Effective:
17 October 2025
Version 017

# AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

**A Company limited by Guarantee**

# Code Set

for

# ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

## Volume 4
## Device Requirements and Cryptographic Management

Commenced 1 July 2015



**Australian Payments Network Limited**
Telephone: (02) 9216 4888

**Code Set for**

**ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK**

**Volume 4**
**Device Requirements and Cryptographic Management**

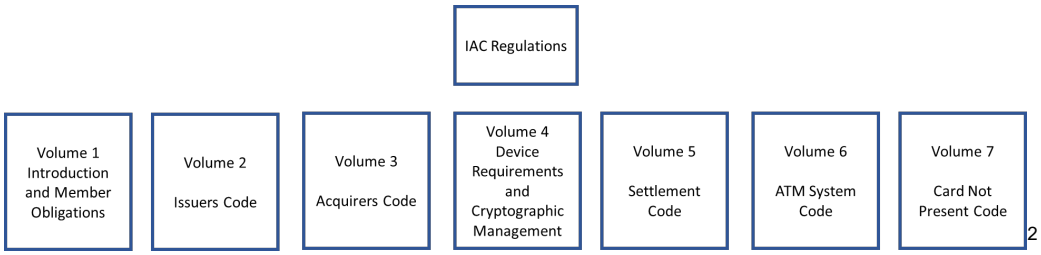
# INDEX

# PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

## 1.1 Purpose of this volume[1]

The IAC has been established to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. These include minimum security standards, interoperability standards and value added services that support how payment cards are used throughout Australia.

These standards and requirements are contained within the IAC Code Set which is structured as follows:



[2]

Volume 4 is intended to be read in conjunction with Volumes 1, 2 & 3.[3]

It is an IAC requirement that all Devices, Solutions and Non-Standard Technologies hold a current AusPayNet approval prior to and during use within the IAC.[4]

This volume is structured in four parts. Part 1 provides introductory material and details the definitions that are used throughout the IAC Code Set. Part 2 is no longer used. Part 3 addresses the process of approval for Devices, Solutions and Non-Standard Technologies. Cryptographic standards such as key length and approved algorithms are detailed in Part 4 including Terminal Key Management requirements.[5]

## 1.2 Interpretation[6]

Interpretations are located in a separate document entitled ‘Interpretation & Definitions'.

## 1.3 Definitions

Definitions are located in a separate document entitled ‘Interpretation & Definitions’.

**Next page is Part 2**

[1] Amended effective 1/1/19, version 008 r&p 002.18
[2] Amended effective 1/7/19, version 009 r&p 001.19
[3] Amended effective 16/12/21, version 013 r&p 001.21
[4] Last amended effective 16/12/21, version 013 r&p 001.21
[5] Last amended effective 17/10/25, version 017 r&p 001.25
[6] Amended effective 1/1/23, version 014 r&p 002.22

# PART 2 DEVICE SECURITY STANDARDS [DELETED][7]

**[Deleted]**

**Next page is Part 3**

[7] Deleted effective 16/12/21, version 013 r&p 001.21

# PART 3 DEVICE APPROVALS [8]

This Part 3 contains the IAC's requirements of the Company in relation to the approval of Devices, Solutions and Non-Standard Technologies for use in Interchange. Part 1.1 of this Volume 4 states the purpose of the IAC. In the context of Approved Devices that purpose includes balancing the interest of maintaining the security and integrity of Australian Card Payments with the interest of promoting innovation and competition.

## 3.1 Device Approval Process[9]

(a) The Company is responsible for:

(i) establishing the Device Approval Process;

(ii) reviewing and determining applications from Device Approval Applicants for approval of Non-Standard Technologies including determining any conditions to be attached to an approval and issuing Letters of Approval;[10]

(iii) revocation of any device approval, as contemplated in the Device Approval Process.[11]

(iv) amending the Device Approval Process; and

(v) publishing the Approved Devices List on the AusPayNet website.

(b) Each of the responsibilities of the Company specified in (a) may be exercised by the Company with the approval of the Chief Executive Officer, without the need to obtain approval of the IAF or any other person.

## 3.2 Approved Devices[12]

(a) The Device Approval Process sets out the process for approval of Devices for use in the IAC.

