AS 2805.6.5.3(Int):2017
Expires 2 November 2019

AS 2805.6.5.3(Int):2017

Interim Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.5.3: Key management—TCU initialization—Asymmetric

This Interim Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 11 October 2017.
This Interim Standard was published on 2 November 2017.

The following are represented on Committee IT-005:

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

This Interim Standard was issued in draft form for comment as DR AS 2805.6.5.3:2017.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Interim 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Standards may also be withdrawn.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.

Interim Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 6.5.3: Key management—TCU initialization—Asymmetric

Originally as AS 2805.6.5.3—1992.
Previous edition 2004.
Revised and redesignated as AS 2805.6.5.3(Int):2017.

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

ISBN 978 1 76035 938 6

PREFACE

This Interim Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.6.5.3—2004.

The objective of this Interim 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 revision increases the DEA 2 key sizes employed, and allows for hashes of keys to be used.

Attention is drawn to the fact that this is an Interim Standard and should be regarded as a developmental Standard and liable to future alteration. This Interim Standard will have a currency of up to two years from its date of publication.

At the conclusion of that period it will be superseded by an Australian Standard or the currency of the Interim Standard extended for a further two year period or withdrawn.

This Interim Standard is Part 6.5.3 of the AS 2805 series of Standards:

AS		
2805		Electronic funds transfer—Requirements for interfaces
2805.2	Part 2:	Message structure, format and content
2805.3.1	Part 3.1:	PIN management and security—General
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
2805.6.1.1	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
2805.9	Part 9:	Privacy of communications
2805.10	Part 10.1:	File transfer integrity validation
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

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

SAA 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, the definitions of words and phrases used are specific to the Part in which they appear.

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

Standards Australia welcomes comments on this Interim Standard. Please contact Standards Australia at mail@standards.org.au for a copy of the commenting template and return the completed form to the same email address. Standards Australia Committee IT-005 will review comments received.

CONTENTS

Page

FOREWORD

Key management is a critical part of application specifications. In the AS 2805 series, Part 6.5.1, *Key management—TCU initialization—Principles*, defines the principles to be observed for terminal cryptographic unit (TCU) initialization. Part 6.5.2, *Key management—TCU initialization—Symmetric,* describes a TCU initialization scheme which utilizes a symmetric cipher, whereas Part 6.5.3, *Key management—TCU initialization—Asymmetric* (this Interim 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 Interim Standard defines the interface and method to initialize remotely a terminal cryptographic unit (TCU). In the context of this Interim 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 Interim 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 Interim Standard shall be used in conjunction with the key management scheme requirements in AS 2805.6.2, *Electronic funds transfer—Requirements for interfaces*, Part 6.2, *Key management—Transaction keys* and AS 2805.6.4, *Electronic funds transfer—Requirements for interfaces*, Part 6.4, *Key management—Session keys—Terminal to acquirer*.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Interim Standard:

AS

2805	Electronic funds transfer—Requirements for interfaces	
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
2805.6.1.1	Part 6.1.1:	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

ISO/IEC

10118	Information technology—Security techniques—Hash-functions	
10118-3	Part 3:	Dedicated hash-functions
18031	Information Technology—Random number generation	