# 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

**Code Set for**

**ISSUERS AND ACQUIRERS COMMUNITY
FRAMEWORK**

**Volume 4
Device Requirements and Cryptographic Management**

**INDEX**

**Australian Payments Network Limited [ABN 12 055 136 519]**

**Australian Payments Network Limited [ABN 12 055 136 519]**

## PART 1   INTRODUCTION, INTERPRETATION AND DEFINITIONS

### 1.1   Purpose of this volume

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:
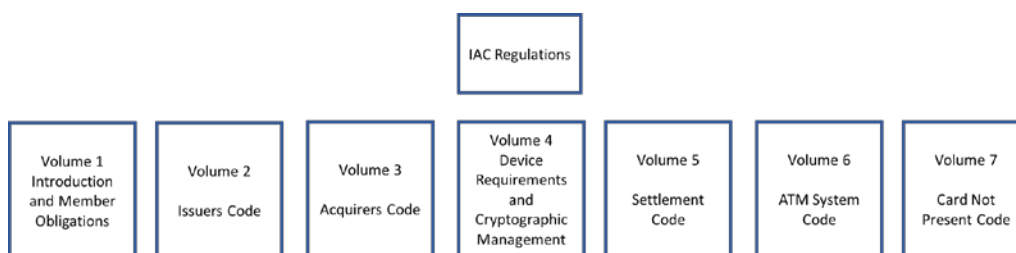
Volume 4 is intended to be read in conjunction with Volumes 1, 2 & 3 with this volume specifying the security requirements applicable to Terminals, Security Control Modules and Key Injection and Loading devices that apply to all Secure Cryptographic Devices suitable for use under the IAC.

It is an IAC requirement that all Secure Cryptographic Devices, all Software-based PIN entry on COTS (SPoC) solutions, all Contactless Payments on COTS (CPoC) Solutions and all other standard and non-standard solutions and POI Technology hold a current AusPayNet approval prior to and during use within the IAC.

This volume is structured in four parts.  Part 1 provides introductory material and details the definitions that are used throughout the IAC Manual.  Device security and SPoC Solution and CPoC Solution requirements are contained in Part 2 with Part 3 addressing device, SPoC Solution, CPoC Solution and other standard and Non-standard POI Technology approvals.  Cryptographic standards such as key length and approved algorithms are detailed in Part 4 including Terminal Key Management requirements.

### 1.2   Interpretation

In this IAC Code Set:

(a)   words importing any one gender include the other gender;

(b)   the word 'person' includes a firm, body corporate, an unincorporated association or an authority;

(c)     the singular includes the plural and vice versa;

(d)     unless the contrary intention appears, a reference to a clause, part or annexure is a reference to a clause, part or annexure of the volume of the IAC Code Set in which the reference appears;

(e)     a reference to a statute, code or the Corporations Law (or to a provision of a statute, code or the Corporations Law) means the statute, the code, the Corporations Law or the provisions as modified or amended and in operation for the time being, or any statute, code or provision enacted in lieu thereof and includes any regulation or rule for the time being in force under the statute, the code, the Corporations Law or the provision;

(f)     a reference to a specific time means that time in Sydney unless the context requires otherwise;

(g)     words defined in the Corporations Law have, unless the contrary intention appears, the same meaning in this IAC Code Set;

(h)     words defined in the Regulations have, unless the contrary intention appears, the same meaning in this IAC Code Set;

(i)     this IAC Code Set has been determined by the Management Committee and takes effect on the date specified by the Chief Executive Officer pursuant to Regulation 1.2; and

(j)     headings are inserted for convenience and do not affect the interpretation of this IAC Code Set.

## 1.3     Definitions

In this IAC Code Set the following words have the following meanings unless the contrary intention appears.

"**Acquirer**" is defined in the IAC Regulations and means a Constitutional Corporation that in connection with a Transaction:

Amended effective 1.1.20

(a)     under arrangement with and on behalf of an Issuer, discharges the obligations owed by that Issuer to the relevant Cardholder; and

(b)     engages in Interchange Activity with that Issuer as a result.

"**Acquirer Identification Number**" and "**AIN**" The six-digit number assigned by ISO to identify an acquiring Framework Participant (see also IIN, BIN).

"**Acquirer Reference Number**" [Deleted]

Deleted effective 20.8.18

"**AID**" means Application ID present in an ICC chip card.

Inserted effective 21.11.17

"**Approved Cardholder**" means:

Inserted effective 1.1.16

(a) a customer of an Issuer (or third party represented by an IA Participant) who has been issued with a Card and a PIN by that IA Participant or by a third party represented by the IA Participant; or

(b) any person who operates an account or has access to an account held with an IA Participant (or third party represented by an IA Participant) who has been issued with a Card and PIN by the IA Participant (or third party represented by an IA Participant).

"**Approved Card Payment System**" is defined in the IAC Regulations and means a Card Payment System which:

Amended effective 1.1.20

(a) is, or is eligible to be, a Recognised APS; and

(b) is determined by the IAF to satisfy the Approval Criteria for Approved Card Payment Systems.

"**Approved CPoC Solution**" means a CPoC Solution that has been evaluated in accordance with Annexure G of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use within IAC.  All such CPoC Solutions must have been approved by PCISSC prior to evaluation by AusPayNet.

Inserted effective 1.7.20

"**Approved Device**" means a Secure Cryptographic Device that has been evaluated in accordance with clause 3.1 of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) which has been approved for use within IAC.

Amended effective 1.1.16

"**Approved Evaluation Facility**" and "**AEF**" means a testing laboratory that has been accredited by the Company to conduct SCD security compliance testing and is listed on the Company's website as an Approved Evaluation Facility.

Amended effective 1.1.19

"**Approved Non-standard POI Technology**" means a Non-standard POI Technology that has been evaluated in accordance with Annexure G of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use within IAC.

Inserted effective 1.1.20

"**Approved SPoC Solution**" means a SPoC solution that has been evaluated in accordance with Annexure G of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use within IAC.  All such SPoC solutions must have been approved by PCISSC prior to evaluation by AusPayNet.

Inserted effective 1.1.19

"**AS**" means Australian Standard as published by Standards Australia.

"**ATM**" or "**ATM Terminal**" means an approved electronic device capable of automatically dispensing Cash in response to a Cash withdrawal Transaction initiated by a Cardholder.  Other Transactions (initiated by a Card) such as funds transfers, deposits and balance enquiries may also be supported.  The device must accept either magnetic stripe Cards or smart (chip) Cards where Transactions are initiated by the Cardholder keying in a Personal Identification Number (PIN).  Limited service devices (known as "Cash dispensers") that only allow for Cash withdrawal are included.

*Amended effective 1.1.16*

"**ATM Access Regime**" means the access regime imposed by the Reserve Bank of Australia under section 12 of the *Payment Systems (Regulation) Act 1998* by regulatory instrument dated 23 February 2009.

*Inserted effective 1.1.16*

"**ATM Affiliate**" means an Affiliate which has subscribed to IAC Code Set Volume 6 (ATM System Code).

*Last amended effective 1.1.20*

"**ATM Code Committee**" means the committee established by the IAF pursuant to Part 11 of the IAC Regulations.

*Inserted effective 1.1.16*

"**ATM Direct Charging Date**" means 3 March 2009.

"**ATM Framework Participant**" means a Constitutional Corporation which pursuant to the IAC Regulations, is a Framework Participant in the IAC, and is a subscriber to IAC Code Set Volume 6 (ATM System Code) pursuant to Part 2, clause 2.2 of Volume 6  and includes, for the avoidance of doubt, each:

*Last amended effective 1.1.20*

(a)     IA Participant;

(b)     ATM Operator Member; and

(c)     ATM Affiliate.

"**ATM Interchange**" is defined in the IAC Regulations and means the exchange of payment instructions for value between Acquirers (whether for itself or on behalf of a third party) and Issuers, via an Interchange Link, as a result of the use of an Issuer's Card by a Cardholder to generate an ATM Transaction. Interchange arrangements may, but need not, be reciprocal.

*Last amended effective 1.1.20*

"**ATM Law**" means a law of the Commonwealth or of any State or Territory in relation to the operation of ATM Terminals.

*Inserted effective 1.1.16*

"**ATM Operator Fee**" means a fee paid by a Cardholder to the operator of an ATM to effect a Transaction through their Terminal.

"**ATM Operator Member**" means an Operator Member which has subscribed to IAC Code Set Volume 6 (ATM System Code).

*Last amended effective 1.1.20*

"**ATM System**" is defined in the IAC Regulations and means the network of direct and indirect Interchange Lines, Interchange Links, associated hardware, software and operational procedures that facilitate the transmission, authorisation and reconciliation of ATM Transactions between IA Participants in Australia.

"**ATM Transaction**" is defined in the IAC Regulations and means, for the purposes of this IAC Code Set, a Cash deposit, a Cash withdrawal, or a balance enquiry effected by a Cardholder at an ATM.

"**ATM Transaction Listing**" means a listing which complies with the requirements of Part 4, clause 11 of the IAC Code Set Volume 6 (ATM System Code).

"**AusPayNet**" is defined in the IAC Regulations and means Australian Payments Network Limited (ABN 12 055 136 519).

"**Australian IC Card**" means an IC Card in respect of which the EMV Issuer Country Code data element (tag 5F28) equal to "036" (Australia).

"**Authentication**" [Deleted]

"**Authorisation**" in relation to a Transaction, means confirmation given by an Issuer that funds will be made available for the benefit of an Acquirer, in accordance with the terms of the relevant Interchange Agreement, to the amount of that Transaction. Except in the circumstances specified in this IAC Code Set, Authorisation is effected online. 'Authorised' has a corresponding meaning.

"**Bank Identification Number**" and "**BIN**" means the registered identification number allocated by Standards Australia Limited in accordance with AS 3523 (also known as an Issuer Identification Number (IIN)).

"**Business Day**" means a day on which banks are open for general banking business in Sydney or Melbourne and on which the RITS is operating to process payments.

"**Card**" is defined in the IAC Regulations and means any card, device, application or identifier authorised by an Issuer, which is linked to an account or credit facility with the Issuer, for the purpose of effecting a Card Payment.

"**Cardholder**" is defined in the IAC Regulations and means a customer of an Issuer who is issued with a Card and PIN or other authentication method or process.

"**Cardholder Data**" means any information that is stored on, or which appears on, a Card, and includes but it not necessarily limited to:

(a)    Primary Account Number;

(b)    Cardholder Name;

(c)     Service Framework; and

(d)     Expiration Date.

"**Card Payment**" is defined in the IAC Regulations and means a Transaction under the rules of an Approved Card Payment System which is initiated by a Cardholder using a Card in Australia, irrespective of the infrastructure or network, including as the context requires, ATM Transactions, EFTPOS Transactions, Card-Not-Present Transactions and any adjustments in connection with those Transactions.

"**Card Payment System**" is defined in the IAC Regulations and means, for the purposes of the IAC, the set of functions, procedures, arrangements, rules and devices that enable a Cardholder to effect a Card Payment with a third party other than the Card Issuer. For the avoidance of doubt, a Card Payment System may be a three-party scheme or a four-party scheme.

"**Card Security Code**" and "**CSC**" is a 3 or 4 digit number:

(a)     embossed or printed on a payment card (often referred to as CVC2);

(b)     encoded in the Track Two Equivalent Data of the magnetic stripe for card present transactions (often referred to as CVC1); or

(c)     encoded in the Track Two Equivalent Data of the magnetic stripe equivalent for contactless and chip cards (often referred to as iCVV or Dynamic CVV).

Alternative terminology for CSC includes "CAV", "CVC", "CVD", "CVN", "CVV" and "SPC".

"**Cash**" is defined in the IAC Regulations and means Australian legal tender.

"**Certification**" is defined in the IAC Regulations and means in relation to an IA Participant initial certification or re-certification, in either case to the extent required by and in accordance with, Regulation 5.1(b) and f the IAC Code Set.

"**Certification Checklist**" means in relation to an Acquirer, a checklist in the form of Annexure B.1 in IAC Code Set Volume 1 (Introduction and Member Obligations) and in relation to an Issuer, a checklist in the form of Annexure B.2 in IAC Code Set Volume 1 (Introduction and Member Obligations).

"**Certification Undertakings**" means all undertakings and representations given to the Company for the purposes of obtaining Certification.

"**Clearing/Settlement Agent**" means a Direct Clearer/Settler that clears and settles on behalf of Issuers and/or Acquirers which are not Direct Clearer/Settlers.

"**Clearing System**" is defined in the IAC Regulations and means a domestic payments clearing and settlement system established in accordance with the Constitution which is operated by, or under the auspices of, the Company.

<div align="right">Amended effective 1.1.20</div>

"**Closed Loop Cards**" means electronic payment cards that are restricted in terms of where they can be used at the time of purchase.

<div align="right">Inserted effective 1.1.20</div>

"**CNP Transaction**" means a transaction which is initiated by a Cardholder using a Card to make a purchase from a Merchant not in the same physical location. For example, over the internet (including via a mobile browser) or in an application.

<div align="right">Inserted effective 1.07.19</div>

"**Code**" and "**IAC Code**" is defined in the IAC Regulations and means:

<div align="right">Amended effective 1.1.20</div>

(a)     Volume 1 of the IAC Code Set (Introduction and Member Obligations);

(b)     Volume 2 of the IAC Code Set (Issuers Code);

(c)     Volume 3 of the IAC Code Set (Acquirers Code);

(d)     Volume 4 of the IAC Code Set (Device Requirements and Cryptographic Management);

(e)     Volume 5 of the IAC Code Set (Settlement Code);

(f)     Volume 6 of the IAC Code Set (ATM System Code);

(g)     Volume 7 of the IAC Code Set (Card Not Present Code); and

(h)     any other set of threshold industry standards or requirements for Card Payments which the IAF may adopt as industry standards or requirements for the purposes of these Regulations, from time to time.