(b) Subject to the Device Approval Process, a Device is approved for use in the IAC if the Device is:

(i) listed as approved on the website of an Approved Standards Entity and complies with an Accepted Standard; or

(ii) listed in the AusPayNet-Approved Devices List published on the Company's website; or

[8] Last amended effective 16/12/21, version 013 r&p 001.21
[9] Last amended effective 16/12/21, version 013 r&p 001.21
[10] Amended effective 1/1/25, version 016 r&p 001.24
[11] Amended effective 1/1/25, version 016 r&p 001.24
[12] Inserted effective 1/1/25, version 016 r&p 001.24

(iii) approved for the use in a pilot under a Pilot Letter of Approval issued by the Company.

## 3.3 Period of permitted use of Approved Devices[13]

(a) The Device Approval Process determines the period of permitted use in the IAC of Approved Devices.

(b) Subject to the Device Approval Process, the period of permitted use in the IAC:

(i) for Devices listed as approved on the website of an Approved Standards Entity is:

(A) the Approval Period which expires on the expiry date for the Approved Device; and

(B) the Sunset Period which expires on the sunset date published in the schedule of sunset dates on the Company's website;

(ii) for Devices listed in the AusPayNet-Approved Devices List is:

(C) the Approval Period which expires on the expiry date for the Approved Device; and

(D) the Sunset Period which expires on the Device's sunset date published in the AusPayNet-Approved Devices List;

(iii) for Devices approved for use in a pilot the Approval Period which expires on the date stated in the Pilot Letter of Approval.

(c) During a Sunset Period only Devices purchased during the Approved Period can be used.

(d) The period of permitted use in the IAC may be revoked by the Company as provided in the Device Approval Process and if revoked will be published in the revocation section of the AusPayNet-Approved Devices List.

## 3.4 Approval of Devices [Deleted][14]

## 3.5 Approved Evaluation Facilities [Deleted][15]

## 3.6 Evaluation Costs [Deleted][16]

[13] Inserted effective 1/1/25, version 016 r&p 001.24
[14] Deleted effective 16/12/21, version 013 r&p 001.21
[15] Deleted effective 16/12/21, version 013 r&p 001.21
[16] Deleted effective 1/1/19, version 008 r&p 002.18

## 3.7 Agreements [Deleted][17]

## 3.8 Evaluation Facility Accreditation Process [Deleted][18]

**Next page is Part 4**

[17] Deleted effective 1/1/19, version 008 r&p 002.18
[18] Deleted effective 1/1/19, version 008 r&p 002.18

# PART 4 CRYPTOGRAPHIC STANDARDS AND KEY MANAGEMENT

## 4.1 Cryptographic Key Management – General

Unless specifically detailed elsewhere, the following key management practices must apply. All cryptographic key management practices must conform to ISO 11568 (where practicable) or AS 2805.6.1.[19]

## 4.2 Transport Keys [Deleted][20]

### 4.2.1 *Approved Encryption Algorithms for Transport Keys [Deleted]*[21]

### 4.2.2 *Minimum Key Length for Transport Keys [Deleted]*[22]

### 4.2.3 *Key Life Cycle Practices for Transport Keys [Deleted]*[23]

## 4.3 Domain Master Keys (DMK)

These keys are used within a financial institution to protect keys stored internal to the organisation.

### 4.3.1 *Minimum Key Length for Domain Master Keys*

Domain Master Keys must be DEA 3 or AES keys and must be equal or higher in strength than any keys being protected.[24]

## 4.4 IAC Interchange Cryptographic Keys[25]

### 4.4.1 *Introduction*

Interchange keys are used to protect financial Transactions initiated at Acquirer Terminals while in transit to the Issuer institution. Interchange keys may be either:

(a) PIN encrypting keys – used to protect the customer PIN from the point of origin to the point of authorisation. PIN encrypting keys are a specific instance of session keys;

(b) Message authentication keys – used to ensure message integrity. Message authentication keys are a specific instance of session keys;

(c) Data Protection Keys – used to provide confidentiality of messages. Data protection keys are a specific instance of session keys;

