.1.1: Key management—Principles (ISO 11568-1:2005, MOD)*;

(b) AS 2805.6.1.2:2009, *Electronic funds transfer—Requirements for interfaces, Part 6.1.2: Key management—Symmetric ciphers, their key management and life cycle;* and

(c) AS 2805.6.1.4:2009, *Electronic funds transfer—Requirements for interfaces, Part 6.1.4: Key management—Asymmetric cryptosystems—Key management and life cycle*.

The objective of this document is to describe the management of symmetric and asymmetric cryptographic keys that can be used to protect sensitive information in financial services related to retail payments. The document covers all aspects of retail financial services, including connections between a card-accepting device and an Acquirer, between an Acquirer and a card Issuer, and between an ICC and a card-accepting device. It covers all phases of the key life cycle, including the generation, distribution, utilization, archiving, replacement and destruction of the keying material. This document covers manual and automated management of keying material, and any combination thereof, used for retail financial services. It includes guidance and requirements related to key separation, substitution prevention, identification, synchronization, integrity, confidentiality and compromise, as well as logging and auditing of key management events.

Requirements associated with hardware used to manage keys have also been included in this document.

This document is identical to, and has been reproduced from, ISO 11568:2023, *Financial services — Key management (retail)*. 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 ... **vi**

Introduction ... **vii**

1 Scope ... **1**
1.1 General ... 1
1.2 Scope exclusions ... 1

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Key management requirements ... **12**
4.1 General ... 12
4.1.1 Key management strategy ... 12
4.1.2 Dual control and split knowledge of secret or private keys ... 12
4.1.3 Permissible key forms ... 12
4.1.4 Logging ... 14
4.1.5 Cryptographic strength ... 14
4.1.6 Key locations ... 15
4.1.7 Single-purpose key usage ... 15
4.2 Secure cryptographic device ... 17
4.2.1 General requirements ... 17
4.2.2 Additional SCD requirements for devices used in SKDAT ... 18
4.3 Additional CA requirements ... 19
4.4 Additional RA requirements ... 19
4.5 Key blocks ... 20
4.5.1 Overview of key blocks ... 20
4.5.2 Key attributes ... 21
4.5.3 Integrity of the key block ... 21
4.5.4 Key and sensitive attributes field ... 21
4.6 Key creation ... 22
4.6.1 Symmetric key creation ... 22
4.6.2 Asymmetric key creation ... 23
4.7 Key component and key share creation ... 23
4.8 Check values ... 24
4.8.1 Introduction ... 24
4.8.2 Symmetric key check value calculation ... 24
4.8.3 Asymmetric key check value calculation ... 25
4.9 Key distribution ... 25
4.9.1 Symmetric key distribution ... 25
4.9.2 SKDAT asymmetric key distribution ... 28
4.10 Key loading ... 30
4.10.1 General ... 30
4.10.2 Loading key components or shares ... 31
4.11 Key utilization ... 31
4.11.1 General key utilization requirements ... 31
4.11.2 Additional key utilization requirements for SKDAT ... 32
4.12 Key storage ... 33
4.12.1 Cleartext key component and share storage ... 33
4.12.2 Public key storage ... 33
4.13 Key replacement ... 33
4.14 Key destruction ... 34
4.14.1 General ... 34
4.14.2 Key destruction from an SCD ... 35
4.14.3 Destruction of a key in cryptogram form ... 35

4.14.4 Component and share destruction ... 35
4.15 Key backup ... 35
4.16 Key archiving ... 36
4.17 Key compromise ... 36

5 Transaction key management techniques ... 38
5.1 General ... 38
5.2 Method: master keys or transaction keys ... 38
5.3 Derived unique key per transaction ... 38
5.3.1 General ... 38
5.3.2 DUKPT key management ... 39
5.3.3 Unique initial keys ... 41
5.3.4 AES DUKPT ... 42
5.3.5 KSN compatibility mode ... 45
5.3.6 Derived key OIDs ... 46
5.3.7 Keys and key sizes ... 46
5.3.8 Helper functions and definitions ... 47
5.3.9 Key derivation function algorithm ... 48
5.3.10 Derivation data ... 49
5.3.11 "Create Derivation Data" (local subroutine) ... 50
5.3.12 Security considerations ... 51
5.3.13 Host security module algorithm ... 53
5.3.14 General ... 53
5.3.15 "Derive Initial Key" ... 53
5.3.16 "Host Derive Working Key" ... 54
5.3.17 Intermediate derivation key derivation data examples ... 54
5.3.18 Working key derivation data examples ... 55
5.3.19 Transaction-originating device algorithm ... 56
5.4 Host-to-host UKPT ... 61

Annex A (informative) **Key and component check values ... 63**
Annex B (normative) **Split knowledge during transport ... 67**
Annex C (informative) **Trust models and key establishment ... 69**
Annex D (informative) **Symmetric key life cycle ... 77**
Annex E (informative) **Asymmetric key life cycle phases ... 79**
Annex F (normative) **Approved algorithms ... 82**
Annex G (informative) **AES DUKPT pseudocode notation ... 83**
Annex H (informative) **AES DUKPT test vectors ... 86**
Annex I (informative) **TDEA-derived unique key per transaction ... 87**
Annex J (informative) **Roles in payment environment ... 108**
Annex K (informative) **Roles in symmetric key distribution using asymmetric techniques ... 111**

Bibliography ... 114

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 document cancels and replaces the former ISO 11568 series, which has been technically revised.

The main changes are as follows:

— all parts of the series combined into a single document;

— fixed key no longer included in the permissible methods of transaction key management;

— required key replacement policy (see 4.13) added;

— cleartext key injection removed;

— AES DUKPT introduced as a key management method.

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

Retail financial transactions are often transmitted over potentially non-secure channels, which, if exploited, can result in fraud. The vast range in value and volume of such transactions exposes participants to severe risks, which can be uninsurable. To protect against these risks, many institutions are employing encryption. The encryption algorithms used are in the public domain. The security and reliability of any process based on these algorithms is directly dependent on the protection afforded to secrets called cryptographic keys.

This document describes requirements and provides guidance for the secure management of cryptographic keys used to protect sensitive information in a retail financial services environment, for example in messages between a card acceptor and an Acquirer. Typical services in the retail financial services domain include point-of-sale (POS) debit and credit authorizations and automated teller machine (ATM) transactions. While it is designed with these environments in mind, it may also be used in unrelated applications. For example, such keys could be used for:

— encrypting Personal Identification Numbers (PIN) (see ISO 9564-1);

— authenticating messages;

— encrypting other data;

— encrypting or deriving cryptographic keys;

— automated symmetric key distribution using asymmetric techniques.

© Standards Australia Limited 2025

NOTES

Australian Standard®

Financial services — Key management (retail)

1 Scope

1.1 General

This document describes the management of symmetric and asymmetric cryptographic keys that can be used to protect sensitive information in financial services related to retail payments. The document covers all aspects of retail financial services, including connections between a card-accepting device and an Acquirer, between an Acquirer and a card Issuer, and between an ICC and a card-accepting device. It covers all phases of the key life cycle, including the generation, distribution, utilization, archiving, replacement and destruction of the keying material. This document covers manual and automated management of keying material, and any combination thereof, used for retail financial services. It includes guidance and requirements related to key separation, substitution prevention, identification, synchronization, integrity, confidentiality and compromise, as well as logging and auditing of key management events.

Requirements associated with hardware used to manage keys have also been included in this document.

1.2 Scope exclusions

This document does not specifically address internet banking services offered by an Issuer to their own customers through that financial institution's website or applications.

This document does not address using asymmetric keys to encrypt the Personal Identification Number (PIN) or any other data and does not address asymmetric keys managed with asymmetric keys.

This document is not intended to apply to the management of the keys installed in an ICC during manufacturing or the initial key established in an ICC during card personalization.

This document is not intended to address post-quantum encryption considerations. Key management using quantum technologies is out of 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/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO/IEC 11770 (all parts), *Information security — Key management*

ISO 13491 (all parts), *Financial services — Secure cryptographic devices (retail)*

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

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

ISO/IEC 18032, *Information security — Prime number generation*

ISO/IEC 18033 (all parts), *Information security — Encryption algorithms*

ISO/IEC 19592-2, *Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms*

ISO/IEC 19772, *Information security — Authenticated encryption*

© Standards Australia Limited 2025