"**Commencement Date**" is defined in the IAC Regulations and means, subject to IAC Regulation 1.6(b), 1 July 2015.

<div align="right">Amended effective 1.1.20</div>

"**Committee of Management**" means the IAF.

<div align="right">Amended effective 1.1.20</div>

"**Commercial off-the-shelf**" and "**COTS**" means a product that is designed for mass-market distribution and can be bought by any civilian entity, i.e. an unrestricted product not solely used by the military.

<div align="right">Inserted effective 1.1.19</div>

"**Company**" means AusPayNet.

"**Compliance Date**" means 31 December 2016.

"**Compromised Terminal**" means a Terminal that has been tampered with for fraudulent purposes.

"**Constitution**" is defined in the IAC Regulations and means the constitution of AusPayNet as amended from time to time.

<div align="right">Amended effective 1.1.20</div>

"**Contactless Payment on COTS**" and "**CPoC**" means the term Contactless Payment on COTS as used in the PCISSC CPoC standards.

<div align="right">Inserted effective 1.7.20</div>

"**Corporations Law**" means the Corporations Act 2001 (Cth) and associated subordinate legislation as amended from time to time.

"**Counterfeit ATM Transaction**" means a fraudulent ATM Transaction initiated with a counterfeit copy of a chip Card.

"**Counterfeit ATM Transaction Chargeback Date**" [Deleted]

<div align="right">Deleted effective 3.7.17</div>

"**Counterfeit ATM Transaction Claim**" means a claim by an Issuer under the indemnity in clause 4.5(c) (Liability Shift for Counterfeit ATM Transaction), made in the manner set out in clause 4.6 (Liability Shift Claim Process) of the IAC Code Set Volume 6 (ATM System Code).

<div align="right">Amended effective 3.7.17</div>

"**Counterparty**" means the IA Participant direct settler (for example, an Issuer) identified in a File Settlement Instruction submitted by an Originator (for example, an Acquirer or Lead Institution), in accordance with this IAC Code Set and the requirements of the RITS Low Value Settlement Service.

"**Credit Items**" is defined in the IAC Regulations to include all credit payment instructions, usually electronically transmitted, which give rise to Interchange Activity, except as may be specifically excluded by the IAC Regulations or the IAC Code Set.

<div align="right">Amended effective 1.1.20</div>

"**CVC**" and "**Card Verification Code**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**CVC1**" and "**Card Verification Code1**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**CVD**" and "**Card Verification Data**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**CVM**" means Cardholder Verification Method.

<div align="right">Inserted effective 20.8.18</div>

"**CVN**" and "**Card Verification Number**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**CVV**" and "**Card Verification Value**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**CVV2**" and "**Card Verification Value2**": see "**Card Security Code**".

<div align="right">Inserted effective 1.7.20</div>

"**Debit Chip Application**" means domestically issued debit chip application.

"**Debit Items**" is defined in the IAC Regulations to include all debit payment instructions, usually electronically transmitted, which give rise to Interchange Activity, except as may be specifically excluded by the IAC Regulations or the IAC Code Set.

<div align="right">Amended effective 1.1.20</div>

---

"**Device Approval Applicant**" means:

<div style="float:right"><small>Last amended effective 1.7.20</small></div>

(a)    in relation to standard technologies (including SPoC solutions and CPoC Solutions), the Sponsor, Acquirer, Third Party provider, device manufacturer or any third party who submits a device approval application; or

(b)    in relation to non-standard technologies, the Acquirer;

seeking approval of that device, solution or non-standard technology in accordance with Part 3 of IAC Code Set Volume 4.

"**Device Approval Process**" means the Device Approval Process for standard technologies and non-standard technologies published by AusPayNet, as updated from time to time, and a copy of which appears at Annexure G of IAC Code Set Volume 4.

<small>Last amended effective 1.1.20</small>

"**Direct Charge**" means a direct charge applied by an IA Participant under the Direct Charging Rules in Annexure F of IAC Code Set Volume 6 (ATM System Code).

<small>Inserted effective 1.1.16</small>

"**Direct Clearing/Settlement Arrangements**" means an arrangement between two indirectly connected IA Participants for the purposes of clearing and settlement with each other as Direct Clearer/Settlers.

<small>Inserted effective 1.1.16</small>

"**Direct Connection**" means a direct communications link between two IA Participants for the purposes of:

<small>Inserted effective 1.1.16</small>

(a)    exchanging ATM Transaction messages in respect of their own activities as an Issuer or as an Acquirer; and/or

(b)    exchanging ATM Transaction messages on behalf of other Issuers or Acquirers.

"**Direct Settler**" or "**Direct Clearer/Settler**" means:

<small>Inserted effective 1.1.16</small>

(a)    an Acquirer that is an IA Participant that:

(i)    clears Items directly; and

(ii)    settles directly, using its own ESA or using a means approved by the Management Committee,

with an Issuer, or with a representative of an Issuer appointed to settle on behalf of that Issuer for the value of payment obligations arising from Interchange Activities between it and that Issuer;

(b)    an Issuer that is an IA Participant that:

(i)    clears Items directly; and

(ii)    settles directly, using its own ESA,

with an Acquirer, or with a representative of an Acquirer appointed to settle on behalf of that Acquirer for the value of payment obligations arising from Interchange Activities between it and that Acquirer; or

(c)    a body corporate of the kind referred to in Volume 4 of the IAC Regulations, which represents one or more Acquirers or Issuers and, in such capacity, settles directly in accordance with Regulation 11.3(a) for the value of payment obligations arising from the Interchange Activities of those Acquirers or Issuers.

"**Disputed Transaction**" means an ATM Transaction:    <span style="float:right">Amended effective 1.1.16</span>

(a)    which the Cardholder denies having initiated; or    <span style="float:right">Inserted effective 1.1.16</span>

(b)    where the ATM Transaction amount is claimed to be incorrect; or    <span style="float:right">Inserted effective 1.1.16</span>

(c)    in respect of which the ATM Operator Fee is claimed to be incorrect.    <span style="float:right">Inserted effective 1.1.16</span>

"**Disruptive Event**" means any processing, communications or other failure of a technical nature, which affects, or may affect, the ability of any IA Participant to engage in Interchange Activity.

"**Double-length Key**" means a key of length 128 bits including parity bits or 112 bits excluding parity bits.

"**Doubtful ATM Transactions**" means those ATM Transactions which appear to have been successfully completed, although the ATM Transaction may not be recorded against the relevant Cardholder account.    <span style="float:right">Last amended effective 21.11.16</span>

"**EFT**" means Electronic Funds Transfer.

"**EFTPOS**" means Electronic Funds Transfer at Point of Sale.

"**EFTPOS PED**" [Deleted]    <span style="float:right">Deleted effective 20.8.18</span>

"**EFTPOS Terminal**" means a Terminal for processing EFTPOS Transactions.    <span style="float:right">Inserted effective 1.1.19</span>

"**EFTPOS Transaction**" is defined in the IAC Regulations and means a Transaction conducted at a Merchant's point of sale using a Terminal.    <span style="float:right">Last amended effective 1.1.20</span>

"**EMV**" means the specifications as published by EMV Co. LLC.

"**EMV@ATM Terminal Standards**" means the standards and requirements set out in IAC Code Set Volume 6 (ATM System Code) Annexure G.    <span style="float:right">Amended effective 1.1.20</span>

"**EMV Compliant**" in relation to an ATM Terminal means the ATM Terminal is certified by an Approved Evaluation Facility to be compliant with the EMV@ATM Terminal Standards.

---

"**EMV Phase 1**" means the transition arrangements through which a Transaction is created from the use of an EMV compliant Australian IC Card prior to the migration of the ATM system to full EMV functionality.

"**EMV Standards**" means:

(a)     in relation to Cards, the standards applicable to the Debit Chip Application loaded on the Card; and

(b)     in relation to ATM Terminals, means the standards set out in the IAC Code Set Volume 6 (ATM System Code) Annexure G EMV@ATM Terminal Standards.

"**Encapsulating Security Payload**" and "**ESP**" is a member of the IPsec protocol suite providing origin authenticity, integrity, and confidentiality protection of packets in tunnel mode, where the entire original IP packet is encapsulated, with a new packet header added which remains unprotected.

"**Encrypting PIN Pad**" and "**EPP**" means an approved device which is a component of a Terminal that provides secure PIN entry and cryptographic services to that Terminal.

"**ePayments Code**" means the code of conduct administered by the Australian Securities and Investments Commission.

"**Error of Magnitude**" means an error (or a series of errors) of or exceeding $2 million or such other amount as may be determined from time to time by the Committee of Management.

"**Evaluation Facility**" [Deleted]

"**Evaluation Report**" means a report prepared by:

(a)     an Approved Evaluation Facility; or

(b)     a laboratory authorised by the Company for the purpose of a non-standard technology;

under the Device Approval Process.

"**Exchange Settlement Account**" and "**ESA**" means an exchange settlement account, or similar account, maintained by a Framework Participant with the RBA used for, among other things, effecting settlement of inter-institutional payment obligations.

"**Fallback Transaction**" means an ATM Transaction initiated using a chip Card, which is processed and authorized by the Issuer using magnetic stripe data, in the circumstances described in IAC Code Set Volume 6 (ATM System Code) Annexure G.5.1.

"**File Recall Instruction**" means a file in the format prescribed by the Reserve Bank of Australia and complying with the specifications for the RITS Low Value Settlement Service which can be accessed via a link on the Company's extranet.

"**File Recall Response**" means a response to a File Recall Instruction, generated by the RITS Low Value Settlement Service.

"**File Settlement Advice**" means an advice in relation to a File Settlement Instruction, generated by the RITS Low Value Settlement Service.

"**File Settlement Instruction**" means a file in the format prescribed by the Reserve Bank and complying with the specifications for the RITS Low Value Settlement Service which can be accessed via a link on the Company's extranet.

"**File Settlement Response**" means a response to a File Settlement Instruction, generated by the RITS Low Value Settlement Service.

"**Framework Participant**" is defined in the IAC Regulations and means a Constitutional Corporation: <span style="float:right">Amended effective 1.1.20</span>

(a)    which is deemed to be a Framework Participant pursuant to Regulation 4.4; or

(b)    whose Membership Application has been accepted pursuant to Regulation 4.3(f); and

in each case whose membership has not been terminated pursuant to Regulation 6.5.

"**Fraudulent CNP Transaction**" means a CNP Transaction which is also a Fraudulent Transaction. <span style="float:right">Inserted effective 1.07.19</span>

"**Fraudulent Transaction**" means a Transaction reported to an international card scheme as fraudulent which: <span style="float:right">Inserted effective 1.07.19</span>

(a)    includes but is not limited to unauthorised payment transactions and authorised payers acting dishonestly;

(b)    but excludes Transactions with Cards that were originally established using stolen or false identity information.

"**HMAC**" and "**Hash-based Message Authentication Code**" is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. HMACs are formed in conformance with AS2805.4.2 Electronic funds transfer—Requirements for interfaces Information technology -- Security techniques -- Message Authentication Codes (MACs) - Mechanisms using a dedicated hash-function.

"**Hot Card**" means a Card which has been reported by the Cardholder as lost or stolen, or for which there is evidence of fraudulent use.

"**IA Participant**" is defined in the IAC Regulations and means a Framework Participant which is either:

Amended effective 1.1.20

(a)    an Issuer; or

(b)    an Acquirer; or

(c)    a body corporate which represents one or more Issuers or Acquirers and, in such capacity, settles directly in accordance with Regulation 11.3(a)(ii) for the value of the payment obligations arising from the Interchange Activities of those Acquirers or Issuers.

"**IAC**" is defined in the IAC Regulations and means the Issuers and Acquirers Community constituted by the IAC Regulations.

Amended effective 1.1.20

"**IAC Card Standards**" means the standards for Cards set out in the IAC Code Set Volume 2 (Issuer Code).

Amended effective 1.1.20

"**IAC Code Set**" is defined in the IAC Regulations and means the codes, practices, procedures, standards and/or specifications published pursuant to Regulation 11.1.

Amended effective 1.1.20

"**IAC Interchange Line**" means an Interchange Line that is not otherwise prescribed by an Approved Card Payment System.

Inserted effective 1.1.20

"**IAC Interchange Link**" means an Interchange Link that is not otherwise prescribed by an Approved Card Payment System.

Inserted effective 1.1.20

"**IAC Operational Broadcast**" means the form set out in IAC Code Set Volume 1 (Introduction and Member Obligations) Annexure D.

Amended effective 1.1.20

"**IAC Settlement Rules**" means the set of rules and requirements for the settlement of obligations arising as a result of exchange of Items set out in IAC Code Volume 5 (Settlement Code).

Amended effective 1.1.20

"**IAF**" or "**Issuers and Acquirers Forum**" is defined in the IAC Regulations and means the governing body for the IAC constituted by Part 7 of the IAC Regulations.

Amended effective 1.1.20

"**IC Card**" and "**ICC**" means a Card that contains an integrated circuit and that conforms to the EMV specifications.

"**iCVV**" and "**iCard Verification Value**": see "**Card Security Code**".

