

AS 2805.6.9:2022



Electronic funds transfers — Requirements for interfaces

Part 6.9 **This is a preview. Click here to purchase the full publication.**



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

This is a preview. Click here to purchase the full publication.

- 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~~

This is a preview. [Click here to purchase the full publication.](#)

First published as AS 2805.6.9:2022.

© Standards Australia Limited 2022

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).

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 part of the AS 2805.6 series, summarized as follows:

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.