AS 2805.9:2026

Australian STANDARD®

STANDARDS Australia

Electronic funds transfer — Requirements for interfaces

Part 9: Privacy of communications



AS 2805.9:2026

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 09 March 2026.

This Standard was published on 8 May 2026.

The following are represented on Committee IT-005:

ANZ Banking Group
Australian Payments Network
Australian Retailers Association
Australian Securities and Investments Commission
Coles Group
Diebold Nixdorf
EFTPOS Payments Australia
National Australia Bank
New Payments Platform Australia
Pacific Research
SWIFT
Thales Australia
Triton Systems of Delaware
UL Transaction Security
Verisec International

This Standard was issued for comment as DR AS 2805.9:2025

Status of this document

Standards Australia publications are periodically reviewed to ensure their ongoing relevance and accuracy. This document may be withdrawn, revised, or superseded at any time. To verify this document's current status, visit:

www.standards.org.au

ISBN: 978 1 76175 664 1

Australian Standard®

Electronic funds transfer — Requirements for interfaces

Part 9: Privacy of communications

Originated as AS 2805.9—1991.
Second edition AS 2805.9:2000.
This document AS 2805.9:2026.

© Standards Australia Ltd 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).

Users must not use the content in this publication in combination with artificial intelligence (AI) tools for any purpose, unless they have the express prior written consent from Standards Australia.

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 AS 2805.9:2000, *Electronic funds transfer — Requirements for interfaces, Part 9: Privacy of communications*.

This document specifies methods of protecting from disclosure the information contained in electronic messages formatted in accordance with AS 2805. This document is not intended to address the issue within operational facilities, which are assumed to have controlled access and effective physical security.

This version of the document introduces the following:

(a) AES as the approved encryption algorithm.

(b) DUKPT as a key management methodology.

(c) New worked examples using AES.

A list of all parts in the AS 2805 series can be found in the Standards Australia online catalogue.

© Standards Australia Limited 2026

Contents

Page

Preface ..... **v**
1 Scope **1**
2 Application **1**
3 Normative references **1**
4 Terms and definitions **1**
5 Principles **4**
5.1 General 4
5.2 Protection 4
5.3 Protected elements 4
5.3.1 General 4
5.3.2 Point-to-point communications 4
5.3.3 Switched communications 4
6 Encryption **5**
6.1 Point-to-point communications 5
6.2 Switched communications 5
6.2.1 General 5
6.2.2 Message encipherment 6
6.3 Key management 6
6.3.1 General 6
6.3.2 Key update 6
7 Order of cryptographic processing **6**
Appendix A (informative) **Example message encipherment** **7**
Bibliography **9**

© Standards Australia Limited 2026

Australian Standard®

Electronic funds transfer — Requirements for interfaces

Part 9: Privacy of communications

1 Scope

This document specifies methods of protecting from disclosure the information contained in electronic messages formatted in accordance with AS 2805. This document is not intended to address the issue within operational facilities, which are assumed to have controlled access and effective physical security.

2 Application

This document may be adopted in all situations where protection against unauthorized disclosure is required.

3 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.

NOTE Documents referenced for informative purposes are listed in the Bibliography.

AS 2805, *Electronic funds transfers — Requirements for interfaces*

AS ISO 11568, *Financial services — Key management (retail)*

4 Terms and definitions

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

4.1
acquirer
institution (or its agent) that acquires from the card acceptor the financial data relating to the transaction and initiates such data into an interchange system

[SOURCE: ISO 9564-1:2017(en), 3.1]

4.2
advanced encryption standard
AES
16-byte block cipher with three possible key sizes

Note 1 to entry: This is defined in ISO/IEC 18033-3.

4.3
cipher text
data in their encrypted form

4.4
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

© Standards Australia Limited 2026