Inserted effective 1.7.20

"**Institutional Identifier Change Date**" means one of at least three dates in each calendar year specified by the IAF and notified by the Company to IA Participants prior to the commencement of that calendar year as being the Institutional Identifier Change Dates for that year.

"**Interchange**" means the exchange of Items for value between Acquirers and Issuers, via an Interchange Link, as a result of the use of an Issuer's Card by a Cardholder to generate a Transaction.  Interchange arrangements may, but need not, be reciprocal.

"**Interchange Activity**" is defined in the IAC Regulations and means:

(a)   the direct or indirect exchange of Items for value between Acquirers and Issuers, as a result of the use of an Issuer's Card by a Cardholder to generate a Card Payment from facilities owned and/or operated by the Acquirer or a third party.  Interchange arrangements may, but need not be, reciprocal; or

(b)   the exchange of Card Payment instructions and related messages between Acquirers and Issuers, pursuant to the rules of an Approved Card Payment System; or

(c)   any other Card-based electronic interchange activities from time to time approved for the purposes of this definition by the IAF.

"**Interchange Agreement**" means an agreement between an Acquirer and an Issuer that regulates the arrangements relating to Interchange Activity between them.

"**Interchange Fee**" means a fee charged to one party to an Interchange Activity by the other party to the Interchange Activity for access to its consumer electronic payments facilities.

"**Interchange Line**" means the physical communications infrastructure that provides the medium over which Interchange Activity is supported.  An Interchange Line contains, at a minimum, one Interchange Link.

"**Interchange Line Encryption**" means encryption of the entire message, with the exception of communication headers and trailers that is being passed across an Interchange Line using, as a minimum, double-length keys and a triple-DES process.

"**Interchange Link**" means the logical link between an Acquirer and an Issuer which facilitates Interchange Activity between them.  Interchange Links are supported physically by an Interchange Line, and are either direct between an Acquirer and Issuer or indirect via a third party intermediary.

"**Interchange Link Message Authentication**" means calculation and verification of the Message Authentication Code (MAC) that is being passed across an Interchange Link.

"**Interchange Link PIN Encryption**" means encryption of the PIN in accordance with ISO 9564.1 and IAC Code Set Volume 4 Clause 2.7(d)(i).

Amended effective 21.11.16

"**Interchange Settlement Report**" means a report substantially in the form of Annexure A in IAC Code Set Volume 5 (Settlement Code).

"**Internet Key Exchange**" and "**IKE**" is the protocol used to set up a security association in the IPsec protocol suite.

"**ISO**" means an international standard as published by the International Standards Organization.

"**Issuer**" is defined in the IAC Regulations and means a Constitutional Corporation which, pursuant to the rules of an Approved Card Payment System, issues a Card to a Cardholder and, in
connection with any Card Payment effected using that Card:

Amended effective 1.1.20

(a) assumes obligations to the relevant Cardholder, which obligations are in the first instance discharged on its behalf by an Acquirer; and

(b) engages, directly or indirectly, in Interchange Activity with that Acquirer as a result.

"**Issuer Authentication**" [Deleted]

Deleted effective 1.01.20

"**Issuer Fraud Rate**" means the aggregate of Fraudulent Transactions as calculated in accordance with the IAC Code Set Volume 7 (Card Not Present Code), clause 3.1.1.

Amended effective 1.01.20

"**Issuer Fraud Threshold**" means the maximum allowable Issuer Fraud Rate as set out at IAC Code Set Volume 7 (Card Not Present Code clause 3.1.1(b).

Amended effective 1.01.20

"**Issuer Identification Number**" and "**IIN**" means a six digit number issued by ISO or Standards Australia that identifies the major industry and the card issuer. The IIN also forms the first part of the primary account number on the Card.

"**Issuer Sequence Number**" means a one or two digit number used at the option of the Issuer to identify a Card which may have the same primary account number as another Card and possible different accessible linked accounts.

"**Items**" is defined in the IAC Regulations and means Credit Items or Debit Items.

Amended effective 1.1.20

"**Key Encrypting Key**" and "**KEK**" means a key which is used to encipher other keys in transport and which can be used to exchange Session Keys between two systems.

"**Key Loading Device/Key Injection Device**" and "**KLD/KID**" means a hardware device and its associated software that is used to inject keys into a Terminal.

Amended effective 29.4.16

---

"**Key Transfer Device**" and "**KTD**" means a hardware device that is used to transfer a cryptographic key between devices. Typically KTDs are used to transfer keys from the point of creation to Terminals in the field.

"**Lead Institution**" means a financial institution responsible for direct settlement of scheme payment obligations.

"**Letter of Approval**" means a letter, issued by the Company, approving the use of a Secure Cryptographic Device within IAC.

"**LVSS**" means the RITS Low Value Settlement Service.

"**LVSS BCP Arrangements**" means the contingency plan and associated documents published by the Reserve Bank of Australia for the purposes of the RITS Low Value Settlement Service, and which can be accessed via a link on the Company's extranet.

"**LVSS Contact**" means the person nominated by a IA Participant as its primary contact for LVSS inquiries, as listed on the Company's extranet.

"**Merchant**" means a person which:

(a)    supplies goods or services to a Cardholder; and

(b)    has an agreement with an Acquirer to process and settle Card Payments.

Amended effective 1.1.19

"**Merchant Fraud Rate**" means the aggregate of Fraudulent Transactions as calculated in accordance with IAC Code Set Volume 7 (Card Not Present Code), clause 3.3.2(a).

Amended effective 1.01.20

"**Merchant Fraud Threshold**" means the maximum allowable Merchant Fraud Rate as set at IAC Code Set Volume 7 (Card Not Present Code),clause 3.3.2(b).

Amended effective 1.01.20

"**Message Authentication Code**" and "**MAC**" means a code, formed using a secret key, appended to a message to detect whether the message has been altered (data integrity) and to provide data origin authentication, MACs are formed in conformance with AS 2805.4.

Amended effective 20.8.18

"**Nine AM (9am) Settlement**" means the multilateral settlement of obligations arising from previous days' clearings of low value payments which occurs in RITS at around 9am each business day that RITS is open.

"**NODE**" or "**Node**" means a processing centre such as an Acquirer, an Issuer, or an intermediate network facility.

"**Non-standard POI Technology**" means a POI solution/technology that by nature of its design is unable to meet certain Australian or global payment standards identified in IAC Code Set Volume 4 (Device Requirements) Annexure G Schedule 1.

Inserted effective 1.1.20

"**Notice of Standard – Merchant Pricing for Credit, Debit and Prepaid Card Transactions**" is the informative guide referred to in clause 2.1.2 and set out in Annexure F to the IAC Code Set Volume 1 (Introduction and Member Obligations) relating to the notification requirements in the Reserve Bank's Scheme Rules relating to Merchant Pricing for Credit, Debit and Prepaid Card Transactions (Standard No. 3 of 2016).

<div align="right">Inserted effective 1.6.17</div>

"**On-us Transactions**" means Transactions that do not traverse Interchange and where the Acquirer and card Issuer are the same entity.

<div align="right">Inserted effective 1.1.20</div>

"**Originator**" means the party (for example an Acquirer direct settler or Lead Institution) which, as a result of either acquiring a Transaction or, in the case of a Lead Institution, by arrangement, is responsible for the submission of a File Settlement Instruction in accordance with this IAC Code Set and the requirements of the RITS Low Value Settlement Service.

"**Operator Member**" is defined in the IAC Regulations and means a Constitutional Corporation which:

<div align="right">Amended effective 1.1.20</div>

(a)     has been admitted, or which is eligible for admission, to membership of the Company pursuant to Article 2.11 of the Constitution;

(b)     is the operator or administrator of an Approved Card Payment System; and

(c)     is determined by the IAF to meet the Approval Criteria for Operator Members.

"**Partial Dispense**" means a Transaction that results in an amount of Cash being dispensed from an ATM that is less than the amount requested by the Cardholder.

"**PCISSC**" means the Payment Card Industry Security Standards Council.

<div align="right">Amended effective 20.8.18</div>

"**PCI Evaluation Report**" means an Evaluation Report, prepared in respect of the requirements set out in PCI PTS published standards. (PCI standards can be found at https://www.pcisecuritystandards.org).

<div align="right">Amended effective 1.1.19</div>

"**PCI Plus Evaluation Report**" means an Evaluation Report, prepared in respect of the PCI Plus Requirements, and if applicable, includes any delta report prepared in respect of the device.

<div align="right">Amended effective 1.1.19</div>

"**PCI Plus Requirements**" means the requirements set out in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) Annexure B which are determined by the Company to be additional to the requirements of PCI PTS.

<div align="right">Last amended effective 1.1.20</div>

"**PCI Points**" means the attack potential calculated in accordance with Appendix B of the Payments Card Industry (PCI) document "PCI PIN Transaction Security Point of Interaction Modular Derived Test Requirements".

<div align="right">Amended effective 1.1.20</div>

---

"**PED**" means a PIN Entry Device.

"**Physically Secure Device**" means a device meeting the requirements specified in AS 2805.14.1 for a physically secure device.  Such a device, when operated in its intended manner and environment, cannot be successfully penetrated or manipulated to disclose all or part of any cryptographic key, PIN, or other secret value resident within the device.  Penetration of such a device shall cause the automatic and immediate erasure of all PINs, cryptographic keys and other secret values contained within the device.

Amended effective 21.11.16

"**PIN**" is defined in the IAC Regulations and means a personal identification number which is either issued by an Issuer, or selected by a Cardholder for the purpose of authenticating the Cardholder by the Issuer of the Card.

Amended effective 1.1.20

"**PIN Entry Device**" and "**PED**" means a component of a Terminal which provides for the secure entry and encryption of PINs in processing a Transaction.

"**POI**" means Point Of Interaction technologies that can be provided to a Merchant to undertake Card Payments.  POI technologies include attended and unattended Point of Sale (POS) devices and ATMs.

Inserted effective 1.1.16

"**POS**" means Point of Sale.

Inserted effective 1.1.19

"**Prepaid Card**" means a Card that:

(a)    enables the Prepaid Cardholder to initiate electronic funds transfers up to a specified amount (subject to any other conditions that may apply); and

(b)    draws on funds held by the Prepaid Program Provider or third party by arrangement with the Program Provider (as opposed to funds held by the Prepaid Cardholder).

The definition of a Prepaid Card extends to both single use and reloadable/multiple use Cards.

"**Prepaid Cardholder**" means a person that is in possession of a Prepaid Card.

"**Prepaid Program Provider**" means either:

(a)    an Issuer that issues a Prepaid Card; or

(b)    a person that issues a Prepaid Card in conjunction with a sponsoring Issuer.

"**PVC**" means Public Key Verification Code.

Inserted effective 20.8.18

"**Quarter**" means the unit of 3 months commencing on either 1 January, 1 April, 1 July or 1 October.

Inserted effective 1.07.19

"**Recognised APS**" is defined in the IAC Regulations and has the meaning given in the Constitution. <small>Amended effective 1.1.20</small>

"**Record of Transaction**" has the meaning given in the ePayments Code and IAC Code Set Volume 3 (Acquirer Code).

"**Regulations** or the "**IAC Regulations**" is defined in the IAC Regulations and means the regulations for IAC (including, without limitation, the annexures and schedules to the Regulations) as amended from time to time.  A reference to a particular Regulation has a corresponding meaning. <small>Amended effective 1.1.20</small>

"**Remote Management Solution**" and "**RMS**" means a solution comprising both hardware and software which connects to an SCM over a network and provides access to an SCM while it is in a sensitive state.

"**Reporting Date**" means the 30th day of the month which follows the end of each Quarter, being 30 April, 30 July, 30 October or 30 January.  If the 30th day of the month occurs on a weekend, the Reporting Date for that month will be the first business day following the 30th day. <small>Amended effective 1.1.21</small>

"**Reserve Bank**" means the Reserve Bank of Australia.

"**Retained Card**" in relation to an ATM Transaction, has the meaning given in clause 2.8 of IAC Code Set Volume 6 (ATM System Code).

"**Risk Based Analysis**" has the meaning given to it  in IAC Code Set Volume 7 (Card Not Present Code),clause 2.1.1. <small>Amended effective 1.01.20</small>

"**RITS**" means the Reserve Bank Information and Transfer System.

"**RITS Low Value Settlement Service**" means the Reserve Bank's settlement file transfer facility which must be used by:

(a)     each Acquirer and Lead Institution to submit File Settlement Instructions and associated File Recall Instructions; and

(b)     each Acquirer, Lead Institution and Issuer, if it so elects, to receive File Settlement Advices, File Settlement Responses and File Recall Responses.

"**RITS Regulations**" means the regulations for RITS published by the Reserve Bank of Australia.

"**SCD Security Standards**" in relation to an SCD, means the standards from time to time published in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), Part 2. <small>Last amended effective 1.1.20</small>

"**SCM**" means a Security Control Module sometimes referred to as a Hardware Security Module (HSM). <small>Amended effective 20.8.18</small>

---

"**Secretary**" is defined in the IAC Regulations and means a person appointed by the Chief Executive Officer to perform the duties of secretary of the IAF under Regulation 7.14.

"**Secure Card Reader PIN**" and "**SCRP**" means a physical card reader that has been approved by PCI PTS and is a component of a SPOC Solution.

"**Secure Cryptographic Device**" and "**SCD**" means a device that provides physically and logically protected cryptographic or PIN handling services and storage e.g., EPP, Terminal, Key Injection Device or hardware security module.