[19] Amended effective 17/10/25, version 017 r&p 001.25
[20] Deleted effective 17/10/25, version 017 r&p 001.25
[21] Deleted effective 17/10/25, version 017 r&p 001.25
[22] Deleted effective 17/10/25, version 017 r&p 001.25
[23] Deleted effective 17/10/25, version 017 r&p 001.25
[24] Amended effective 17/10/25, version 017 r&p 001.25
[25] Amended effective 1/1/20, version 010 r&p 002.19

(d) Session keys – used to secure, validate and protect the financial message. Session keys can be further qualified into those used in the Terminal to Acquirer environment (Terminal session keys) or on node to node links (interchange session keys);

(e) Key Encrypting Keys (KEK)– used to protect other keys (e.g., session keys) during encrypted key exchange; or[26]

(f) Transport Keys – used to protect keys (e.g., KEKs) during transport to the partner institution.

### 4.4.2 *Cryptographic Algorithms*[27]

(a) DEA 3, DEA 2, AES and ECC are the only approved algorithms for the protection of interchange information and keys in transport.[28]

(b) The following are the minimum acceptable requirements for the effective protection of interchange information:[29]

(i) DEA 3 with a key length of 128 bits or greater.[30]

(ii) DEA 2 with a key length of 2048 bits or greater.[31]

(iii) AES with a key length of 128, 192 or 256 bits.[32]

(iv) ECC with a key length of 256 bits or greater.[33]

(c) In accordance with ISO 9564-2, DEA3 or AES must be used for online PIN encipherment and DEA 2 must be used for offline PIN encipherment. Acquirers who do not comply with this requirement are responsible for any Issuer loss (direct or indirect) arising from the compromise of PIN data due to a breach of this requirement.[34]

### 4.4.3 *Key Management Practices for Transport Keys*[35]

(a) DEA 3 Transport Keys must be freshly generated to protect keys in transport and then securely destroyed after use.

(b) DEA 2 Transport Keys with key lengths of 2048 bits or greater, ECC Transport Keys with key lengths of 256 bits or greater and AES Transport Keys with key lengths of 128 bits or greater are deemed acceptable for a key change interval (lifetime) of two (2) years.

---

[26] Amended effective 17/10/25, version 017 r&p 001.25
[27] Amended effective 17/10/25, version 017 r&p 001.25
[28] Amended effective 17/10/25, version 017 r&p 001.25
[29] Amended effective 17/10/25, version 017 r&p 001.25
[30] Inserted effective 17/10/25, version 017 r&p 001.25
[31] Inserted effective 17/10/25, version 017 r&p 001.25
[32] Inserted effective 17/10/25, version 017 r&p 001.25
[33] Inserted effective 17/10/25, version 017 r&p 001.25
[34] Last amended effective 17/10/25, version 017 r&p 001.25
[35] Inserted effective 17/10/25, version 017 r&p 001.25

(c) DEA 2 Transport Keys of less than 2048 bits shall be treated as single use keys for transporting DEA 3 keys and their use is deprecated in all new implementations.

(d) DEA 2 key lengths of less than 1024-bits are unsuitable for general use. Preferred DEA 2 Transport Key lengths are equal to or greater than 2048 bits and should be used for transporting DEA 3 keys in all new implementations where hardware constraints do not exist.

## 4.5 IAC Interchange Links[36]

### 4.5.1 *IAC Interchange Security Requirements*[37]

For all IAC Interchange Links, Issuers and Acquirers must ensure that: [38]

(a) security for Transactions processed over that IAC Interchange Link complies with: AS 2805.6 series or ISO 11568;[39]

(b) security for Transactions from Terminal to Acquirer and from Acquirer to Issuer complies with: AS 2805.6 series or ISO 11568;[40]

(c) PIN security and encryption complies with ISO 9564and clause 4.8 of this IAC Code Set Volume 4;[41]

(d) Key management practices comply with ISO 11568 or AS 2805.6.1;[42]

(e) Message Authentication must apply to all IAC Interchange Links;[43]

(f) Message Authentication Code (MAC) must be calculated using DEA 3 or AES and a MAC algorithm conforming to ISO 16609; and[44]

(g) all interchange PIN and MAC cryptographic functions must be performed within an SCM that is an Approved Device.[45]

[36] Amended effective 1/1/20, version 010 r&p 002.19
[37] Amended effective 1/1/20, version 010 r&p 002.19
[38] Amended effective 1/1/20, version 010 r&p 002.19
[39] Last amended effective 17/10/25, version 017 r&p 001.25
[40] Amended effective 17/10/25, version 017 r&p 001.25
[41] Last amended effective 17/10/25, version 017 r&p 001.25
[42] Amended effective 17/10/25, version 017 r&p 001.25
[43] Amended effective 1/1/20, version 010 r&p 002.19
[44] Amended effective 17/10/25, version 017 r&p 001.25
[45] Amended effective 16/12/21, version 013 r&p 001.21

### 4.5.2 *Key Management Practices – IAC Interchange Links*[46]

***Clause 4.5.2 is Confidential***

## 4.6 KEK Establishment

### 4.6.1 *Introduction*[52]

(a) The security of Interchange is critically dependent on the secure installation of the Interchange Key Encrypting Keys. It is critically important that safe, sound and secure practices be adopted for the generation, handling, transport, storage and installation of Interchange Key Encrypting Keys.[53]

(b) The initial establishment of Interchange Key Encrypting Keys must employ one of the methods identified in this clause namely:[54]

[46] Amended effective 1/1/20, version 010 r&p 002.19
[53] Amended effective 17/10/25, version 017 r&p 001.25
[53] Amended effective 17/10/25, version 017 r&p 001.25
[54] Amended effective 17/10/25, version 017 r&p 001.25

(i) AS 2805.6.6 method;

(ii) Native RSA key method;

(iii) KTK method;

(iv) KEK Component method.

(v) Methods that conform to ISO 11568.[55]

### 4.6.2 *AS 2805.6.6 method*

(a) This Interchange key initialisation process employs an RSA key pair generated internally by the Security Control Module (SCM).

(b) With this method each SCM has a set of pre-generated RSA key pairs.

(c) The key exchange procedure is the following:

(i) partners exchange (via a secure channel[56]) their public RSA keys (IPK) and the associated verification codes;

(ii) each partner authenticates and installs the partner's IPK;

(iii) Key management proceeds in accordance with the requirements of AS 2805.6.6.

(d) Advantages

This method is the only mechanism providing for full automation of subsequent key changes and for that reason is preferred.

(e) Disadvantages

This method may require changes to the application if it is to be supported.

### 4.6.3 *Native RSA key method* [57]

(a) This Interchange key initialisation process employs a RSA key pair generated internally by the Security Control Module (SCM).

(b) With this method each SCM has a set of pre-generated RSA key pairs.

[55] Inserted effective 17/10/25, version 017 r&p 001.25

[56] In the absence of a secure email channel, authenticity of public keys should be achieved by some other means, for example by verifying the corresponding PVC-s through a different communication channel, such as telephone or facsimile

[57] Amended effective 17/10/25, version 017 r&p 001.25

(c) When generated on request, the Interchange Key Encrypting Key (KEKs) is signed by the native private key[58] and encrypted by the partner's public key. In this signed and encrypted format, the Interchange KEKs will be sent to the partner where it will be translated into the form required by the application (that is by encryption under the KM). For the receiving partner it will become KEK Receive.

(d) The key exchange procedure is the following:

(i) Partners exchange (via a secure channel[59]) their public RSA keys. This is a prerequisite to generate KEKs. The format of the data for the exchange of the public key uses three lines of text:

(A) the public key modulus;

(B) the public key exponent; and

(C) the public key verification code (PVC).

*Note that the ASCII hex presentation of data applies.*

(e) The PVC will be mutually confirmed over the telephone by the key exchange representatives:

(i) Each partner generates their KEK Send, that is cryptographically protected under RSA;

(ii) Each partner submits the protected KEK Send to the Interchange partner (typically by secure email). The format of the data for the exchange of the KEK uses three lines of text:

(A) the signed hash;

(B) the encrypted KEK; and

(C) the key verification code (KVC).

*Note that the ASCII hex presentation of data applies.*

(f) The KVC will be mutually confirmed over the telephone by the key exchange representatives.

(i) the received KEK becomes KEK Receive. KEK Receive is translated from encryption/signing under RSA(s) to encryption under KM for local key database storage;

[58] Actually the hash of the key is signed.

[59] In the absence of a secure email channel, authenticity of public keys should be achieved by some other means, for example by verifying the corresponding PVC-s through a different communication channel, such as telephone or facsimile.

