AS 2805.6.9:2026

Australian STANDARD®

STANDARDS Australia

Electronic funds transfers — Requirements for interfaces

Part 6.9: Key management — AES Session keys — Node-to-node



AS 2805.6.9:2026

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 Pty
SWIFT
Thales Australia
Triton Systems of Delaware
UL Transaction Security
Verisec International

This Standard was issued for comment as DR AS 2805.6.9:2025

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 This document may be withdrawn, revised, or superseded at any time.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 665 8

Australian Standard®

Electronic funds transfers — Requirements for interfaces

Part 6.9: Key management — AES Session keys — Node-to-node

Originated as AS 2805.6.9:2022.
This document AS 2805.6.9:2026.

© 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 2805.6.9:2022.

The objective of this document is to provide an interoperable method to transact within a node-to-node environment using the Advanced Encryption Standard (AES). It specifies management procedures applied in the authentication, encryption and decryption of electronic messages relating to financial transactions utilizing session keys.

This document —

(a) specifies the security interface methods between nodes;

(b) defines methods of interchange of the various encipherment keys used for securing transaction; and

(c) ensures that nodes can only authenticate messages at their correct destination.

This version of the document —

(i) clarifies key block protection key (KBPK) initialization and confirmation while adding an informative appendix with guidance on practical considerations;

(ii) adds necessary definitions; and

(iii) provides guidance on the cryptoperiod of both KBPKs and session keys.

This document is intended to be read in conjunction with AS ISO 20038, *Banking and related financial services — Key wrap using AES*, which is the basis for the requirements of this document, and AS ISO 11568, *Financial Services – Key management (retail)* and ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems.*

A list of all parts in the AS 2805.6 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 Overview **5**
5.1 General 5
5.2 Objectives of the scheme 5
5.3 Different keys for each function 5
5.4 Wrapped key block mechanism 6

6 Node-to-node AES key blocks **6**
6.1 General 6
6.2 Level 1: Key block protection key 7
6.3 Level 2: Key block authentication and encryption keys 7
6.4 Level 3: Session keys (KS) 8

7 Key initialization and session key changes **8**
7.1 Initialization 8
7.2 Changing session keys 8
7.2.1 General 8
7.2.2 Session key change 9
7.2.3 Synchronization of session key changes 9
7.2.4 Resynchronization 9

8 Storage and transport of keys **9**
8.1 General 9
8.2 Transport of session keys 10
8.3 Storage of session keys 11
8.4 KBPK storage 11

Appendix A (informative) **KBPK initialization — practical constraints** **12**

Bibliography **13**

© Standards Australia Limited 2026

Australian Standard®

Electronic funds transfers — Requirements for interfaces

Part 6.9: Key management — AES Session keys — Node-to-node

1 Scope

This document provides an interoperable method to transact within a node-to-node environment using the AES. It specifies management procedures applied in the authentication, encryption and decryption of electronic messages relating to financial transactions utilizing session keys.

This document —

(a) specifies the security interface methods between nodes;

(b) defines methods of interchange of the various encipherment keys used for securing transactions; and

(c) ensures that nodes can only authenticate messages at their correct destination.

NOTE Principles concerning key management and physical security are dealt with in AS ISO 11568 and AS ISO 20038, while PIN management is dealt with in ISO 9564-1.

2 Application

This document is intended for use in institutions where a node-to-node dialogue is required using AES keys.

3 Normative references

The following document is referred to in the text in such a way that some or all of their content constitutes the requirements of this document.

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

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

AS ISO 20038, *Banking and related financial services — Key wrap using AES*

4 Terms and definitions

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

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

(a) IEC Electropedia: available at http://www.electropedia.org/.

(b) ISO Online browsing platform: available at https://www.iso.org/obp.

4.1
algorithm
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

[SOURCE: AS ISO 16609:2025, 3.1]

© Standards Australia Limited 2026