"**Security Control Module**" and "**SCM**" means a physically and logically protected hardware device that provides an intentionally limited set of secure cryptographic services.

"**Session Key**" is a generic reference to any one of a group of keys used to protect Transaction level data. Session keys exist between two discrete points within a network (e.g., host-to-host and host-to-terminal).

"**Settlement Items**" is defined in the IAC Regulations and means, Items which are either:

(a)    ATM Transactions cleared under the auspices of the IAC Code Set Volume 6 (ATM System Code); or

(b)    EFTPOS Transactions cleared pursuant to the Rules prescribed for the EFTPOS Card Payment System (as defined in those Rules) by the administrator of that system; or

(c)    credit payment instructions referable to a transaction of the type described in paragraphs (a) and (b).

"**Software-based PIN entry on COTS**" and "**SPoC**" means the term Software-based PIN entry on COTS as used in the PCISSC SPoC standards.

"**SPC**" and "**Signature Panel Code**": see "**Card Security Code**".

"**Sponsor**" means the Acquirer which, as among all Acquirers for a Terminal, is taken to be the lead Acquirer for that Terminal, with ultimate responsibility for the integrity and security of software and encryption keys for Transactions involving that Terminal.

"**Standard Interchange Specification**" means the technical specification set out in Annexure A of IAC Code Set Volume 6 (ATM System Code).

"**Statistically Unique**" means an acceptably low statistical probability of an entity being duplicated by either chance or intent. Technically, statistically unique is defined as follows:

*"For the generation of n-bit quantities, the probability of two values repeating is less than or equal to the probability of two n-bit random quantities repeating. Thus, an element chosen from a finite set of 2n elements is said to be statistically unique if the process that governs the selection of this element provides a guarantee that for any integer $L \leq 2n$ the probability that all of the first L selected elements are different is no smaller than the probability of this happening when the elements are drawn uniformly at random from the set."*

"**Strong Customer Authentication**" or ("**SCA**") has the meaning given to it in IAC Code Set Volume 7 (Card Not Present Code), clause 2.1.2.

*Amended effective 1.01.20*

"**Tamper-responsive SCM**" means a Security Control Module that when operated in its intended manner and environment, will cause the immediate and automatic erasure of all keys and other secret data and all useful residues of such data when subjected to any feasible attack. A Tamper-responsive SCM must comply with the requirements of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

"**Terminal**" means an electronic device which can be used to initiate a Transaction e.g. ATM, UPT or EFTPOS Terminal.

*Last amended effective 1.1.19*

"**Terminal Identification Number**" means the unique identification number assigned by an Acquirer to identify a particular Terminal.

"**Terminal Sequence Number**" means a number allocated sequentially to each Transaction by the relevant Terminal.

"**Third Party Provider**" means a body corporate which provides an outsourced facility to a IA Participant for any function involving:

(a)     interchange;

(b)     PIN processing;

(c)     transaction processing;

(d)     key management; or

(e)     any other service which directly or indirectly supports any of the functions described in clauses (a) to (d) above.

"**Threshold Requirement**" is defined in the IAC Regulations and means a requirement under the IAC Regulations or in this IAC Code Set which the IAF determines to be so fundamental to the integrity and safety of Card Payments that compliance is to be enforceable by imposition of a fine under Regulation 6.2, the details of which are published on the Company's extranet.

"**Track Two Equivalent Data**" means the contents of the EMV data element tag 57. This data element contains the data elements of track two according to AS 3524-2008, excluding start sentinel, end sentinel and Longitudinal Redundancy Check.

"**Transaction**" is defined in the IAC Regulations and means an electronic funds transfer, cash withdrawal or other transaction initiated by a Cardholder using a Card which allows for the accessing of available funds held in an account, or a credit facility linked to an account, or account information.

"**Triple-DES**" means the encryption and decryption of data using a defined compound operation of the DEA-1 encryption and decryption operations. Triple-DES is described in AS2805.5.4.

"**Unattended Device**" means a device intended for principal deployment in a location not subject to the regular day-to-day oversight by a trusted employee of the Acquirer or their trusted agent.

"**Unattended Payment Terminal**" and "**UPT**" means a Terminal intended for deployment in an EFTPOS network without Merchant oversight.

**Next page is 2.1**

## PART 2   DEVICE SECURITY STANDARDS

This part sets out the minimum security standards applicable to secure cryptographic devices (SCDs) that are required to be met by all IA Participants.

### 2.1   Relevant Standards

The Company is committed to the use of the latest national and international standards in the Interchange environment.  The requirements contained in:

(a)   AS 2805 all parts;

(b)   ISO 9564 all parts;

(c)   ISO 13491 all parts;

(d)   ISO 11568 all parts;

(e)   ISO TR14742 Recommendations of cryptographic algorithms and their use;

(f)   PCI PIN Transaction Security, (PCI PTS);

(g)   PCI PIN Transaction Security Point of Interaction Derived Test Requirements;

are considered normative to this security standard.  In all cases the latest version of each of these standards should be taken to be applicable (unless specifically identified otherwise).

### 2.2   References

The following documents are referenced in this Part 2:

(a)   AS 2805.2-2007/Amdt 2/2008 Electronic funds transfer – Requirements for interfaces Part 2: Message structure, format and content;

(b)   AS 2805.4.1-2001/Amdt 1/2006 Electronic funds transfer – Requirements for interfaces Part 4.1: Message authentication – Mechanism using a block cipher;

(c)   AS 2805.6.3-2000/Amdt 1/2003 Electronic funds transfer – Requirements for interfaces Part 6.3: Key management – Session Keys – Node to node;

(d)   AS 2805.6.1-2002/Amdt 3/2007 Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles;

(e)   AS 2805.9-2000 Electronic funds transfer – Requirements for interfaces Part 9: Privacy of communications;

---

(f)  AS 2805.16 Electronic funds transfer – Requirements for interfaces Merchant Category Codes;

(g)  AS 2805.6.6-2006 Electronic funds transfer – Requirements for interfaces Part 6.6: Key management – Session Keys – Node to node with KEK replacement;

(h)  AS 2805.6.7–2011 Electronic funds transfer - Requirements for interfaces. Part 6.7: Key management - Transaction keys - Derived unique key per transaction (DUKPT);

(i)  ISO 9564.1-2011 Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems;

*Inserted effective 21.11.16*

(j)  Payment Card Industry Data Security Standard – Version 1.2.

## 2.3    Interpretation

The following definitions supersede the equivalent definitions provided in AS 2805.14 series (ISO 13491).

### 2.3.1    *Not Feasible*

(a)  "Not Feasible" means in the case of attacks:

(i)  against the Cardholder PIN, the device is to be resistant to any Phase 1 attack costing less than 26 PCI Points and to any Phase 2 attack costing less than 13 PCI Points;

(ii)  against PIN-security related cryptographic keys, components and residues including access codes and passwords protecting sensitive states, symmetric and private cryptographic keys, MAC keys or other such sensitive data, the device is to be resistant to any attacks costing less than 35 PCI Points and to any Phase 2 attack costing less than 15 PCI Points;

(iii)  against the integrity of public keys, the device is to be resistant to any Phase 1 attack costing less than 35 PCI Points and to any Phase 2 attack costing less than 15 PCI Points;

(iv)  against Tamper Evident protections, the device is to be resistant to any Phase 1 attack costing less than 14 PCI Points and to any Phase 2 attack costing less than 8 PCI Points;

(v)  for EFTPOS Terminals, against the Magnetic-stripe reader, (if present), and its connection path the device is to be resistant to any Phase 1 attack costing less than 16 PCI Points and to any Phase 2 attack costing less than 8 PCI Points;

*Amended effective 20.8.18*

(vi)    for EFTPOS Terminals, against the ICC reader (if present) and its connection path, the device is to be resistant to any Phase 1 attack costing less than 20 PCI Points and to any Phase 2 attack costing less than 10 PCI Points;

<div style="text-align:right">Amended effective 20.8.18</div>

(vii)    for EFTPOS Terminals, against prompts for cardholder data entry and display messages, (if present), the device is to be resistant to any Phase 1 attack costing less than 18 PCI Points and to any Phase 2 attack costing less than 9 PCI Points;

<div style="text-align:right">Amended effective 20.8.18</div>

(viii)    for ATM devices, the magnetic-stripe reader, associated software and connection path, and against any ICC reader (if present) hardware, associated software and connection path, and against the outer shell of the device, the device is to be resistant to any Phase 1 attack costing less than 14 PCI points and to any Phase 2 attack costing less than 9 PCI Points;

(ix)    for ATM devices, against unauthorised changing of prompts, the device is to be resistant to any Phase 1 attack costing less than 16 PCI Points and to any Phase 2 attack costing less than 9 PCI Points;

(x)    for Unattended Devices ATM devices, against removal of ATM secure components, the device is to be resistant to any Phase 1 attack costing less than 18 PCI Points and to any Phase 2 attack costing less than 9 PCI Points; and

(xi)    for Unattended Devices (other than ATM Devices), against the removal of secure components to protect against unauthorised removal and/or reinstallation, the device is to be resistant to any Phase 1 attack costing less than 18 PCI points and to any Phase 2 attack costing less than 9 PCI Points.

(b)    In this Part, "Phase 1" and "Phase 2" have the meaning given to those terms, or to cognate expressions of them, in PCI PTS Point of Interaction Derived Test Requirements version 3.0, Appendix B, and in relation to the term "Phase 2" incorporates any temporal limitation or requirement specified in that document.

### 2.3.2   *PCI Points*

The calculation of attack resistance (measured as PCI Points in the preceding clause 2.3.1) must be performed using the method specified in Appendix B of the PCI PTS Derived Test Requirements.

### 2.3.3   *ISO 11568 - Key Management (retail)*

References to the ISO key management standard must be taken as references to AS 2805.6 series.

---

### 2.3.4 *ISO 9797 series - Requirements for message authentication*

References to the ISO message authentication standard must be taken as references to AS 2805.4.1.

## 2.4 Device Security Evaluation Criteria

This part sets out the minimum security standards for SCDs and the device evaluation process.

<div style="float:right">Amended effective 1.1.19</div>

### 2.4.1 *Applicable Version of AS 2805 part 14.2*

(a)    From 20 April 2010 all devices shall be evaluated using AS 2805.14.2-2009 and all references to AS 2805.14.2 in the IAC Code shall be construed as a reference to AS 2805.14.2-2009.

(b)    Prior to 20 April 2010:

   (i)    if a device has ICC functionality then the ICC reader must be tested against the requirements in AS 2805.14.2-2009; and

   (ii)    subject to clause 2.4.1(b)(i), devices may be evaluated using AS 2805.14.2-2009 or AS 2805.14.2-2009;

<div style="float:right">Amended effective 29.4.16</div>

and all references to AS2805 part 14.2 in the IAC Code shall be construed accordingly.

### 2.4.2 *Applicable Version of PCI PTS for PEDs*

All references to PCI PTS in the IAC Code shall be construed as a reference to PCI PIN Transaction Security, version 3.0 – 2011.

### 2.4.3 *Financial Terminals*

A financial Terminal consists of a number of components, which may include: PIN Entry Device (PED), printer, communications devices, customer/merchant interface, Acquirer application, IC Card reader and magnetic stripe reader. These components may be configured in various fashions, dependent upon requirements.

<div style="float:right">Amended effective 20.8.18</div>

Those components of a Terminal that provide cryptographic services and any services involved in requesting, reception and/or processing of the Cardholder PIN must collectively meet the requirements of a secure cryptographic device (SCD) as defined in AS 2805.14.2 for on-line devices and be approved for use by the Company (see IAC Code Set Volume 4 (Device Requirements and Cryptographic Management)).

<div style="float:right">Amended effective 21.11.16</div>

### 2.4.4     *Requirements for SCDs*

SCDs must meet the relevant requirements of AS 2805.14 (ISO 13491) and be evaluated against the requirements specified in AS 2805.14.2 Annex A, and additionally D (message authentication), E (key generation) and G (digital signature) if these functions exist in the SCD.

### 2.4.5     *EFTPOS Terminals*

<div align="right"><sub>Amended<br>effective 20.8.18</sub></div>

(c)     Where an EFTPOS Terminal includes a PED component it must be evaluated using the requirements specified in Part 2 and additionally AS 2805.14.2 Annexes A, B, D and G if digital signature functionality is used.

<div align="right"><sub>Amended<br>effective 20.8.18</sub></div>

(d)     Where an EFTPOS Terminal has PIN management functionality, including PIN translation, then it must also be evaluated using the requirements specified in Annex C of AS 2805.14.2.

<div align="right"><sub>Amended<br>effective 1.1.20</sub></div>

(e)     Where an EFTPOS Terminal does not include a PED component:

       (i)     it must also not include an MSR; and

       (ii)     it must be evaluated using the requirements specified in Part 2, and additionally, AS 2805.14.2 Annexe A, D and G if digital signature functionality is used, and only the following requirements of Annex B: B7, B13, B14, B19, B20, B23, B24 and B26.

### 2.4.6     *Privacy of Communication (EFTPOS Terminals)*

(a)     All EFTPOS Terminals must provide support for privacy of communication in a manner compliant with AS 2805.9 or any other privacy of communication standard approved by the Management Committee.

(b)     All application level data elements, including but not limited to fields P-45 (Track 1 data) and P-35 (Track 2 data), as defined in AS 2805.2, must be protected except those fields necessary to indicate the origin of the transaction and information required to correctly reconstruct the message. The latter may include the data required to derive the privacy key.

(c)     Where AS 2805.6.7 (DUKPT) is used to secure the dialogue between a Terminal and an Acquirer, compliance with AS 2805.9 must be achieved as per Appendix C of AS 2805.6.7.

### 2.4.7     *TCP/IP Support*

All Terminals capable of supporting TCP/IP as a communications protocol must additionally be evaluated against the requirements in Annexure A.

### 2.4.8 *Terminals Running Multiple Applications*

(a) Where a Terminal is running multiple applications, the Payment application and its associated data (especially PINs and cryptographic keys) must be protected from any interference or corruption caused by any other data or other application(s).

(b) Payment Applications must be evaluated according to the Device Approval Process.

(c) Non-payment applications require individual evaluation and authorisation by the Acquirer, or a party explicitly trusted by the Acquirer, for each application to be deployed or updated.

(d) The Terminal shall authenticate all non-payment applications using cryptographic mechanisms.

(e) The Acquirer shall have documented, auditable, key management procedures, which are compliant to AS2805.6.1 for any key used in the authentication processes associated with the Terminal software's authentication.

(f) If a party other than the Acquirer owns these keys, then the Acquirer shall assure themselves that the party (e.g. Terminal vendor or third party developer) has documented auditable, key management procedures which are compliant to AS2805.6.1 for any key used in the authentication processes associated with the Terminal software's authentication.

(g) All non-payment applications or updates to existing non-payment applications must be authenticated by the same cryptographic mechanism that is approved under Part 3.

(h) Acquirers shall maintain a register of all authorised non-payment applications per Terminal.

### 2.4.9 *Security Control Modules*

(a) Security Control Modules must be evaluated using AS 2805.14.2, Annexes A, C, D, E, F and, if digital signature functionality is provided, Annex G. Furthermore Annex H must be used to categorize the acceptable deployment environments for Security Control Modules. Uncontrolled environments are not suitable for the deployment of Security Control Modules.

(i) This clause describes the Controlled[+] environment, listing requirements, which when in addition to those required by AS 2805.14.2 Annex H for Controlled environments are considered to meet the requirements for a Secure environment for the deployment of SCMs:

(A) SCMs shall be housed in a stand-alone secure cabinet[1].

---

[1] Cabinets meeting Australian government Security Construction Equipment Committee (SCEC) Class C Security Containers satisfy this requirement.

(B) The secure cabinet shall be contained in an environment meeting a Controlled environment as specified in AS 2805.14.2 clause H.4.

(C) No other equipment shall be contained in the secure cabinet, including the host (other than that associated with the SCM e.g., management PC or monitoring device).

(D) The secure cabinet shall be fitted with dual, pick resistant locks, keyed uniquely from all other cabinets in the controlled environment.

(E) The keys for the secure cabinet shall be kept under dual control and only be made available to authorised custodians.

(F) All access to the secure cabinet shall be under dual control, logged and subject to regular audit.

(b) Security Control Modules that have been evaluated and found to be compliant with PCI HSM Security Requirements version 3 or later are deemed to satisfy the above physical and logical requirements. <sub>Inserted effective 21.11.16</sub>

(c) The functions provided by the SCM must be in accordance with clause 2.4.10.

### 2.4.10 *Limitations on Functions (SCM)*

A Security Control Module (SCM) must contain the following limitations on its functions: <sub>Amended effective 1.1.19</sub>

(a) The function set must be so designed that no single function, nor any combination of functions, can result in disclosure of secret information, except as explicitly allowed by these specifications.

(b) The only function calls and sensitive operator functions that can exist in the SCM are:

    (i) standard functions approved in writing by the Company (e.g., AusPayNet Specification for a Security Control Module Function Set);

    (ii) proprietary functions that are either:

        (A) totally equivalent to a series of standard functions and approved functions, or

        (B) approved in writing by the Company; or

(C) limited to use only proprietary variants of *KM in function inputs and outputs.

(c) Proprietary functions, whether SCM function calls or operator functions, are specifically prohibited from outputting any keys resident in the SCM, or protected by standard variants in any form whatsoever.

(d) No proprietary function, nor any combination of functions can result in the outputting of a clear-text PIN, or the outputting of such a PIN except as component of a PIN block enciphered under a key used only for protection of translated PIN blocks.

(e) Where the functionality of the SCM includes the ability to print clear-text PINs for example on PIN mailers, such functionality must only become operative whilst the module is under dual control.

(f) Where the SCM can have its functionality modified e.g., by loading of software, then unless any such modification is performed while the SCM is in a sensitive state under dual control and that the software or firmware is cryptographically authenticated any such modification is preceded by erasure of all cryptographic keys and sensitive data in the SCM.

(g) Additionally, where the SCM provides support for ISO format 1 PIN blocks, such functionality must be disabled in all Acquiring and switching systems from 1 January 2016.

<div style="text-align:right"><small>Amended<br>effective 20.8.18</small></div>

### 2.4.11 *SCM Remote Management*

(a) Devices providing a Remote Management Solution for Security Control Modules must be evaluated using AS 2805.14.2, Annex A - Logical security characteristics only; Annexes D, E - Physical and logical security characteristics only; Annex F - Physical and logical security characteristics only, and Annex G if digital signature functionality is provided. Annex H must be used to categorize the acceptable deployment environments for a Remote Management Solution for Security Control Modules. Uncontrolled environments are not suitable for the deployment of a Remote Management of Security Control Modules Solution.

(b) Remote Management Solutions may only be used with AusPayNet approved SCMs.

(c) Those components of a Remote Management Solution that provide any services involved in the management of an SCM must meet the following requirements:

   (i) Remote Management Solutions must support appropriate threat management techniques relevant to their operating platform, such as malware protection with up to date signatures and maintenance, vulnerability patching;

---

(ii) Remote Management Solutions must be cryptographically authenticated by the SCMs;

(iii) Remote management devices may only be deployed in a minimally controlled environment, a controlled environment or a secure environment as per Annex H of AS 2805.14.2. At a minimum:

(A) the storage of the Remote Management Solution must be under dual control;

(B) the operation of the Remote Management Solution must be under dual control; and

(C) while the Remote Management Solution is in operation access must be restricted to authorised personnel.

(d) Remote Management Systems must meet the key management requirements as set out in clauses 4.1, 4.2 and 4.3.

### 2.4.12    *Key Transfer and Loading Devices*

Key Transfer and Loading Devices must be evaluated using AS 2805.14.2, Annexes E and F.

Key Transfer and Loading Devices Modules that have been evaluated and found to be compliant with PCI HSM Security Requirements version 3 or later are deemed to satisfy the above physical and logical requirements.

*Inserted effective 21.11.16*

## 2.5    Privacy shielding

In accordance with AS 2805.14.2, Terminals must provide privacy shielding such that during normal operation, keys pressed will not be easily observable to other persons. (For example, the device could be designed and installed so that the device can be picked up and shielded from monitoring by the user's own body). As an alternative, where the device, in itself, does not provide sufficient shielding it is permissible to rely on external physical environment provided that the vendor supplies rules and guidance as to how the visual observation is to be deterred by the environment in which the Terminal is to be installed. Such rules and guidance must be provided to the Evaluation Facility, and to all prospective purchasers, for evaluation.

*Amended effective 20.8.18*

## 2.6    Device management

(a) Some of the checklist items in sections A.3 and B.3 of Annexes A and B of AS 2805.14.2 relate to management of an SCD after deployment and therefore do not need to be considered by Approved Evaluation Facilities when evaluating SCDs.

(b)     Approved Evaluation Facilities should complete checklist item A.3(b) based on assurances from the device manufacturer or an independent auditor.

## 2.7     Physical Characteristics and Key Management Protocols

If Terminals employ key-management schemes not specifically permitted in AS 2805.6 series, Acquirers may seek approval for their deployment from the Company.  This request for approval will be dealt with by the Company but is not a request to which the Device Approval Process applies.

*Last amended effective 1.1.19*

For the avoidance of doubt, a Terminal shall not rely on tamper evidence as its sole physical security characteristic (ISO 9564.1 clause 5.1).  Terminals must also meet the following requirements:

*Last amended effective 20.8.18*

(a)     when employing a "master/session key" key-management scheme (e.g., AS 2805.6.4); or

*Amended effective 21.11.16*

(b)     when employing a "unique key per Transaction" key-management scheme (e.g., AS 2805.6.2) meet, at a minimum, the requirements of a Physically Secure Device as defined in AS 2805.14.1;

(c)     devices must generate and verify Message Authentication Codes as per AS 2805.4.1 for all value Transaction messages; and

*Amended effective 21.11.16*

(d)     use one of the PIN block formats, excluding format 1, specified in ISO 9564.1.  Format 3 is preferred.  Format 8, here described, may also be used where required:

*Amended effective 21.11.16*

(i)     A format 8 PIN block may be used where a PIN Block is required but no PIN is available.  The PIN block is constructed by the modulo 2 addition of two 64-bit fields formatted as follows:

*Inserted effective 21.11.16*

1.     a plain text field

*Inserted effective 21.11.16*

Bit

| 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 64 |
|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|-------|
| C | N | R | R | R | R | R | R | R | R | R | R | R | R | F | F |

and;

2.     the account number field

*Inserted effective 21.11.16*

Bit

| 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 | 64 |
|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 0 | 0 | 0 | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 | A11 | A12 |

Where:

| | | | | |
|---|---|---|---|---|
| C | = | Control Field | • | 1000 (binary) |
| N | = | PIN length | • | 0000 (binary) |
| R | = | Random digit | • | 4-bit binary field with each occurrence being randomly chosen form the range 0000 (zero) to 1111 (fifteen). |
| | | | • | The resultant 48-bit random number shall be unique (except by chance) for each occurrence of a format 8 PIN block. |
| | | | • | The random number shall not be transmitted in the clear. |
| F | = | Fill digit | • | 1111 (binary) |
| 0 | = | Pad digit | • | 0000 (binary) |
| A1 to A12 | = | Account number | • | Content is the 12 right-most digits of the primary account number (PAN) in 4-bit binary representation, excluding the check digit. |
| | | | • | A12 is the digit immediately preceding the PAN's check digit. |
| | | | • | If the PAN excluding the check digit is less than 12 digits, the digits are right justified and padded to the left with 0000 (zero). |
| | | | • | Permissible values are 0000 (zero) to 1001 (nine) |

and;

(e)  use only those hash algorithms specified in ISO TR-14742 Recommendations on Cryptographic Algorithms and their Use – Technical Report.  Those algorithms must be implemented in accordance with the guidelines given in that technical report.

## 2.8     Device Classification

### 2.8.1    *Unattended device*

(a)  A device intended for principal deployment in a location not subject to the regular day-to-day oversight by a trusted employee of the Acquirer or their trusted agent is termed an "Unattended Device". Unattended Devices shall comply with the appropriate requirements for PIN Entry devices given in ISO 9564.1 and shall have both tamper responsive and tamper evident characteristics.

(b)  Additionally, each secure component intended for an Unattended device must contain an anti-removal mechanism to protect against unauthorised removal and/or unauthorised re-installation.

### 2.8.2 *Attended device*

A device complying with the requirements for PIN Entry devices given in ISO 9564.1 and intended for use within attended environments, and shall have both tamper responsive and tamper evident characteristics.

## 2.9 Software-based PIN entry on COTS (SPoC)

Inserted effective 1.1.19

### 2.9.1 *SPoC Solution Security Standards*

This part sets out the minimum security standards applicable to secure SPoC solutions that are required to be met by all IA Participants.

The requirements contained in:

Amended effective 1.1.20

(a)   PCISSC Software-Based PIN entry on COTS Security Requirements; and

(b)   PCISSC Software-Based PIN entry on COTS Test Requirements,

are considered normative for SPoC solutions.

The document PCISSC Software-Based PIN entry on COTS Magnetic Stripe Readers Annex Security and Test Requirements is not applicable.

Amended effective 1.1.20

Any amendment or variation to the PCISSC Software-Based PIN entry on COTS Security Requirements or Test Requirements listed above must be reviewed and accepted by the Company before they are considered normative for SPoC solutions.  Any amendment or variation accepted by the Company will be listed on the Company's website, (https://www.auspaynet.com.au/resources/cards-and-devices).

Inserted effective 1.7.20

### 2.9.2 *SPoC Solution Security Evaluation Criteria*

This part sets out the minimum security standards for SPoC Solutions and the SPoC Solution evaluation process.

(a)   All SPoC Solutions must have been approved by PCISSC and must be listed on the PCISSC website for Approved SPoC Solutions.

(b)   The SCRP component of a SPoC Solution must meet the relevant PCI Plus security requirements of Annexure B of this Volume.

(c)   The Company will assess individually the PCISSC SPoC FAQs for suitability to the Australian payments industry.  The Company will formally communicate each unacceptable FAQ to the SPoC Solution Approved Evaluation Facilities.

Amended effective 1.7.20

---

(d) All SPoC Solutions must be evaluated by reference to those PCI SSC SPoC FAQs suitable to the Australian payments industry and listed on the Company's website, https://www.auspaynet.com.au/resources/cards-and-devices.

<div style="text-align: right">Amended effective 1.7.20</div>

## 2.10 Contactless Payments on COTS (CPoC)

<div style="text-align: right">Inserted effective 1.7.20</div>

### 2.10.1 *CPoC Solution Security Standards*

This part sets out the minimum security standards applicable to secure CPoC Solutions that are required to be met by all IA Participants.

The requirements contained in:

(a) PCISSC Contactless Payments on COTS Security and Test Requirements; and

(b) PCISSC Contactless Payments on COTS Program Guide,

are considered normative for CPoC solutions.