(ii) both KEK Send and KEK Receive are stored in the required location in the key database; ensuring that the corresponding KEK KVC matches on both sides;

(iii) the interchange is started using the new Interchange KEK keys.

(g) Advantages

(i) This method does not require any specific update/integration on the application part. i.e., the use of RSA is completely transparent to the application and therefore all Interchange parties can exchange keys through this method without any proprietary changes to their native application (as long as they have the required functions in their SCM).

(ii) There is significant current experience with this method more so than with the other two random KEK methods - this method has proved to be very efficient and reliable in practice.

(h) Disadvantages

(i) The main operational disadvantage is the dependency upon a particular ("dedicated") security device. In a generic case there is no guarantee that the used RSA key pair, from a particular SCM device, has not changed since the last key exchange, e.g., if the device was reset or a new device installed. Therefore the interchange key (KEK) change process requires exchange of RSA keys every time. For this reason this method is currently implemented as an off-line process and as such it is not recommended for automation.

### 4.6.4 *KTK Method* [60]

(a) This method relies on a symmetric transport key that is provided to the SCMs of both Interchange partners and used to encrypt the Interchange KEKs. For key loading, KTK will typically be presented in multiple full length key components and each partner will contribute to its construction supplying at least one component.[61]

(b) When generated on request, the Interchange key (KEK Send) is encrypted under the KTK and submitted to the partner where it needs to be translated into the form required by the application (encryption under the KM). For the receiving partner it will become KEK Receive.

(c) The key exchange procedure is the following:

(i) each interchange partner generates at least one KTK component and submits it with its KVC in a pre-numbered tamper evident envelope through a secure courier to the corresponding Interchange partner for loading into an SCM;[62]

[60] Amended effective 17/10/25, version 017 r&p 001.25
[61] Amended effective 17/10/25, version 017 r&p 001.25
[62] Amended effective 17/10/25, version 017 r&p 001.25

(ii) the consignment number and serial number of the tamper evident envelope are communicated with the interchange partner separately via a different communication channel;[63]

(iii) consignment number and serial number of the tamper evident envelope are verified by each interchange partner upon receipt;[64]

(iv) KTK is loaded by each partner and their KVCs are verified;[65]

(v) each partner generates their KEK Send, that is cryptographically protected under KTK;

(vi) AES KEK Send must be protected in ISO 20038 key block using an AES KTK as the key block protection key;[66]

(vii) each partner submits the protected (encrypted) KEK Send to the partner (typically by secure email);

(viii) the received KEK becomes KEK Receive. KEK Receive is translated from encryption under KTK to encryption under KM for local key database storage;

(ix) both KEK Send and KEK Receive are stored in the required location in the key database; ensuring that the corresponding KVC matches on both sides;

(x) the interchange is re-started using the new Interchange keys.

(d) Advantages

For parties that cannot support RSA keys either functionally or by security policy, this is a simple reliable 'traditional' approach. Its impact to the application design is the same as for the RSA native method, i.e., either method may be used transparently to the application as long as the SCM interface utility supports the corresponding SCM calls.

(e) Disadvantages

The clear KTK components must be securely exchanged between the partners and also loaded into the SCMs through a 'secure key entry process'. They also must be securely stored e.g., in a safe. All these operational support requirements increase the operational cost of this method and security risks (of staff collusion, negligence, etc.).

[63] Inserted effective 17/10/25, version 017 r&p 001.25
[64] Inserted effective 17/10/25, version 017 r&p 001.25
[65] Amended effective 17/10/25, version 017 r&p 001.25
[66] Inserted effective 17/10/25, version 017 r&p 001.25

### 4.6.5 *KEK Component Method*[67]

(a) This method is a 'traditional' method of the interchange key initialisation and as such is supported by older Security Control Module designs. It is still maintained by many interchange partners and in particular by many smaller organizations.

(b) This method does not involve use of initial keys such as RSA or KTK but is based on manual key management processes of DEA 3 or AES interchange KEKs in conjunction with the use of SCM devices. The interchange KEKs in this method are generated externally and are loaded into the device in components using SCM devices. The key material requires a secure key generation, conveyancing, loading and storage procedures of the key components.[68]

(c) This method is included for 'backward compatibility' and for a fall-back situation.

