Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.5.3: Key management—TCU initialization—Asymmetric

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 21 November 2003.
This Standard was published on 24 February 2004.

The following are represented on Committee IT-005:

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

This Standard was issued in draft form for comment as DR 02561.

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 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Standards may also be withdrawn.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.

AS 2805.6.5.3—2004
(Incorporating Amendment No. 1)

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.5.3: Key management—TCU initialization—Asymmetric

Originated as AS 2805.6.5.3—1992.
Second edition 2004.
Reissued incorporating Amendment No. 1 (January 2007).

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

ISBN 0 7337 5637 9

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems to supersede AS 2805.6.5.3—1992.

This Standard incorporates Amendment No. 1 (January 2007). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

The objective of this Standard is to specify the definition of the interface and method to initialize remotely a terminal cryptographic unit (TCU) when the TCU is not required to be delivered via a sponsor's facility.

This Standard is Part 6.5.3 of AS 2805 *Electronic funds transfer—Requirements for interfaces* which, when complete, will consist of the following:

Part 1: Communications
Part 2: Message structure, format and content
Part 3: PIN management and security
Part 4.1: Message authentication—Mechanisms using a block cipher
Part 4.2: Message authentication—Mechanisms using a hash function
Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)
Part 5.2: Ciphers—Modes of operation for an n-bit block cipher algorithm
Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)
Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
Part 6.1: Key management—Principles
Part 6.2: Key management—Transaction keys
Part 6.3: Key management—Session keys—Node to node
Part 6.4: Key management—Session keys—Terminal to acquirer
Part 6.5.1: Key management—TCU initialization—Principles
Part 6.5.2: Key management—TCU initialization—Symmetric
Part 6.5.3: Key management—TCU initialization—Asymmetric (this Standard)
Part 9: Privacy of communications
Part 10: File transfer integrity validation
Part 10.2: Secure file transfer (retail)
Part 11: Card parameter table
Part 12.1: Message content—Structure and format
Part 12.2: Message content—Codes
Part 12.3: Message content—Maintenance of codes
Part 13.1: Secure hash functions—General
Part 13.2: Secure hash functions—MD5
Part 13.3: Secure hash functions—SHA-1
Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems
Part 15: ICC base stored value/inter-sector electronic purse—Principles

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)
HB 128 Electronic funds transfer—Implementing message content Standards—Terminal Handbook

HB 129 Electronic funds transfer—Implementing message content Standards—Interchange Handbook

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

This Standard differs from the previous edition in the following aspects:

(a) The original Appendix A has been withdrawn as all required notation can be found in AS 2805.6.1, and it has been replaced with a new Appendix for Message Sequence Summary.

(b) It has been updated to increase the DEA2 key sizes employed.

(c) The content has been extended to include all initialization required to prepare the TCU for financial transactions and provides a better linkage to AS 2805.6.2 and AS 2805.6.4.

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 only for information and guidance.

CONTENTS

FOREWORD

Key management is a critical part of application specifications. In the AS 2805 series, Part 6.5.1 defines the principles to be observed for terminal cryptographic unit (TCU) initialization. Part 6.5.2 describes a TCU initialization scheme which utilizes a symmetric cipher, whereas Part 6.5.3 (this Standard) describes a scheme which incorporates the use of an asymmetric cipher.

Choice of an appropriate implementation will be governed by the nature of the interface application and the constraints of maintaining the security principles within it.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 6.5.3: Key management—TCU initialization—Asymmetric

1 SCOPE

This Standard defines the interface and method to initialize remotely a terminal cryptographic unit (TCU). In the context of this Standard the term initialization refers only to the initial set-up of a symmetric cryptographic keying relationship between the TCU and the acquirer(s).

2 APPLICATION

This Standard is designed to be adopted wherever secure remote terminal initialization is required and where the TCU is not required to be delivered via a sponsor's facility.

This Standard shall be used in conjunction with the key management systems described in AS 2805.6.2 and AS 2805.6.4.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS		
2805		
2805.2	Part 2:	Message structure, format and content
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
2805.6.5.1	Part 6.5.1:	Key management—TCU initialization—Principles
2805.11	Part 11:	Card parameter table
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, which acquires from the card acceptor the financial data relating to the transaction, and which may initiate that data into an interchange system.

4.2 Acquirer initialization key (KIA)

A DEA 3 key established in the TCU during its initialization process, and used to establish an initial key for the key management scheme between the TCU and acquirer. The key for acquirer 'n' is denoted KIA_n.

4.3 Acquiring institution identification code (AIIC)

This code is used to uniquely identify the acquiring institution.

