AS ISO 13492:2026
ISO 13492:2019

Australian STANDARD®

STANDARDS Australia

Financial services — Key-management-related data element — Application and usage of AS ISO 8583 data elements for encryption



AS ISO 13492:2026

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 5 January 2026.

This Standard was published on 16 January 2026.

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 for comment as DR AS ISO 13492:2025

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 products by visiting:

www.standards.org.au

ISBN: 978 1 76175 565 1

AS ISO 13492:2026
ISO 13492:2019

Australian Standard®

Financial services — Key-management-related data element — Application and usage of AS ISO 8583 data elements for encryption

First published as AS ISO 13492:2026.

© ISO 2026 — All rights reserved
© Standards Australia Limited 2026

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.

The objective of this document is to describe a data element related to key management which can be transmitted either in transaction messages to convey information about cryptographic keys used to secure the current transaction, or in cryptographic service messages to convey information about cryptographic keys to be used to secure future transactions.

This document addresses the requirements for the use of the data element related to key management within AS ISO 8583, using the following two AS ISO 8583 data elements for DEA and TDEA:

(a) Security related control information (data element 53).

(b) Key management data (data element 96).

The data element related to key management for DEA and TDEA is constructed from the concatenation of two AS ISO 8583 message elements, data element 53 — security related control information, and data element 96 — key management data. It conveys information about the associated transaction's cryptographic key(s) and is divided into subfields including a control field, a key-set identifier and additional optional information. For AES implementations, the data elements are summarized in one field.

This document is applicable to either symmetric or asymmetric cipher systems.

This document is identical to, and has been reproduced from, ISO 13492:2019, *Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption.*

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 2026

Contents

Page

Preface ..... **v**
Foreword ..... **vii**
Introduction ..... **viii**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Data representation **3**
6 Requirements for key-management-related data element **3**
6.1 Introduction 3
6.2 Data element structure 5
6.2.1 Data element structure for field 53 and 96 5
6.2.2 Data element structure for field 50, 110, 111 6
6.3 Key-set identifier concepts 11
7 Security related control information usage format **11**
7.1 Control field format 11
7.2 Key-set identifier 12
7.2.1 Format A 12
7.2.2 Format B 12
7.3 Algorithm field 12
7.4 Key length (in bytes) field 13
7.5 Key protection field 13
7.6 Padding method field 13
7.7 Encrypted data format field 13
Bibliography **15**

© Standards Australia Limited 2026

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 third edition cancels and replaces the second edition (ISO 13492:2007), which has been technically revised.

The main changes compared to the previous edition are as follows:

— introduction of the support of the AES encryption algorithm, resulting in a complete restructuring and editing of the previous edition.

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 2026

Introduction

This document describes the structure and contents of a data element related to key management which can be conveyed in electronically transmitted messages within the financial services environment to support the secure management of cryptographic keys, where the financial services environment involves the communications between a card-accepting device and an acquirer, and between an acquirer and a card issuer. Key management of keys used in an Integrated Circuit Card (ICC) and the related data elements are not covered in this document. Key management procedures for the secure management of the cryptographic keys within the financial services environment are described in ISO 11568. Security-related data, such as Personal Identification Number (PIN) data and MACs, are described in ISO 9564 and ISO 16609, respectively.

This document provides key management information, including that related to the use and application of ISO 8583-1, i.e. the interchange messages used in processing card transactions, which are referenced in ISO 8583-1. However, the data elements assigned in ISO 8583-1 were built to accommodate earlier encryption technologies (e.g. data encryption standard, triple data encryption standard) and they are not long enough to accommodate the advanced encryption standard (AES) and/or other encryption methods for encrypting sensitive payment card data, which require longer data fields. Accordingly, in order to facilitate the use of AES for key management purposes related to ISO 8583-1, it has been proposed to expand the relevant data element fields in ISO 8583-1.

Although ISO 8583-1 is the most recent standard, in practice, many card processing parties still use older documents, either ISO 8583:1987 or ISO 8583:1993. Both of these documents have been withdrawn and replaced by the ISO 8583 series.

This document accommodates data encryption algorithm (DEA), triple data encryption algorithm (TDEA) and AES as encryption technologies. For DEA and TDEA, fields 52, 53 and 96 are used. For AES, depending on the key management and data encryption processes, fields 110, 111 or 50 can be used.

This document provides compatibility with the existing ISO standard on bank card originated messages (ISO 8583-1).

© Standards Australia Limited 2026

Australian Standard®

Financial services — Key-management-related data element — Application and usage of AS ISO 8583 data elements for encryption

1 Scope

This document describes a data element related to key management which can be transmitted either in transaction messages to convey information about cryptographic keys used to secure the current transaction, or in cryptographic service messages to convey information about cryptographic keys to be used to secure future transactions.

This document addresses the requirements for the use of the data element related to key management within ISO 8583-1, using the following two ISO 8583-1 data elements for DEA and TDEA:

— security related control information (data element 53);

— key management data (data element 96).

The data element related to key management for DEA and TDEA is constructed from the concatenation of two ISO 8583-1 message elements, data element 53 — security related control information, and data element 96 — key management data. It conveys information about the associated transaction's cryptographic key(s) and is divided into subfields including a control field, a key-set identifier and additional optional information. For AES implementations, the data elements are summarized in one field.

This document is applicable to either symmetric or asymmetric cipher systems.

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 8583-1, *Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 8583-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

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

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

3.1
asymmetric cipher
cipher in which the encipherment key and the decipherment key are different and it is computationally infeasible to deduce the (private) decipherment key from the (public) encipherment key

© Standards Australia Limited 2026