(d) The key exchange procedure is the following:

(i) the partners generate each interchange KEK in at least two full length key (XOR) components and exchange the key components along with their corresponding KVCs using a minimum of two separate secure channels;[69]

(ii) the keys components are loaded into the SCM device under dual control and all KVCs are verified ; the keys may also be encrypted under the DMK for storage in the key data base;[70]

(iii) the key component materials may be stored in secure storage (e.g., safes under dual control) until after the interchange KEKs have been confirmed fully operational;[71]

(iv) afterwards, the KEKs are ready for use.

(e) Advantages

This method is still in wide spread use across the industry. For this reason and because of its manual handling nature, it is a good fallback solution.

[67] Amended effective 17/10/25, version 017 r&p 001.25
[68] Amended effective 17/10/25, version 017 r&p 001.25
[69] Amended effective 17/10/25, version 017 r&p 001.25
[70] Amended effective 17/10/25, version 017 r&p 001.25
[71] Amended effective 17/10/25, version 017 r&p 001.25

(f) Disadvantages

The extensive use of manual procedures renders subsequent key changes, as are required under IAC Rules more difficult than some of the other methods.

### 4.6.6 *Methods that conform to ISO 11568*[72]

(a) This option allows any other methods that conform to ISO 11568 to establish AES or DEA 3 Interchange KEKs between Interchange partners.

(b) In accordance with ISO 11568, if a Transport Key is used to protect Interchange KEKs in transit, the Transport Key must be equal to or greater strength than the Interchange KEK.

(c) ECC is the preferred algorithm for protecting AES Interchange KEKs in transit.

## 4.7 IAC Interchange Lines[73]

IAC Interchange Lines must be subject to whole-of-message encryption, excluding communications headers, using DEA 3 or AES key.[74]

### 4.7.1 *IAC Interchange Line Cryptographic Management*[75]

(a) Where IAC Interchange Links are transported through the COIN, these IAC Interchange Line Cryptographic Management Practices do not apply.[76]

(b) The use of transport level data encryption (e.g., IPSec) is permitted subject to the following conditions:[77]

(i) data encryption must use either DEA 3 or AES;[78]

(ii) the data stream must be fully encrypted with the exception of communication headers;

(iii) where IPSec is used, the system must be configured to use Encapsulating Security Payload, and authentication must be HMAC-SHA-256;[79]

(iv) either certificates or encrypted pre-shared secrets must be used (plain text shared secrets are not acceptable);[80]

[72] Inserted effective 17/10/25, version 017 r&p 001.25
[73] Amended effective 1/1/20, version 010 r&p 002.19
[74] Amended effective 17/10/25, version 017 r&p 001.25
[75] Amended effective 1/1/21, version 012 r&p 002.20
[76] Inserted effective 17/10/25, version 017 r&p 001.25
[77] Amended effective 17/10/25, version 017 r&p 001.25
[78] Amended effective 17/10/25, version 017 r&p 001.25
[79] Amended effective 17/10/25, version 017 r&p 001.25
[80] Amended effective 17/10/25, version 017 r&p 001.25

(v) tunnel termination points must be within the IA Participant's or their trusted agent's facilities;

(vi) the facility must be supported by documented device management procedures with identified roles and responsibilities and subject to internal audit as prescribed by the IA Participant's security policy;

(vii) ownership and control of end-points must reside with the terminating IA Participant or their Third Party Provider;[81]

(viii) split tunnelling is not to be used; and

(ix) the minimum Diffie-Hellman group size is 2048-bits for MODP and 256 bits for ECP;[82]

(x) Internet Key Exchange, if used, must be configured to only use main mode.

