AS 2805.6.5.3:2020

Australian STANDARD®

Electronic funds transfer — Requirements for interfaces

Part 6.5.3: Key management — TCU initialization — Asymmetric

STANDARDS Australia

AS 2805.6.5.3:2020

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 4 June 2020.

This Standard was published on 19 June 2020.

The following are represented on Committee IT-005:

Australian Payments Council
Australian Payments Network
EFTPOS Payments Australia
New Payments Platform Australia

Additional Interests

American Express
ANZ Banking Group
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
FIS Global
Gemalto
Mag-Tek
National Australia Bank
Pacific Research
SWIFT
Thales e-Security
Triton Systems of Delaware LLC
UL Transaction Security
Westpac Banking Corporation
Woolworths Group

This Standard was issued in draft form for comment as DR AS 2805.6.5.3:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 876 2

Electronic funds transfer — Requirements for interfaces

Part 6.5.3: Key management — TCU initialization — Asymmetric

Originated as AS 2805.6.5.3—1992.
Previous edition 2004.
Revised and redesignated as AS 2805.6.5.3(Int):2017.
Revised and redesignated as AS 2805.6.5.3:2020.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.6.5.3 Int:2017.

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.

The major changes in this edition are as follows:

(a) Increase in the DEA 2 key sizes employed.

(b) Allows for hashes of keys to be used.

This Standard is Part 6.5.3 of the following series of Standards:

AS 2805.2, *Electronic funds transfer — Requirements for interfaces, Part 2: Message structure, format and content*

AS 2805.3.1, *Electronic funds transfer — Requirements for interfaces, Part 3.1: PIN management and security — General*

AS 2805.4.1, *Electronic funds transfer — Requirements for interfaces, Part 4.1: Message authentication — Mechanisms using a block cipher*

AS 2805.4.2, *Electronic funds transfer — Requirements for interfaces, Part 4.2: Message authentication — Mechanisms using a hash function*

AS 2805.5.1, *Electronic funds transfer — Requirements for interfaces, Part 5.1: Ciphers — Data encipherment algorithm 1 (DEA 1)*

AS 2805.5.2, *Electronic funds transfer — Requirements for interfaces, Part 5.2: Ciphers — Modes of operation for an n-bit block cipher algorithm*

AS 2805.5.3, *Electronic funds transfer — Requirements for interfaces, Part 5.3: Ciphers — Data encipherment algorithm 2 (DEA 2)*

AS 2805.5.4, *Electronic funds transfer — Requirements for interfaces, Part 5.4: Ciphers — Data encipherment algorithm 3 (DEA 3) and related techniques*

AS 2805.6.1.1, *Electronic funds transfer — Requirements for interfaces, Part 6.1.1: Key management — Principles*

AS 2805.6.1.2, *Electronic funds transfer — Requirements for interfaces, Part 6.1.2: Key management — Symmetric ciphers, their key management and life cycle*

AS 2805.6.1.4, *Electronic funds transfer — Requirements for interfaces, Part 6.1.4: Key management — Asymmetric cryptosystems — Key management and life cycle*

AS 2805.6.2, *Electronic funds transfer — Requirements for interfaces, Part 6.2: Key management — Transaction keys*

AS 2805.6.3, *Electronic funds transfer — Requirements for interfaces, Part 6.3: Key management — Session keys — Node to node*

AS 2805.6.4, *Electronic funds transfer — Requirements for interfaces, Part 6.4: Key management — Session keys — Terminal to acquirer*

AS 2805.6.5.1, *Electronic funds transfer — Requirements for interfaces, Part 6.5.1: Key management — TCU initialization — Principles*

AS 2805.6.5.2, *Electronic funds transfer — Requirements for interfaces, Part 6.5.2: Key management — TCU initialization — Symmetric*

AS 2805.9, *Electronic funds transfer — Requirements for interfaces, Part 9: Privacy of communications*

AS 2805.10, *Electronic funds transfer — Requirements for interfaces, Part 10.1: File transfer integrity validation*

AS 2805.11, *Electronic funds transfer — Requirements for interfaces, Part 11: Card parameter table*

AS 2805.12.1, *Electronic funds transfer — Requirements for interfaces, Part 12.1: Message content — Structure and format*

AS 2805.12.2, *Electronic funds transfer — Requirements for interfaces, Part 12.2: Application and registration procedures for Institution Identification codes (IIC)*

AS 2805.12.3, *Electronic funds transfer — Requirements for interfaces, Part 12.3: Maintenance procedures for messages, data elements and code values*

AS 2805.13.1, *Electronic funds transfer — Requirements for interfaces, Part 13.1: Secure hash functions — General*

AS 2805.13.2, *Electronic funds transfer — Requirements for interfaces, Part 13.2: Secure hash functions — MD5*

AS 2805.13.3, *Electronic funds transfer — Requirements for interfaces, Part 13.3: Secure hash functions—SHA-1*

AS 2805.14.1, *Electronic funds transfer — Requirements for interfaces, Part 14.1: Secure cryptographic devices (retail) — Concepts, requirements and evaluation methods*

AS 2805.14.2, *Electronic funds transfer — Requirements for interfaces, 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)*

SAA HB 128, *Electronic funds transfer — Implementing message content Standards — Terminal Handbook*

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

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

The term “informative” is used in Standards to define the application of the appendix to which it applies. An “informative” appendix is only for information and guidance.

Contents

Introduction

Key management is a critical part of application specifications. In the AS 2805 series —

(a) AS 2805.6.5.1, *Key management — TCU initialization — Principles*, defines the principles to be observed for terminal cryptographic unit (TCU) initialization;

(b) AS 2805.6.5.2, *Key management — TCU initialization — Symmetric*, describes a TCU initialization scheme which utilizes a symmetric cipher; whereas

(c) AS 2805.6.5.3, *Key management — TCU initialization — Asymmetric* (this Standard), describes a scheme which incorporates the use of an asymmetric cipher.

The relevant Standard will be determined by the nature of the interface application and the constraints of maintaining the security principles within it.

NOTES

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).

This Standard provides a method that removes the requirement for visits by agents of sponsors and acquirers during the life of a TCU for the purpose of initialization of key management cryptographic variables.

This Standard defines the technique by which TCUs can be remotely initialized. Initialization is limited to cryptographic initialization of the first symmetric key of the key management scheme used between the TCU and each acquirer.

This Standard minimizes the probability of initialization of TCUs unknown to the sponsor.

2 Application

This Standard is intended for use 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 scheme requirements in AS 2805.6.2 and AS 2805.6.4.

3 Normative documents

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document.

NOTE Documents for informative purposes are listed in the Bibliography.

AS 2805.5.3, *Electronic funds transfer — Requirements for interfaces, Part 5.3: Ciphers — Data encipherment algorithm 2 (DEA 2)*

AS 2805.6.1.1, *Electronic funds transfer — Requirements for interfaces, Part 6.1.1: Key management — Principles*

AS 2805.6.2, *Electronic funds transfer — Requirements for interfaces, Part 6.2: Key management — Transaction keys*

AS 2805.6.4, *Electronic funds transfer — Requirements for interfaces, Part 6.4: Key management — Session keys — Terminal to acquirer*

AS 2805.6.5.1, *Electronic funds transfer — Requirements for interfaces, Part 6.5.1: Key management — TCU initialization — Principles*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

4 Terms and definitions

For the purpose of this document, the following terms and definitions apply.