Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.3—KEY MANAGEMENT—SESSION KEYS—NODE TO NODE

This Australian Standard was prepared by Committee IS/5, Electronic Funds Transfer. It was approved on behalf of the Council of the Standards Association of Australia on 17 December 1987 and published on 5 February 1988.

The following interests are represented on Committee IS/5:

Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Computer Equipment Manufacturers Association
Australian Electrical and Electronics Manufacturers Association
Australian Federation of Credit Unions Ltd
Australian Information Industry Association Ltd
Australian Institute of Petroleum
Australian Retailers Association
Australian Software Houses Association
Catering Institute of Australia
Life Insurance Federation of Australia
National card issuers
National network operators
Reserve Bank of Australia
Telecom Australia

This Standard was issued in draft form for comment as DR 87056.

Australian Standard®

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

Part 6.3—KEY MANAGEMENT—SESSION KEYS—NODE TO NODE

First published as AS 2805.6.3—1988.

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140

ISBN 0 7262 4835 5

PREFACE

This Standard was prepared by the Association's Committee on Electronic Funds Transfer as Part 6.3 of the AS 2805 series of Standards on electronic funds transfer (EFT) requirements for interfaces. 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: Data Encryption Algorithm

Part 6.1: Key Management — Principles*

Part 6.2: Key Management — Transaction Keys*

Part 6.3: Key Management — Session Keys — Node to Node* (this Standard)

Part 6.4: Key Management — Session Keys — Terminal to Acquirer*

Part 7: POS Message Content

Part 8: Financial Institution Message Content

Parts 1 to 5 were first published on 17 May 1985 and Parts 7 and 8 were first published on 3 November 1986.

This Standard (AS 2805.6.3) was developed from the experience gained by existing providers of EFT/POS systems in Australia, and by subsequent international developments in the area. It is not intended to invalidate existing EFT/POS systems, but to constitute a formal specification which will standardize future development of EFT/POS systems in Australia.

Appendix B is included for the guidance of users but does not form part of the requirements of this Standard.

---

* Published simultaneously.

CONTENTS

FOREWORD

Keys must be protected. Maintaining the secrecy of keys is of the utmost importance because the compromise of any key allows the compromise of all data ever encrypted under it. The generation, distribution, and protection of keys is called 'key management'.

Key management is a critical part of application specifications. In the AS 2805 series, Part 6.1 defines the principles to be observed for key management when developing specifications. Part 6.2 deals with transaction keys, Part 6.3 (this Standard) with node-to-node session keys and Part 6.4 with terminal-to-acquirer session keys. 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.

The key management system described in this Standard uses session keys. The advantages of this system are as follows:

(a) The scheme is independent of the network architecture and allows for gateways to other networks, e.g. international cards.

(b) The node to node scheme can be used in conjunction with the schemes described in AS 2805.6.2 and AS 2805.6.4.

STANDARDS ASSOCIATION OF AUSTRALIA

Australian Standard

ELECTRONIC FUNDS TRANSFER—REQUIREMENTS FOR INTERFACES

PART 6.3: KEY MANAGEMENT—SESSION KEYS—NODE TO NODE

1 SCOPE. This Standard specifies key management techniques for keys used in the authentication, encryption and decryption of electronic messages relating to financial transactions using session keys.

In particular, this Standard—

(a) defines security interface procedures between nodes;

(b) defines methods of interchange of the various encryption keys used for securing transactions; and

(c) ensures that messages can only be authenticated at their correct destination.

NOTE: Principles concerning key management and physical security are dealt with in AS 2805.6.1.

2 APPLICATION. This Standard may be adopted in all situations where a secure node-to-node dialogue is desired.

This Standard can be used in conjunction with the terminal-to-acquirer 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
- AS 2805.2 Message Structure, Format and Content
- AS 2805.3 PIN Management and Security
- AS 2805.4 Message Authentication
- AS 2805.5 Data Encryption Algorithm
- AS 2805.6.1 Key Management—Principles
- AS 2805.6.2 Key Management— Transaction Keys
- AS 2805.6.4 Key Management— Session Keys— Terminal to Acquirer
- AS 2805.8 Financial Institution Message Content

ISO TR 8509 Information Processing Systems—Open Systems Interconnection— Service Conventions.

4 DEFINITIONS. For the purpose of this Standard, the definitions below apply.

4.1 Acquirer—the institution, or its agent, which acquires, from the card acceptor, the financial data relating to the transaction, and which initiates that data into an interchange system.

4.2 Acquirer network—a network of one or more processing centres which may represent one or more acquirers or card issuers or both.

4.3 Authentication—the act of determining that a message comes from a source authorized to originate messages of that type and that the message is as authorized.

4.4 Back tracking—the ability to use current key values together with information previously transmitted or received, to determine previous key values.

4.5 Card issuer—the institution, or its agent, which issues the identification card to the cardholder.

NOTE: Hereinafter referred to as 'issuer'.

4.6 Cipher text—clear text that has been encrypted.

4.7 Clear text—intelligible text or signals that have meaning and that can be read and used.

4.8 Completion message—a message generated to confirm that a transaction has been completed.

4.9 Confirmation message—a message generated to confirm that a transaction has been completed.

4.10 Data Encryption Algorithm (DEA)—an encryption algorithm designed to encrypt and decrypt blocks of data.

NOTE: A DEA is specified in AS 2805.5.

4.11 Data key (KD)—generic reference to a session key used to encrypt/decrypt data excluding PIN data.

NOTE: The data encryption send key (KDs) is used for outgoing messages and the data encryption receive key (KDr) is used for incoming messages.

4.12 Decryption—the transformation of cipher text into clear text.

NOTE: 'Decryption' is sometimes referred to as 'decipherment'.

4.13 Domain master key (KM)—a key which is used to protect other key encrypting keys while held in secondary storage.

NOTE: The KM is the highest level and therefore the most important key at each node.

4.14 Dual control—a process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single person is able to access or utilize the materials, e.g. keys.

4.15 Encryption—the transformation of clear text into cipher text for the purpose of security or privacy.

NOTE: 'Encryption' is sometimes referred to as 'encipherment'.

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