AS 2805.6.7—2011

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.7: Key management—Transaction keys—Derived unique key per transaction (DUKPT)

STANDARDS Australia

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 30 November 2011.
This Standard was published on 23 December 2011.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
- Australian Bankers Association
- Australian Industry Group
- Australian Payments Clearing Association
- EFTPOS Payments Australia

Additional Interests:

- Akyman Communications
- Australia and New Zealand Banking Group
- Coles Group
- Eracom Technologies Australia
- Inter-Tech Global Transaction Services
- Mag-Tek
- National Australia Bank
- NCR Australia
- Pacific Research
- Quest Software
- SecureNet
- Sundial
- Technical Security and Recovery Services
- Witham Laboratories

This Standard was issued in draft form for comment as DR AS 2805.6.7.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.7: Key management—Transaction keys—Derived unique key per transaction (DUKPT)

First published as AS 2805.6.7—2011.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 74342 008 9

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

This Standard is Part 6.7 of the following series:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.1	Part 1:	Communications
2805.2	Part 2:	Message structures, format and content
2805.3.1	Part 3.1:	PIN management and security—General
2805.3.2	Part 3.2:	PIN management and security—Offline
2805.4.1	Part 4.1:	Message authentication—Mechanism using a block cipher
2805.4.2	Part 4.2:	Message authentication—Mechanisms using a hash-function
2805.5.1	Part 5.1:	Ciphers—Data encipherment algorithm 1 (DEA 1)
2805.5.2	Part 5.2:	Ciphers—Modes of operation for an *n*-bit block cipher
2805.5.3	Part 5.3:	Ciphers—Data encipherment algorithm 2 (DEA 2)
2805.5.4	Part 5.4:	Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
2805.6.1.1	Part 6.1.1:	Key management—Principles
2805.6.1.2	Part 6.1.2:	Key management—Symmetric ciphers, their key management and life cycle
2805.6.1.4	Part 6.1.4:	Key management—Asymmetric cryptosystems—Key management and life cycle
2805.6.2	Part 6.2:	Key management—Transaction keys
2805.6.3	Part 6.3:	Key management—Session keys—Node to node
2805.6.4	Part 6.4:	Key management—Session keys—Terminal to acquirer
2805.6.5.1	Part 6.5.1:	Key management—TCU initialization—Principles
2805.6.5.2	Part 6.5.2:	Key management—TCU initialization—Symmetric
2805.6.5.3	Part 6.5.3:	Key management—TCU initialization—Asymmetric
2805.6.6	Part 6.6:	Key management—Session keys—Node to node with KEK replacement
2805.6.7	Part 6.7:	Key management—Transaction keys—Derived unique key per transaction (DUKPT) (this Standard)
2805.9	Part 9:	Privacy of communications
2805.10.1	Part 10.1:	File transfer integrity validation
2805.10.2	Part 10.2:	Secure file transfer (retail)
2805.11	Part 11:	Card parameter table
2805.12.1	Part 12.1:	Message content—Structure and format
2805.12.2	Part 12.2:	Application and registration procedures for Institution Identification Codes (IIC)
2805.12.3	Part 12.3:	Maintenance procedures for messages, data elements and code values
2805.13.1	Part 13.1:	Secure hash functions—General
2805.13.2	Part 13.2:	Secure hash functions—MD5
2805.13.3	Part 13.3:	Secure hash functions—SHA-1
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
2805.14.2	Part 14.2:	Secure cryptographic devices (retail)—Security compliance checklists for devices used in financial transactions
2805.16	Part 16:	Merchant category codes

In the AS 2805 series of Standards, definitions are specific to the Part in which they appear.

Acknowledgment is gratefully made to the American National Standards Institute for permission to reproduce certain extracts from the ANSI X9.24-1:2009 (Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques).

The terms ‘normative’ and ‘informative’ have been used in this Standard to define the application of the appendix to which they apply. A ‘normative’ appendix is an integral part of a Standard whereas an ‘informative’ appendix is for information and guidance only.

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 6.7: Key management—Transaction keys—Derived unique key per transaction (DUKPT)

1 SCOPE

This Standard specifies—

(a) a method of key management for keys used in the authentication, encipherment and decipherment of electronic messages relating to financial transactions using transaction keys;

(b) key identification techniques; and

(c) the data elements necessary for the transfer of security or key management information.

NOTE: Principles concerning key management and physical security are dealt with in AS 2805.6.1.1.

2 APPLICATION

This Standard may be adopted in all situations where a secure terminal to acquirer dialogue is desired in conjunction with minimally tamper resistant devices with tamper evidence characteristics as specified in AS 2805.14.1.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.3	Part 3:	PIN management and security (all parts)
2805.4	Part 4:	Message authentication
2805.5.4	Part 5.4:	Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
2805.6.1.1	Part 6.1.1:	Key management—Principles
2805.9	Part 9:	Privacy of communications
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

4 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

4.1 Acquirer

The institution, or its agent, that acquires the financial data relating to the transaction from the card acceptor and initiates that data into an interchange system.

4.2 Acquirer network

A network of one or more processing centres, which may represent one or more acquirers or card issuers or both.