Any amendment or variation to the PCISSC Contactless Payments on COTS Security Requirements, Test Requirements or Program Guide listed above must be reviewed and accepted by the Company before they are considered normative for CPoC Solutions. Any amendment or variation accepted by the Company will be listed on the Company's website, (https://www.auspaynet.com.au/resources/cards-and-devices).

### 2.10.2 *CPoC Solution Security Evaluation Criteria*

This part sets out the minimum security standards for CPoC Solutions and the CPoC Solution evaluation criteria.

(a) All CPoC Solutions must have been approved by PCISSC and must be listed on the PCISSC website for Approved CPoC Solutions.

(b) The Company will assess individually the PCISSC CPoC FAQs and any amendment or variation for suitability to the Australian payments industry. The Company will formally communicate each unacceptable FAQ to the CPoC Solution Approved Evaluation Facilities.

(c) All CPoC solutions must be evaluated by reference to those PCISSC CPoC FAQs suitable to the Australian payments industry and listed on the Company's website, (https://www.auspaynet.com.au/resources/cards-and-devices).

**Next page is 3.1**

## PART 3   DEVICE APPROVALS

This Part 3 contains the IAC's requirements for approval of a device, SPoC Solution, CPoC Solution or non-standard POI Technology for use in Interchange.  Part 1.1 of this Volume 4 states the purpose of the IAC.  In the context of device, SPoC Solution, CPoC Solution and non-standard POI Technology approvals, that purpose includes balancing the interest of maintaining the security and integrity of Australian Card Payments with the interest of promoting innovation and competition.

These Part 3 requirements for approval of a device for use in Interchange apply equally to approval of both a SPoC and a CPoC Solution for use in Interchange and to approval of non-standard POI Technology for use in Interchange.  In considering an application for approval of both a SPoC and a CPoC Solution, when necessary and relevant, all references in Part 3 to a device are to be read and replaced with references to either a SPoC or a CPoC Solution.  In considering an application for approval of non-standard POI Technology, when necessary and relevant, all references in Part 3 to a device are to be read and replaced with references to non-standard POI Technology.

### 3.1      Standards

The Company is responsible for reviewing and determining device approval applications including determining any conditions to be attached to an approval. The process for device approval applications is set out in the Device Approval Process.

(a)     The following standards are to be used, as applicable, in evaluating the device's compliance with Part 2 of IAC Code Set Volume 4:

(i)      in accordance with the process defined in AS 2805.14.1 for the semi-formal methodology and using the requirements and processes specified in Part 2 and Part 3 of this Volume; or

(ii)     if the device is a Key Loading and Transfer device and has been evaluated and determined to be compliant with PCI HSM version 3 or later, application can be made to add the device to the Approved Devices List;

(iii)    if the device is a Security Control Module and has been evaluated and determined to be compliant with PCI HSM version 3 or later, application can be made to evaluate its compliance with clause 2.4.10 of this volume, such examination to be undertaken in accordance with the process defined in AS 2805.14.1 for the semi-formal methodology;

(iv)    if the device has been evaluated and determined to be compliant with a version of PCI PTS listed in Annexure B, application can be made to evaluate its compliance with the requirements in Part 2 of this Volume using Annexure B , such examination to be undertaken in accordance with the process defined in AS 2805.14.1 for the semi-formal methodology;

(b)     When assessing an approval application for a SPoC solution variations to the Device Approval Process are to be applied, as necessary and relevant, to facilitate its application to SPoC solutions.  Such variations include but are not limited to:

   (i)     references to 'Device Approval Applicant' are to be read as 'SPoC Solution Approval Applicant' and references to 'device', 'cryptographic device' and 'SCD' are to be read as references to 'SPoC solution';

   (ii)    references to 'Device Security Standards' and 'Device Evaluation FAQs' are to be read as 'SPoC Solution Standards' detailed in Part 2.9 above and the SPoC FAQs listed on AusPayNet's website;

   (iii)   references to the process for accreditation to perform Secure Cryptographic Device (SCD) security testing are to be read, as relevant, to references to the process for accreditation to perform SPOC solution testing; and

   (iv)    an approved SPoC Solution Test Laboratory will be listed on the AusPayNet website as a SPoC Solution Approved Evaluation Facility.

(c)     When assessing an approval application for a CPoC Solution variations to the Device Approval Process are to be applied, as necessary and relevant, to facilitate its application to CPoC Solutions.  Such variations include but are not limited to:

   (i)     references to 'Device Approval Applicant' are to be read as 'CPoC Solution Approval Applicant' and references to 'device', 'cryptographic device' and 'SCD' are to be read as references to 'CPoC Solution';

   (ii)    references to 'Device Security Standards' and 'Device Evaluation FAQs' are to be read as 'CPoC Solution Standards' detailed in Part 2.10 above and the CPoC FAQs listed on AusPayNet's website;

   (iii)   references to the process for accreditation to perform Secure Cryptographic Device (SCD) security testing are to be read, as relevant, to references to the process for accreditation to perform CPoC solution testing.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(d) When assessing an approval application for a non-standard POI Technology, variations to the Device Approval Process are to be applied, as necessary and relevant, to facilitate its application to non-standard POI Technology.  Such variations include but are not limited to:

> Inserted effective 1.7.19

(i) references to 'Device Approval Applicant' are to be read as 'non-standard POI Technology Approval Applicant' and references to 'device', 'cryptographic device' and 'SCD' are to be read, as appropriate, as references to 'non-standard POI Technology';

(ii) references to the process for accreditation to perform Secure Cryptographic Device (SCD) security testing are to be read as references to identification of laboratories best matched for testing non-standard POI Technology.

## 3.2　Approval of Devices

(a) If the Company approves a device the Company must issue a Letter of Approval to the Device Approval Applicant including any conditions which are attached to the approval.

> Amended effective 1.1.19

(b) If the Company declines to approve a device the Company must notify the Device Approval Applicant of the reasons for its decision including the details of the unacceptable results.

> Amended effective 1.1.19

(c) Device approval must be granted by the Company for a period of three years (the "Approval Period").

> Amended effective 1.1.19

(d) At the conclusion of the Approval Period, the Company may, at its sole discretion, extend the Approval Period for a further period of three years or such other period as it (in its absolute discretion) deems appropriate having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issues.

> Amended effective 1.1.19

(e) The Company may revoke device approval prior to expiry of the Approval Period, (or any extension thereof) if it decides that:

> Amended effective 1.1.19

(i) the device no longer meets the criteria against which the device was approved; or

> Amended effective 1.1.19

(ii) approval of the device has been withdrawn or revoked by any other relevant security standards body; or

(iii) the device is vulnerable to a significant security threat which did not exist or was not apparent at the time the device approval was granted.

(f) A list of approved devices must be made available on the AusPayNet web site.

---

(g)     The Company must only require re-certification upon the expiration of a device's approval, where substantial changes in security technology, applicable standards, security threats and/or knowledge have occurred since the granting of the initial approval.

(h)     The Compay may provide delta approval of a device where there have been changes to device software and/or minor hardware modifications.

Inserted effective 1.1.19

## 3.3     Approved Evaluation Facilities

(a)     A testing laboratory for compliant devices may be accredited as an Approved Evaluation Facility only if:

Amended effective 1.1.19

(i)     the Management Committee is reasonably satisfied as to that entity's credentials, independence and expertise;

(ii)     the Company has obtained that entity's agreement to assess any relevant device for conformity to the SCD Security Standards; and

(iii)     the entity has satisfied the requirements of the Evaluation Facility Accreditation Process as specified in Part 3 of the Device Approval Process.

Amended effective 1.1.19

(b)     Approved Evaluation Facilities will be listed on the AusPayNet website.

## 3.4     Evaluation Costs [DELETED]

Deleted effective 1.1.19

## 3.5     Agreements [DELETED]

Deleted effective 1.1.19

## 3.6     Evaluation Facility Accreditation Process [DELETED]

Deleted effective 1.1.19

**Next page is 4.1**

## 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 AS 2805.6.1.

### 4.2   Transport Keys

#### 4.2.1   *Approved Encryption Algorithms for Transport Keys*

DEA2 and DEA3 are the only approved algorithms for the protection of keys in transport.

#### 4.2.2   *Minimum Key Length for Transport Keys*

(a)   DEA2 keys of less than 2048 bits are to be treated as single use keys and their use is deprecated.

(b)   DEA2 key lengths of less than 1024-bits are unsuitable for general use. Preferred DEA2 key lengths are equal to or greater than 2048 bits in length and should be used in all new implementations where hardware constraints do not exist.

(c)   Triple DES (DEA3) may use either 128-bit or 192-bit key sizes.

#### 4.2.3   *Key Life Cycle Practices for Transport Keys*

(a)   DEA3 Key Transport Keys are single use keys only.

(b)   Symmetric Key Transport Keys must be freshly generated to protect keys in transport and then securely destroyed after use.

(c)   At the time of publication, DEA2 keys of size equal to or in excess of 2048 bits are deemed acceptable for a key change interval (life time) of two (2) years.

### 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 DEA3 keys with a minimum length of 128-bits (112 effective).

## 4.4    IAC Interchange Cryptographic Keys

### 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;

(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 exchange; or

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

### 4.4.2    *Cryptographic Algorithms*

(a)    DEA3 and DEA2 are the only approved algorithms for the protection of interchange information (full details of these algorithms may be found in the Australian standards AS 2805.5.4 and AS 2805.5.3 respectively).

(b)    DEA3 keys are 128 bits in length (effectively 112 bits) and are generally referred to as triple DES or 3DES keys (the corresponding encryption algorithm is specified in AS 2805.5.4).  Triple DES may also be acceptably implemented using a key length of 192 bits (effectively 168 bits).

(c)    DEA3 with a key length of 128 bits and DEA2 with key lengths equal to, or greater than 2048 bits are the minimum acceptable requirements for the effective protection of interchange information at the time of the issuance of this document.

(d)    In accordance with AS 2805.3.1, DEA3 must be used for PIN encipherment.  Acquirers who do not comply with this requirement from 1 February 2008 are responsible for any Issuer loss (direct or indirect) arising from the compromise of PIN data due to a breach of this requirement.

---

**4.5      IAC Interchange Links**                    Amended
                                                       effective 1.1.20

**4.5.1      *IAC Interchange Security Requirements***      Amended
                                                            effective 1.1.20

For all IAC Interchange Links, Issuers and Acquirers must ensure that:      Amended
                                                                            effective 1.1.20

(a)   security for Transactions processed over that IAC Interchange Link      Amended
      complies with: AS 2805.6 series;                                        effective 1.1.20

(b)   security for Transactions from Terminal to Acquirer and from Acquirer to
      Issuer complies with: AS 2805.6 series;

(c)   PIN security and encryption complies with AS 2805. 3.1 and clause 4.8 of      Amended
      this IAC Code Set Volume 4;                                                   effective 29.4.16

(d)   Key management practices comply with AS 2805.6.1;

(e)   Message Authentication must apply to all IAC Interchange Links;      Amended
                                                                          effective 1.1.20

(f)   The Message Authentication Code (MAC) must be calculated using, as a
      minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming
      to AS 2805.4.1; and

(g)   all interchange PIN and MAC cryptographic functions must be performed
      within a Tamper-responsive SCM.

**4.5.2      *Key Management Practices – IAC Interchange Links***      Amended
                                                                      effective 1.1.20

<span style="color:red">***Clause 4.5.2 is Confidential***</span>

                                                       Amended
                                                       effective 1.1.20

**4.6      KEK Establishment**

**4.6.1      *Introduction***

(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.

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

      (i)     AS 2805.6.6 method;

      (ii)    Native RSA key method;

      (iii)   KTK method;

---

(iv)  KEK Component method.

(c)  For those members employing AusPayNet standard Security Control Modules where RSA functionality exists, the Native RSA initialisation method is preferred.

### 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[2]) 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*

(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.

---

[2] 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

(c) When generated on request, the Interchange Key Encrypting Key (KEKs) is signed by the native private key[3] 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[4]) 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.

---

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

[4] 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.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(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;

(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)    The corresponding SCM functions are: C500 GETPUBLIC, C600 NODEKEKSEND, C610 NODEKEKREC.

(h)    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.

(i)    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*

(a)    This method relies on a transport 3DES 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 XOR key components and each partner will contribute to its construction supplying at least one component.

(b)    In the AusPayNet SCM specification SCMs, the functions used are D501 KEKGEN-6.3 and D502 KEKREC-6.3.

(c)  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.

(d)  The key exchange procedure is the following:

   (i)  each interchange partner generates at least one KTK component and submits it through a secure channel to the corresponding Interchange partner for loading into an SCM;

   (ii)  KTK is loaded by each partner;

   (iii)  the KVCs are verified;

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

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

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

   (vii)  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;

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

(e)  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.

(f)  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.).

### 4.6.5  *KEK Component Method*

(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 direct manual storage of 3DES interchange keys in the SCM devices, therefore the interchange keys (KEKs) in this method are generated externally and are loaded into the device in components. The key material requires a secure key loading procedure and also secure storage of the key components.

(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 interchange keys in at least two XOR components and exchange paper components using a secure channel;

(ii)  the keys are loaded into the SCM device under dual control - the corresponding KVCs are noted for verification; the keys may also be encrypted under the KM for storage in the key data base;

(iii)  the partners confirm the KVCs;

(iv)  the paper components are stored in the secure storage (e.g., safes under dual control);

(v)  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.

