AS 2805.6.9:2022

Australian STANDARD®

STANDARDS Australia

Electronic funds transfers — Requirements for interfaces

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

AS 2805.6.9:2022

This Australian Standard ® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 3 March 2022.

This Standard was published on 18 March 2022.

The following are represented on Committee IT-005:

Australian Payments Council
Australian Payments Network
EFTPOS Payments Australia
New Payments Platform Australia

Additional Interests

American Express
ANZ Banking Group
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
FIS Global
Mag-Tek
National Australia Bank
NCR Australia
Pacific Research
SWIFT
Thales Australia
Thales e-Security
Triton Systems of Delaware
UL Transaction Security
Westpac Banking Corporation
Woolworths Group

This Standard was issued in draft form for comment as DR AS 2805.6.9:2021.

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 76113 684 9

Electronic funds transfers — Requirements for interfaces

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

First published as AS 2805.6.9:2022.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, *Financial transaction systems.*

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.

The requirements of this document refer to AS ISO 20038 *Banking and related financial services — Key wrap using AES*.

This document is intended to be read in conjunction with AS ISO 20038:2019, *Banking and related financial services — Key wrap using AES.*

This document is part of the AS 2805.6 series, summarized as follows:

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

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

AS 2805.6.2, *Electronic funds transfer—Requirements for interfaces, Part 6.2: Key management—Transaction keys*

AS 2805.6.3, *Electronic funds transfer—Requirements for interfaces, Part 6.3: Key management—Session keys—Node to node*

AS 2805.6.5.1, *Electronic funds transfer—Requirements for interfaces, Part 6.5.1: Key management—TCU initialization—Principles*

AS 2805.6.5.2, *Electronic funds transfer—Requirements for interfaces, Part 6.5.2: Key management—TCU initialization—Symmetric*

AS 2805.6.5.3, *Electronic funds transfer — Requirements for interfaces, Part 6.5.3: Key management — TCU initialization — Asymmetric*

AS 2805.6.7, *Electronic funds transfer—Requirements for interfaces, Part 6.7: Key management—Transaction keys—Derived unique key per transaction (DUKPT)*

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.

Contents

Preface ..... **ii**

Section 1 Scope and general **1**
1.1 Scope 1
1.2 Application 1
1.3 Normative references 1
1.4 Terms and definitions 1

Section 2 Overview **5**
2.1 General 5
2.2 Objectives of the scheme 5
2.3 Different keys for each function 5
2.4 Wrapped key block mechanism 5

Section 3 Node-to-node AES key blocks **6**
3.1 Key hierarchy and management 6
3.1.1 General 6
3.1.2 Level 1: Key block protection key (KBPK) 7
3.1.3 Level 2: Key block authentication and encryption keys (KBAK and KBEK) 7
3.1.4 Level 3: Session keys (KS) 7

Section 4 Key confirmation and session key changes **8**
4.1 Initialisation 8
4.2 Key confirmation 8
4.3 Changing session keys 8
4.3.1 General 8
4.3.2 Session key change 8
4.3.3 Synchronisation of session key changes 9
4.3.4 Resynchronisation 9

Section 5 Storage and transport of keys **10**
5.1 General 10
5.2 Transport of session keys 10
5.3 Storage of session keys 11

Bibliography **12**

NOTES

Australian Standard®

Electronic funds transfers — Requirements for interfaces

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

Section 1 Scope and general

1.1 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 transaction; 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 2805.6.1.2 and AS ISO 20038

1.2 Application

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

1.3 Normative references

The following documents are 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 20038, *Banking and related financial services — Key wrap using AES*

1.4 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:

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

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

1.4.1
authentication
verification that a message was sent by the purported originator to the intended recipient and that the message was not changed in transit

[SOURCE: ISO/IEC 20944-1:2013, 3.11.1.9]