AS 2805.6.6—2006

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 6.6: Key management—Session keys—Node to node with KEK replacement

This Australian Standard was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 31 March 2006.
This Standard was published on 21 June 2006.

The following are represented on Committee IT-005:

Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Electrical and Electronic Manufacturers Association
Australian Retailers Association
Credit Card Industry
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 04136.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 6.6: Key management—Session keys—Node to node with KEK replacement

First published as AS 2805.6.6—2006.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7530 6

PREFACE

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

This Standard is Part 6.6 of the following series:

AS		
2805		Electronic funds transfer—Requirements for interfaces
2805.1	Part 1:	Communications
2805.2	Part 2:	Message structure, 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—Mechanisms 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 algorithm
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	Part 6.1:	Key management—Principles
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
2805.9	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:	Message content—Codes
2805.12.3	Part 12.3:	Message content—Maintenance of codes
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:	Security, compliance checklists for devises used in magnetic stripe and card systems

The following Handbooks relate to the AS 2805 series of Standards:

HB	
127	Electronic funds transfer—Implementing message content Standards—Conversion Handbook (changing from AS 2805.2 to the AS 2805.12 series)
128	Electronic funds transfer—Implementing message content Standards—Terminal Handbook
129	Electronic funds transfer—Implementing message content Standards—Interchange Handbook

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

Statements expressed in mandatory terms in notes to figures are deemed to be requirements of the Standard.

The term ‘informative’ has been used in this Standard to define the application of the appendix to which it applies. An ‘informative’ appendix is only for information and guidance.

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 6.6: Key management—Session keys—Node to node with KEK replacement

1 SCOPE

This Standard specifies management techniques for keys used in the authentication, encipherment and decipherment of electronic messages relating to financial transactions using session keys.

In particular, this Standard—

(a) defines security interface procedures between nodes;

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

(c) ensures that messages can only be authenticated at their correct destination.

NOTE: Principles concerning key management and physical security are dealt with in AS 2805.6.1.

2 APPLICATION

This Standard may be adopted in all situations where a secure node-to-node dialogue is desired and where on-line KEK replacement is desired.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.2	Part 2:	Message structure, format and contents
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—Mechanisms 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)
2805.5.3	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	Part 6.1:	Key management—Principles
2805.6.2	Part 6.2:	Key management—Transaction keys
2805.6.4	Part 6.4:	Key management—Session keys—Terminal to acquirer
2805.13.1	Part 13.1:	Secure hash functions—General
2805.13.2	Part 13.2:	Secure hash functions—MD5
2805.13.2	Part 13.3:	Secure hash functions—SHA-1
2805.14.1	Part 14.1:	Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods