Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)

STANDARDS AUSTRALIA

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 and published on 1 March 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

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 Standards may also be withdrawn.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 International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 03141.

Australian Standard™

Electronic funds transfer—Requirements for interfaces

Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)

Originated as AS 2805.5.3—1992.
Second edition 2004.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5638 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005 on Financial Transaction Systems to supersede AS 2805.5.3—1992.

The objective of this Standard is to provide a mathematical algorithm for enciphering, deciphering, signing and verifying information relating to financial applications.

This Standard is Part 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: Message authentication
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) (this Standard)
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
Part 7: POS message content
Part 8: Financial institution message content
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

The terms ‘normative’ and ‘informative’ are used 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.

The algorithm specified in this Standard is based on that specified in ISO/IEC 9594-8, *Information Processing Systems—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks*, Appendix E.

CONTENTS

Page

FOREWORD

This Standard specifies a data encipherment algorithm (DEA) for the cryptographic protection of digital data. The DEA is a complete description of a mathematical algorithm for enciphering and deciphering binary coded information. Encipherment transforms data (plain text) into an unintelligible form (cipher text). Decipherment transforms the cipher text back to the original form. The algorithm described in this Standard is an n-bit block cipher algorithm, where n is selectable according to the security level required. The length of a key is related to the block size selected. The algorithm specified in this Standard is identical to the algorithm described in Appendix E of ISO/IEC 9594-8.

The keys are generated in such a way that secret components are unpredictable. The algorithm specified in this Standard is asymmetric in that different keys are used for encipherment and decipherment. The key used to decipher data must be kept secret in order to use this cryptosystem to satisfy security requirements. The encipherment algorithm specified in this Standard is publicly known. Therefore, the cryptographic security of the data depends solely on the security provided for the keys.

The asymmetric nature of the DEA specified in this Standard means that the private key need not be shared at any time during the operation of systems using this algorithm.

STANDARDS AUSTRALIA

Australian Standard
Electronic funds transfer—Requirements for interfaces

Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)

1 SCOPE

This Standard specifies a mathematical algorithm for enciphering, deciphering, signing and verifying information relating to financial applications.

2 APPLICATION

This Standard can be used for all applications (e.g. data transmission, data storage, authentication, privacy) that require encipherment, decipherment, signing and verification of messages relating to financial transactions and information related to the management of components of EFT systems.

3 REFERENCES

AS	
2805	Electronic funds transfer—Requirements for interfaces
2805.6.1	Part 6.1: Key management—Principles
ISO/IEC	
9796	Information technology—Security techniques—Digital signature schemes giving message recovery

4 DEFINITIONS

For the purpose of this Standard the definitions below apply.

4.1 Algorithm

A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

4.2 Cipher text

Enciphered information.

4.3 Clear text

Unenciphered information.

NOTES:

1 ‘Clear text’ may also be referred to as ‘ plain text’.

2 ‘Clear text’ may contain enciphered information from a previous enciphering operation.

4.4 Data encipherment algorithm (DEA)

An algorithm designed to encipher and decipher blocks of data.

4.5 Decipherment

The transformation of cipher text into plain text.

NOTE: ‘ Decipherment’ is also referred to as ‘decryption’.