Australian Standard™

Electronic funds transfer—
Requirements for interfaces

Part 6.5.2: Key management—
TCU initialization—Symmetric

This Australian Standard was prepared by Committee IT/5, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 29 October 1999 and published on 10 January 2000.

The following interests are represented on Committee IT/5:

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Electrical and Electronic Manufacturers Association

Australian Institute of Petroleum

Australian Retailers Association

Consumers Federation of Australia

Credit card industry

Reserve Bank of Australia

Telstra Corporation

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 Standards may also be withdrawn.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 Australia web site 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 Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for the 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.com.au, or write to the Chief Executive, Standards Australia International Ltd, PO Box 1055, Strathfield, NSW 2135.

This Standard was issued in draft form for comment as DR 97381.

Australian Standard™

Electronic funds transfer – Requirements for interfaces

Part 6.5.2: Key management—TCU initialization—Symmetric

First published as AS 2805.6.5.2—2000.

Published by Standards Australia International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 3079 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT/5, Financial Transaction Systems, to define the interface and provide a method initializing remotely a terminal cryptographic unit.

This Standard is part of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interface, which is comprised of the following:

AS		
2805	Electronic funds transfer—Requirements for interfaces	
2805.1	Part 1:	Communications
2805.2	Part 2:	Message structure, format and content
2805.3	Part 3:	PIN management and security
2805.4	Part 4:	Message authentication
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 (this Standard)
2805.6.5.3	Part 6.5.3:	Key management—TCU initialization—Asymmetric
2805.9	Part 9:	Privacy of communications
2805.10	Part 10:	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:	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

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

Part 4.1, Message authentication using DEA 3, of the AS 2805 series is in the course of preparation.

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 ‘normative’ has been used in this Standard to define the application of the appendix to which it applies. A ‘normative’ appendix is an integral part of a Standard.

CONTENTS

Page

FOREWORD 4

1 SCOPE 5
2 APPLICATION 5
3 REFERENCED DOCUMENTS 5
4 ABBREVIATIONS 5
5 DEFINITIONS 6
6 OVERVIEW 8
7 SPECIFICATION OF FUNCTIONAL ELEMENTS 8
8 SCHEME OPERATION 9
9 SCHEME COMPONENTS 10
10 RE-INITIALIZATION 13

APPENDIX A DIAGRAMMATIC EXPLANATIONS OF THE SCHEME IN OPERATION 14

FOREWORD

Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of all data ever enciphered under it. The generation, distribution and protection of cryptographic keys is called ‘key management’.

Key management is a critical part of application specifications. In the AS 2805 series, the intent of AS 2805.6.5.1 is to define the principles to be observed for terminal cryptographic unit (TCU) initialization. This Standard describes a TCU initialization scheme which utilizes a symmetric cipher, whereas AS 2805.6.5.3 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 6.5.2: Key management—TCU initialization—Symmetric

1 SCOPE

This Standard defines the interface and specifies a scheme for initializing remotely a terminal cryptographic unit (TCU).

2 APPLICATION

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

This Standard is intended to 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	Electronic funds transfer—Requirements for interfaces	
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
2805.6.5.1	Part 6.5.1:	Key management—TCU initialization—Principles
2805.11	Part 11:	Card parameter table

4 ABBREVIATIONS

The abbreviations used in this Standard are as follows:

AIIC	Acquiring institution identification code.
CPT	Card parameter table.
DEA	Data encipherment algorithm.
FKM	Key management facility.
KCA_M	Cross acquirer key (manufacturer).
KCA_S	Cross acquirer key (sponsor).
KIA	Acquirer initial key.
KIA_M	Manufacturer's component of acquirer initial key.

