Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)

This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 20 May 1992. This Standard was published on 14 September 1992.

The following are represented on Committee IT-005:

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

This Standard was issued in draft form for comment as DR 90027.

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Standards may also be withdrawn.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.

Australian Standard®

Electronic funds transfer—Requirements for interfaces

Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)

Originally as part of AS 2805.5—1985.
Revised and redesignated in part as AS 2805.5.1—1992.
Reissued incorporating Amendment No. 1 (January 2007).

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

ISBN 0 7262 7603 0

PREFACE

This Standard was prepared by the Standards Australian Committee on Financial Transaction Systems as Part 5.1 of the AS 2805 series of Standards on requirements for interfaces for electronic funds transfer (EFT) to supersede (in part) AS 2805.5—1985, Data Encryption Algorithm. The Parts of AS 2805 are as follows:

Part 1	Communications interface and data representation
Part 2	Message structure, format and content
Part 3	PIN management and security
Part 4	Message authentication
Part 5.1	Ciphers—Data encipherment algorithm 1 (DEA 1) (this Standard)
Part 5.2	Ciphers—Modes of operation for an n-bit cipher algorithm
Part 5.3	Ciphers—Data encipherment algorithm 2 (DEA 2)
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	Secure file transfer (in preparation)
Part 11	Card parameter table (in preparation)

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 algorithm specified in this Standard is based on the algorithm specified in American National Standard ANSI X3.92—1981, American National Standard Data encryption algorithm, copyright 1981 by the American National Standards Institute.

Material from ANSI X3.92 has been incorporated in the present Standard with the permission of the American National Standards Institute and acknowledgement is made of the assistance received from ANSI.

CONTENTS

FOREWORD

This Standard specifies a data encipherment algorithm (DEA) for the cryptographic protection of digital data. The DEA is a mathematical algorithm for enciphering and deciphering binary-coded information. Enciphering data converts it to an unintelligible form. Deciphering converts the data back to the original form. The algorithm described in this Standard specifies both enciphering and deciphering operations, which are based on a binary number called a key. The key consists of 64 binary digits (0s or 1s), of which 56 bits are used directly by the algorithm and 8 bits may be used for error detection. The algorithm specified in this Standard is identical to the algorithm specified in ANSI X3.92 and Federal Information Processing Standard 46 (published by the US National Institute of Standards and Technology/CFIPS).

Binary-coded data may be cryptographically protected using the DEA in conjunction with a key. The key is generated in such a way that each of the 56 bits used directly by the algorithm is random. To decipher data, each member of a group of authorized users of enciphered data must have the key that was used for encipherment. This key, held by each member in common, is used to decipher the data received in enciphered form from other members of the group. 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 key used to encipher and decipher the data.

Data can only be deciphered by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key, cannot decipher it and obtain the original data. However, anyone who does have the key and the algorithm, can easily obtain the original data. A standard algorithm, based on a secure key, thus provides a basis for exchanging enciphered digital data by issuing the key used to encipher it to those authorized to have the data.

STANDARDS AUSTRALIA

Australian Standard

Electronic funds transfer—Requirements for interfaces

Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)

1 SCOPE This Standard specifies a mathematical algorithm for enciphering and deciphering the information relating to financial transactions.

2 APPLICATION This Standard can be used for all applications (e.g. data transmission, data storage, authentication, privacy) that require encipherment and decipherment of messages relating to financial transactions.

3 REFERENCED DOCUMENTS The following documents are referred to in this Standard:

AS
2805.5 Electronic funds transfer—Requirements for interfaces—Ciphers

ANSI
X3.92 Data encryption algorithm 1981

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 encrypted information from a previous encryption 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 clear text.

NOTE: 'Decipherment' is also referred to as 'decryption'.

4.6 Encipherment The transformation of clear text into cipher text for the purpose of security or privacy.

NOTE: 'Encipherment' is also referred to as 'encryption'.

4.7 Encipherment algorithm A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations to the normal representation of information through the use of variable elements controlled by the application of a key.

4.8 Key A 64-bit quantity which is used for transformation between cipher text and clear text.

4.9 Modulo 2 addition A mathematical operation equivalent to binary addition without carry, giving the following values:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

NOTE: 'Modulo 2 addition' is represented by the symbol $\oplus$ and is also referred to as an 'exclusive OR' operation.

5 DATA ENCIPHERMENT ALGORITHM SPECIFICATIONS

5.1 Introduction The data encipherment algorithm (DEA) is designed to encipher and decipher blocks of data consisting of 64 bits, under control of a 64-bit key. Encipherment can only be accomplished by using the same key that was used for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the encipherment process. A block to be enciphered is subject to an initial permutation IP, then to a complex key-dependent computation, and finally to a permutation IP^{-1} that is the inverse of the initial permutation. The key-dependent computation can be simply defined in terms of a function, *f*, called the cipher function, and a function *KS*, called the key schedule. Descriptions of the computation and the encipherment operation are provided in Clause 5.2. The decipherment operation is described in Clause 5.3. Description of the encipherment function *f* is given in Clause 5.4. The *S* and *KS* functions of the algorithm are described in Clause 5.5.

NOTE: The representation of keys, and special key values, are described in Appendix A.