(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.

## 4.7  IAC Interchange Lines

Amended
effective 1.1.20

IAC Interchange Lines must be subject to whole-of-message encryption, excluding communications headers, using at a minimum, triple-DES and a DEA 3 (128-bit)-bit key in accordance with AS 2805.5.4.

---

**4.7.1**     *IAC Interchange Line Cryptographic Management*

<div align="right">Amended<br>effective 1.1.21</div>

(a)    Subject to clause 4.6, the use of transport level data encryption (e.g., IPSec) is permitted subject to the following conditions:

     (i)    data encryption must use either triple DES with either a 112-bit or 168-bit key length, exclusive of parity bits, or AES;

     (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-1;

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

     (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;

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

     (ix)    the minimum Diffie-Hellman MODP group size is 1536-bits;

     (x)    Internet Key Exchange, if used, must be configured to only use main mode.  Specifically, aggressive mode must NOT be used.

(b)    Where encrypted shared-secrets are used, key management, including the process of key (secret) entry must comply with the requirements of AS 2805.6.1, especially the requirement that no one person must have the capability to access or ascertain any plain text secret or private key.

**4.7.2**     *Key Management Practices for IAC Interchange Lines*

<div align="right">Amended<br>effective 1.1.20</div>

<div align="center" style="color:red">***Clause 4.7.2 is Confidential***</div>

## 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: AS 2805.6 series;

(b) PIN security and encryption complies with AS 2805.3.1 and 5.4;

(c) Key management practices comply with AS 2805.6.1;

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

Amended effective 1.1.19

(e) the Message Authentication Code (MAC) must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1; and

(f) all PIN and MAC cryptographic functions must be performed within an SCD.

(g) 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

<span style="color:red">***Clause 4.8.2 is Confidential***</span>

### 4.8.3 Key Rolling Process for Session Keys

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.

**Next page is A.1**

## ANNEXURE A. MINIMUM EVALUATION CRITERIA FOR IP ENABLED TERMINALS

### A.1 Introduction

In addition to the criteria set out in clause 2.4 of this volume, Terminals supporting TCP/IP protocols, their manufacturer and management and installation information must be evaluated for compliance with the requirements specified in this annexure.

### A.2 IP Protocols/Services Requirements

(a) The following requirements pertain to the data link (layer 2) and IP (layer 3) protocol suites:

    (i) the manufacturer provides specific 'best practices' for using the data link and IP layers to developers, integrators and end users;

    (ii) the manufacturer has exercised due diligence in ensuring that the above protocol suites do not contain known vulnerabilities.

(b) The following compliance statements relate to the security of the transport (layer 4) protocol suites (e.g., TCP, UDP) as a whole:

    (i) the Terminal manufacturer has clearly identified all the transport layer protocols present in the Terminal;

    (ii) the Terminal manufacturer has exercised 'due diligence' to ensure that the declared IP Protocols do not contain known vulnerabilities;

    (iii) specific best practices for using the declared transport layer protocols are covered in the security guidance made available to application developers, system integrators and end-users of the Terminal.

(c) The following compliance statements relate to the security protocols (e.g., SSL, IPSec, PPTP, PPP's LCP with CHAP, Radius or TACACS, or proprietary protocols) as a whole. Manufacturers must answer 'Yes' if at least one of the declared security protocols meets a particular requirement. Further, a specific configuration of each declared security protocol must be provided by the manufacturer:

    (i) the Terminal manufacturer has clearly identified all the security protocols present on the Terminal;

    (ii) the Terminal manufacturer has exercised 'due diligence' to ensure that the declared security protocols do not contain known vulnerabilities;

(iii)    specific best practices for using declared security protocols are covered in the security guidance made available to application developers, system integrators and end-users of the Terminal;

(iv)    the Terminal either encrypts, or enables the encryption of, all sensitive data sent over a network connection and uses a session key for that purpose;

(v)    session keys are established in a secure manner, using appropriate key management procedures, such as those listed in AS 2805.6 series;

(vi)    to ensure the confidentiality of sensitive data, the Terminal supports 3DES and/or AES as encryption algorithms to be used by financial applications;

(vii)    the length of symmetric (secret) keys used in the Terminal is at least 112 bits;

(viii)    before encrypting data, the Terminal generates a MAC or signed message digest that is used for message integrity checking, by the host system;

(ix)    the Terminal implements one of the secure SHA series for MAC or message digest computation; as used by financial applications: SHA-224, SHA-256, SHA-384, SHA-512 or AS 2805.4 compliant mechanisms;

(x)    the Terminal is able to authenticate the server based on a public key cryptographic method with the appropriate algorithm/key length, and uses either the RSA or DSS algorithms;

(xi)    when RSA or DSS algorithms are used, the length of the public keys used by the Terminal is at least 2048 bits;

(xii)    the Terminal is able to verify the authenticity of certificates it receives;

(xiii)    the Terminal only contains those certificates necessary for its operation (i.e., no generic certificates);

(xiv)    the key management policy relating to cryptographic keys or certificates for the Terminal is documented;

(xv)    the lifetimes of keys associated with different types of use (e.g., session keys, software update authorization keys, etc.) are documented;

(xvi)    the random number generation process has been validated against NIST SP 800-22 or equivalent.

(d)     The following compliance statements relate to the security of (layer 7) network applications (e.g., DHCP, HTTP, FTP, TFTP, SMTP, SNMP, etc.,) as a whole:

    (i)     the Terminal manufacturer has clearly identified all of the network applications present on the Terminal in the Network Applications Declaration form;

    (ii)     the Terminal manufacturer has exercised 'due diligence' to ensure that the declared network applications do not contain known vulnerabilities;

    (iii)     specific best practices for using the available network applications are covered in the security guidance made available to application developers, system integrators and end-users of the Terminal;

    (iv)     the Terminal does not use IP addresses for the authentication of systems;

    (v)     where authentication is used for management access, the Terminal ensures the confidentiality of passwords by using an appropriate security protocol;

    (vi)     the Terminal keeps track of all connections and restricts the number of client sessions that can remain active on the Terminal to the minimum necessary number;

    (vii)     the Terminal sets time limits for sessions and ensures that sessions are not left unattended and active for longer than necessary;

    (viii)     the Terminal enforces authentication for connecting to network applications.

(e)     The following compliance statements relate to the security management of the Terminal:

    (i)     the manufacturer has put in place due change-control procedures;

    (ii)     the certified firmware is protected and stored in such a manner as to preclude unauthorised modification, e.g., by using dual control or standardised cryptographic authentication procedures;

    (iii)     the Terminal is assembled in a manner that ensures that the components used in the manufacturing process are those hardware and software components that were certified and that unauthorised substitutions have not been made;

    (iv)     production software that is loaded onto Terminals at the time of manufacture is transported, stored and used in a way that prevents unauthorised modifications and/or substitutions;

(v)    the software provider has provided assurance that all firmware and software and any updates have been certified as free from unauthorised modifications;

(vi)    the Terminal manufacturer has a vulnerability disclosure policy that addresses the timely distribution to platform users of information related to newly found vulnerabilities in the Terminal. This information includes both a clear identification of the vulnerability and the recommended mitigation;

(vii)    the Terminal manufacturer implements adequate mechanisms, procedures and documentation to ensure that required security patches are created, distributed and applied;

(viii)    the Terminal supports the validation of the integrity and origin of all application software and software updates;

(ix)    all manual Terminal security initialisation must be conducted under dual control and related evidence kept for audit.

### A.3    Financial Transaction Security Requirements

(a)    Support for financial message encipherment compliant to AS 2805.9 is provided; and

(b)    processing of customer PIN data at the Terminal is confined to secure cryptographic hardware that has been accredited by AusPayNet.

### A.4    Devices Running Multiple Applications

(a)    The Terminal application software must be secured against unauthorised changes or substitution using cryptographic mechanisms.

(b)    The Terminal shall authenticate all applications using cryptographic mechanisms.

**Next page is B.1**

| ANNEXURE B. PCI PLUS REQUIREMENTS |
|---|

| The requirements in the following table applies to Terminals submitted for evaluation under clause 3.1(a)(iv). |
|---|

Amended effective 21.11.16

| **B.1  PCI Plus Requirements for PCI PTS V3.x** |
|---|

Amended effective 20.8.18

| AS 2805 Requirement<br>References below are to requirements specified in Annexes A, B and D of AS 2805.14.2 or clauses of the IAC Code Set | All EFTPOS Terminals including those without a PED component and fully integrated UPTs | UPTs with external controller | ATMs |
|---|---|---|---|
| A3: to protect the important cryptographic keys that may not be held in the Encrypting PIN Pad (EPP) | No | No | Yes |
| A5: some physical protections for the outer casing | No | No | Yes |
| A5A: Use of non-standard components for the device | Yes | No | Yes |
| A6: tamper evidence (still important in those cases where tamper responsiveness can be defeated) | Yes | No | Yes |
| A9, A10 and A12: requirements which ensures device is safe from cold boot attack | No | No | Yes |
| A13 and A14: tamper responsive on non-EPP secure components | No | No | Yes |
| A16, A17 and A21: requirements associated with ensuring the application software and firmware are safe and, in the case of ATMs, requirements associated with ensuring the ATM processor driving the EPP (and other secure components) | Yes | No | Yes |
| A24-A27 and A30: requirements associated with ensuring the ATM/EPP is in a sensitive state when necessary | No | Yes | Yes |
| A29: If cryptographic keys are lost for any reason, e.g., a long-term absence of applied power, the device will enter a non-operational state | Yes | No | Yes |
| B2 and B16: protecting the path to the display to prevent misuse of prompts | No | No | Yes |
| B14, B19 and B20: multi-acquirer | Yes | No | No |
| D1 – D6: MACing | Yes | No | Yes |
| IAC Code Set Volume 4 clause 2.4.6: Privacy of communication complies with AS 2805.9 or any other privacy of communication standard approved by the Management Committee. | Yes | Yes | No |

The requirements in the following table applies to Terminals submitted for evaluation under clause 3.1(a)(iv).

Amended effective 21.11.16

### B.2 PCI Plus Requirements for PCI PTS V4.x and V5.x

Amended effective 3.7.17

| AS 2805 Requirement<br>References below are to requirements specified in Annexes A, B and D of AS 2805.14.2 or clauses of the IAC Code Set | All EFTPOS Terminals including those without a PED component and fully integrated UPTs | UPTs with external controller | ATMs |
|---|---|---|---|
| A3: to protect the important cryptographic keys that may not be held in the Encrypting PIN Pad (EPP) | No | No | Yes |
| A5: some physical protections for the outer casing | No | No | Yes |
| A5A: Use of non-standard components for the device | Yes | No | Yes |
| A6: tamper evidence (still important in those cases where tamper responsiveness can be defeated) | No | No | Yes |
| A17 ensuring the application software and firmware are safe and, in the case of ATMs, ensuring the ATM processor driving the EPP (and other secure components) are safe | Yes | No | Yes |
| A24-A27 and A30: requirements associated with ensuring the ATM/EPP is in a sensitive state when necessary | No | Yes | Yes |
| B2 and B16: protecting the path to the display to prevent misuse of prompts | No | No | Yes |
| B14, B19 and B20: multi-acquirer | Yes | No | No |
| D1, D4 and D5:: MACing | Yes | No | Yes |
| IAC Code Set Volume 4 clause 2.4.6: Privacy of communication complies with AS 2805.9 or any other privacy of communication standard approved by the Management Committee. | Yes | Yes | No |

**Next page is C.1**

## ANNEXURE C.     DEVICE EVALUATION FAQ

*[Informative]*

This FAQ provides answers to questions regarding Australian Payments Network's physical and logical device security requirements and evaluation methodologies as specified in the IAC Code Set.

In so far as it is possible, the terminology used in this Q&A has been aligned with that used in PCI documents, however it needs to be clearly understood that the IAC process is significantly different to the PCI process.

## GENERAL

### C.1     Who is Australian Payments Network Limited (AusPayNet)?

AusPayNet is the payment systems self-regulator which works collaboratively with members, government, regulators and other stakeholders to improve the Australian payments system through:

*Amended effective 1.7.19*

- enabling competition and innovation;

- promoting efficiency; and

- controlling systemic risk.

By doing this, we engender confidence in the Australian payments system and advance the common interest of our members and the interests of the Australian public.

### C.2     Why is there an Australian specific device approval process?

The IAC device security standards are aligned with current Australian and/or international standards.  In some cases the Australian standards are closely aligned with ISO standards, however in many cases there are material differences (see C.26 for further detail).  The Australian device approval process recognises those differences.  In aligning our requirements in this manner we ensure that we are applying national and international best practice in a fair and transparent manner.

The card schemes' approval system (PCI) currently covers Point of Interaction (POI), EPPs, HSMs (otherwise referred to as SCM devices), Key Loading Devices and SPoC Solutions and CPoC Solutions.  In IAC, all devices involved in the initialization of Card-based transaction, i.e. Terminals, PIN handling and/or cryptographic key management are required to be tested and approved.  Other significant differences include the evaluation of security-related application software, mandatory MACing of both request and response messages (PCI has no such mandates), required support of the Australian key-management protocols AS 2805.6.4, 6.2 and 6.7 and the prohibition of fixed-key key management.

*Last amended effective 1.7.20*

**C.3**     **How does the PCI-Software-based PIN on COTS (SPoC) and the PCI Contactless Payments on COTS (CPOC) approval process work within the IAC?**     <sub>Amended effective 1.7.20</sub>

The Device Approval Process, depicted in Figure 1, outlines the standard Australian device approval flow.  A standard device is one which meets the device requirements set out in Volume 4 of the IAC Code Set.