(xi) Specifically, aggressive mode must NOT be used. Where encrypted shared-secrets are used, key management, including the process of key (secret) entry must ensure that no one person must have the capability to access or ascertain any plain text secret or private key.[83]

### 4.7.2 *Key Management Practices for IAC Interchange Lines* [84]

***Clause 4.7.2 is Confidential***

[81] Amended effective 17/10/25, version 017 r&p 001.25
[82] Amended effective 17/10/25, version 017 r&p 001.25
[83] Amended effective 17/10/25, version 017 r&p 001.25
[84] Amended effective 1/1/20, version 010 r&p 002.19

## 4.8 Terminal Key Management

### 4.8.1 *Terminal key management requirements*

For all Terminal to Acquirer Links, Acquirers must ensure that:

(a) Security for Transactions from Terminal to Acquirer complies with: ISO 11568 or AS 2805.6 series;[87]

(b) PIN security and encryption complies with ISO 9564;[88]

(c) Subject to clause 4.8.2(c), key management practices comply with ISO 11568 or AS 2805.6.1;[89]

(d) Message Authentication must apply to all Acquirer Links for all financial and key management messages;[90]

(e) the Message Authentication Code (MAC) must be calculated using a DEA 3 , or an AES key; and[91]

(f) an algorithm conforming to ISO 9797-1 or ISO/IEC 19772;[92]

(g) all PIN cryptographic functions must be performed within an Approved Device;[93]

(h) an Approved Device must be used for one or both of the following cryptographic operations:[94]

(i) MAC generation and verification functions; or

(ii) Encryption and decryption functionality used for privacy of communications;

(i) where MAC cryptographic functions are not performed in an Approved Device, the system components generating or verifying MACs and associated keys shall be considered part of the host system and assessed against the requirements from IAC Code Set Volume 3, clause 3.5;[95]

(j) Message Authentication Codes shall be used to protect all payment-related messages passing through all communication links between a terminal and the host system driving the terminals; and[96]

[87] Amended effective 17/10/25, version 017 r&p 001.25
[88] Amended effective 17/10/25, version 017 r&p 001.25
[89] Amended effective 17/10/25, version 017 r&p 001.25
[90] Amended effective 1/1/19, version 008 r&p 002.18
[91] Last amended effective 17/10/25, version 017 r&p 001.25
[92] Inserted effective 1/1/25, version 016 r&p 001.24
[93] Last amended effective 1/1/25, version 016 r&p 001.24
[94] Amended effective 17/10/25, version 017 r&p 001.25
[95] Inserted effective 1/1/25, version 016 r&p 001.24
[96] Inserted effective 1/1/25, version 016 r&p 001.24

(k) for EFTPOS Terminals privacy of communication complies with AS 2805.9 or any other privacy of communication standard approved by the Management Committee.

### 4.8.2 *Key Management Practices*

***Clause 4.8.2 is Confidential***

### 4.8.3 *Key Rolling Process for Session Keys*

DEA 3 Session Key roll over should occur without operator intervention and in a manner compliant with AS 2805.6.2, AS 2805.6.4 or other AusPayNet approved, Terminal key management protocol.[104]

**Next page is Annexure A**

[104] Amended effective 17/10/25, version 017 r&p 001.25

# ANNEXURE A. MINIMUM EVALUATION CRITERIA FOR IP ENABLED TERMINALS [DELETED][105]

**[Deleted]**

**Next page is Annexure B**

[105] Deleted effective16/12/21, version 013 r&p 001.21

# ANNEXURE B. PCI PLUS REQUIREMENTS [DELETED][106]

**[Deleted]**

**Next page is Annexure C**

[106] Deleted effective16/12/21, version 013 r&p 001.21

# ANNEXURE C. DEVICE EVALUATION FAQ [DELETED][107]

**[Deleted]**

**Next page is Annexure D**

[107] Deleted effective16/12/21, version 013 r&p 001.21

# ANNEXURE D. DEVICE APPROVAL PROCESS [DELETED][108]

**[Deleted]**

**Next page is Annexure E**

[108] Deleted effective16/12/21, version 013 r&p 001.21

# ANNEXURE E. IAC LABORATORY ACCREDITATION CHECKLIST [DELETED][109]

**[Deleted]**

**The next page is Annexure F**

[109] Deleted effective16/12/21, version 013 r&p 001.21.

# ANNEXURE F. INTRODUCTION TO DEVICE SUPPORT AND SCM FUNCTIONALITY [DELETED][110]

**[Deleted]**

**The next page is Annexure G**

[110] Deleted effective 17/10/25, version 017 r&p 001.25

# ANNEXURE G. DEVICE APPROVAL PROCESS [DELETED][111]

**[Deleted]**

**END**

[111] Deleted effective 16/12/21, version 013 r&p 001.21