**SPoC**

PCI-SCC released a standard and approval process in January 2018 for SPoC Solutions.  AusPayNet require that SPoC Solutions must be certified by PCI. Australian specific requirements are enforced, see (https://www.auspaynet.com.au/resources/cards-and-devices).  The SPoC Solution approval process is outlined as part of the IAC Code Set Volume 4, Annexure G.

*Note:*     *For purposes of clarity be aware that transactions originating from magnetic stripe data are **NOT** accepted via SPoC Solutions in Australia.  Any SPoC Solution which includes magnetic stripe functionality is prohibited from implementing that functionality in Australia and any SCRP which include magnetic strip readers will **NOT** be approved.*

**CPoC**

PCI-SCC released a standard and approval process in December 2019 for CPoC Solutions.  AusPayNet require that CPoC Solutions must be certified by PCI.     Australian specific requirements are enforced, see https://www.auspaynet.com.au/resources/cards-and-devices.     The CPoC Solution approval process is outlined as part of the IAC Code Set Volume 4, Annexure G.

**C.4**     **How are approved PCI-SPoC Solutions and CPoC Solutions listed?**     <sub>Amended effective 1.7.20</sub>

**SPoC Solution**

A PCI-SPoC Solution has four parts: The mobile (COTS) device, the secure card reader (SRCP), the PIN CVM Application and the Backend Monitoring System. The four components are listed as a single solution.  Having a solution that has only an approved SCRP component does not mean that the solution is approved. All elements of a solution are evaluated in combination, not as separate components.

**CPoC Solution**

A PCI-CPoC Solution has three parts: The mobile (COTS) device, the Card acceptance COTS Application and the Backend Monitoring System.  The three components are listed as a single solution. All elements of a solution are evaluated in combination, not as separate components.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

**C.5**     **What are non-standard technologies?**     <span style="font-size:small">Inserted effective 1.7.19</span>

Innovation and rapid changes in technology drive the development of payment solutions that do not fit within the paradigm of traditional security standards. In this sense, conventional technologies have existing requirements and approval processes in place. When new technologies cannot be assessed against the current standards and compliance programs, then they may be deemed a non-standard technology.

**C.6**     **What is the process for assessing non-standard technologies in the IAC?**     <span style="font-size:small">Inserted effective 1.7.19</span>

IAC Code Set Volume 4, Annexure G, Schedule 1 outlines a process for the consideration of non-standard technologies at the point of interaction and includes an initial assessment checklist which an Acquirer must complete to initiate an evaluation. The assessment is divided into 6 stages, namely the Request, Identification, Technical Examination, Assessment, Pilot and Decision phase.

## Figure 1: Device Approval Process

Amended
effective
1.1.19



Submission of Device (new or modified ATM, EFTPOS Terminal, SCM, etc)

Device Submitted by Applicant

**Abbrevations**
**AEF: Approved Evaluation Facility**
**ERSC: Evaluation Review Sub-Committee**

Evaluation by an (AEF)

Evaluation Report

Further Clarification Needed

Initial review by AusPayNet

Delta with only minor changes to security

New Device or Delta with significant changes to security

Delegation by AusPayNet under delegated authority

Evaluation Report reviewed by an ERSC

No (Device does not meet requirements)

Yes (Device meets requirements)

Application notified of unacceptable results

Letter of Approval sent to Applicant

Decision by AusPayNet

No (Device does not meet requirements)

Yes (Device meets requirements)

Application notified of unacceptable results

Letter of Approval sent to Applicant

Approval period remains that of originally approved device

Approval period of 3 years

Device added to Approved Devices on AusPayNet website

Device continues to meet approval criteria

Letter of Renewal sent to Applicant (Approval period extended by 3 years)

**C.7**      **Which EFTPOS Terminals require approval for use within IAC?**

Within IAC all services associated with the handling and management of Cardholder PINs and all cryptographic processes within financial Terminals must be performed within a device that meets the requirements of a physically secure cryptographic device. These requirements are defined in ISO 13491-1 for devices employing master/session key or DUKPT key management. The checklists used by Approved Evaluation Facilities (AEFs) in evaluating devices for conformance with these security requirements are specified in AS 2805.14.2 or ISO 13491.2.

Specifically all those components of a financial Terminal that are involved in requesting, collecting and processing of Cardholder PINs and card details are required to meet the requirements of a Secure Cryptographic Device (ref clause 2.4.3 of the IAC Code Set, Volume 4).

This definition may be viewed as illustrated in Figure 1 - SCD & EFTPOS (Financial) Terminal Relationship – Type 1.

Cardholder activated EFTPOS Terminals contain (where present), the PED (keypad), display, magnetic stripe reader (MSR), Integrated Circuit Card (ICC) reader, cryptographic processor and the prompt presentment logic all of which must be contained within a container, as illustrated in figure 1, meeting the requirements of a Secure Cryptographic Device. Where the Acquirer Application has access to clear text keys used to protect either the PIN or the Transaction or controls the presentation prompts for PIN entry, it too must be assessed within the SCD container, see Figure 3 – SCD & EFTPOS (Financial) Terminal Relationship – Type 2. It is possible for a vendor to produce a device where all the components of Figure 1 are within the SCD container.

Approved Evaluation Facilities (AEFs) will evaluate devices for adherence to these requirements using the mechanisms and checklists from AS 2805.14.2. Note that this standard is identical to ISO 13491 part 2:2005.

**C.8**      **What is a PED and what is an EFTPOS Terminal?**

"PIN Entry Device" and "PED" means an optional component of a Terminal which provides for the secure entry and encryption of PINs in processing a Transaction.

"EFTPOS Terminal" means a whole approved device which provides for the secure processing and completion of a Transaction, including the secure entry and encryption of PINs when a PED is present.

For the purposes of the security evaluation the target of evaluation includes all those components associated with the collection and processing of cardholder PINs and card details. This includes where present, the PED, the magnetic stripe reader (MSR), ICC reader, display, prompt storage and presentment logic.

---

Where an EFTPOS Terminal has no PED component it must also not include a magnetic stripe reader (MSR) component and therefore the security requirements related to those components are excluded from the security evaluation. Such devices would only ever process transactions which are either contact or contactless EMV transactions, and would not support the entry of a cardholder's PIN.

*Inserted effective 1.1.20*

### C.9 Which device types are included?

The IAC Rules classify financial Terminals into two broad categories, namely Electronic Funds Transfer Point of Sale (EFTPOS) Terminals and Automatic Teller Machines (ATMs). Additional device types requiring approval include Encrypting PIN Pads (EPPs), host security modules (HSMs), alternatively known as Security Control Modules (SCMs), SPoC Solutions, CPoC Solutions and Key Loading and Transfer Devices (KL/TDs).

*Last amended effective 1.7.20*

IAC device approval can only be granted to complete functioning devices; for financial Terminals this includes where present, the PED, the magnetic stripe reader, ICC reader display and any software involved in PIN security, such as PIN acceptance and handling, cryptographic processes and key management.

*Amended effective 20.8.18*

To assist vendors of encrypting PIN pads (EPPs), devices meeting an appropriate subset of the device security requirements from AS 2805.14.2, will be identified as such on AusPayNet's approved device list. Such listing will not remove the need to obtain device approval for any device that includes the approved EPP as a component; however, by using an already approved EPP, the amount of additional effort required to obtain device approval for the full financial Terminal may be significantly reduced.

Vendors seeking to utilise listed approved EPPs as a component of a new submission must check the EPPs deployment conditions to ensure that the EPP does not have a date listed beyond which it will no longer be accepted as a supported component in the submission for approval of a new device.

*Inserted effective 21.11.16*

### C.10 Unattended Payment Terminals

An Unattended Payment Terminal (UPT) is a financial Terminal, other than an ATM, conforming to the requirements of an SCD that is intended for deployment in an environment not under the constant oversight of the merchant.

UPTs must provide strong deterrence against penetration of their outer shell to protect the individual security related components.

A UPT is currently treated as an EFTPOS Terminal within the IAC Rules.

*Amended effective 29.4.16*

### C.11     How are EFTPOS Terminal approvals classified?

Approval for EFTPOS Terminal types is granted under two categories, Type-1 and Type-2 depending on the level of security functionality provided by the acquirer or end-user application, as described below.  The purpose of assigning these classifications is as an aid for acquirers in determining when re-approval is required as a consequence of changes to the device application.  Please note, these classifications are different from the PCI classifications of POS-A and POS-B.

#### Type-1:

This classification is given to EFTPOS Terminal devices that have no security functionality provided by the acquirer and end-user applications.  This includes the fact that the data-collection prompt presentment cannot be altered by these applications.  To be granted a Type-1 classification, the device must have met all of the applicable security criteria, the end-user must be unable (by device design and construction) to modify the device's data-collection prompts, firmware and cryptographic functions, and only the manufacturer has the capability to modify the prompts and controls for PIN entry.  The mechanisms and controls used to install or modify these sensitive functions and prompts must be distinct from the mechanisms used to control the modification and installation of the acquirer application.  See Figure 2 of this Manual for a diagrammatic representation of a Type-1 device.  Devices meeting the Type-1 specification do not require individual approval for the Acquirer application.
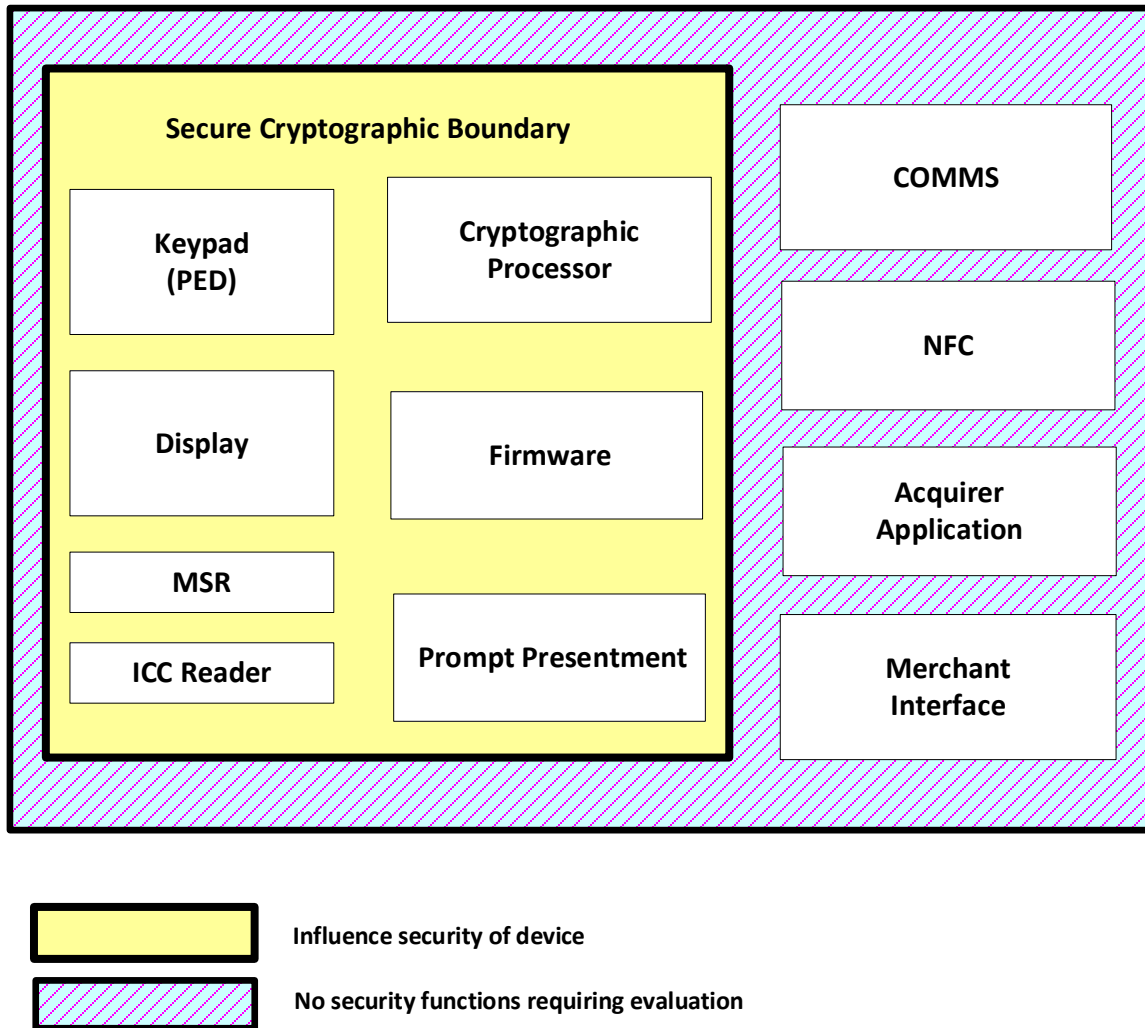
Figure 2 SCD & EFTPOS (financial)Terminal Relationship – Type 1

### Type-2:

This classification is given to EFTPOS Terminal devices where, unlike for Type-1 devices, the end user application can provide some security functionality such as through having un-moderated access to the display and keyboard. This classification includes Point of Sale devices where there are multiple end user applications, including non-payment applications, which have unmodulated access to the display and keyboard. Non-payment applications must be prevented from accessing any payment application and its associated data (especially PINs and cryptographic keys).

## Financial Terminal

Last amended
effective 1.7.19
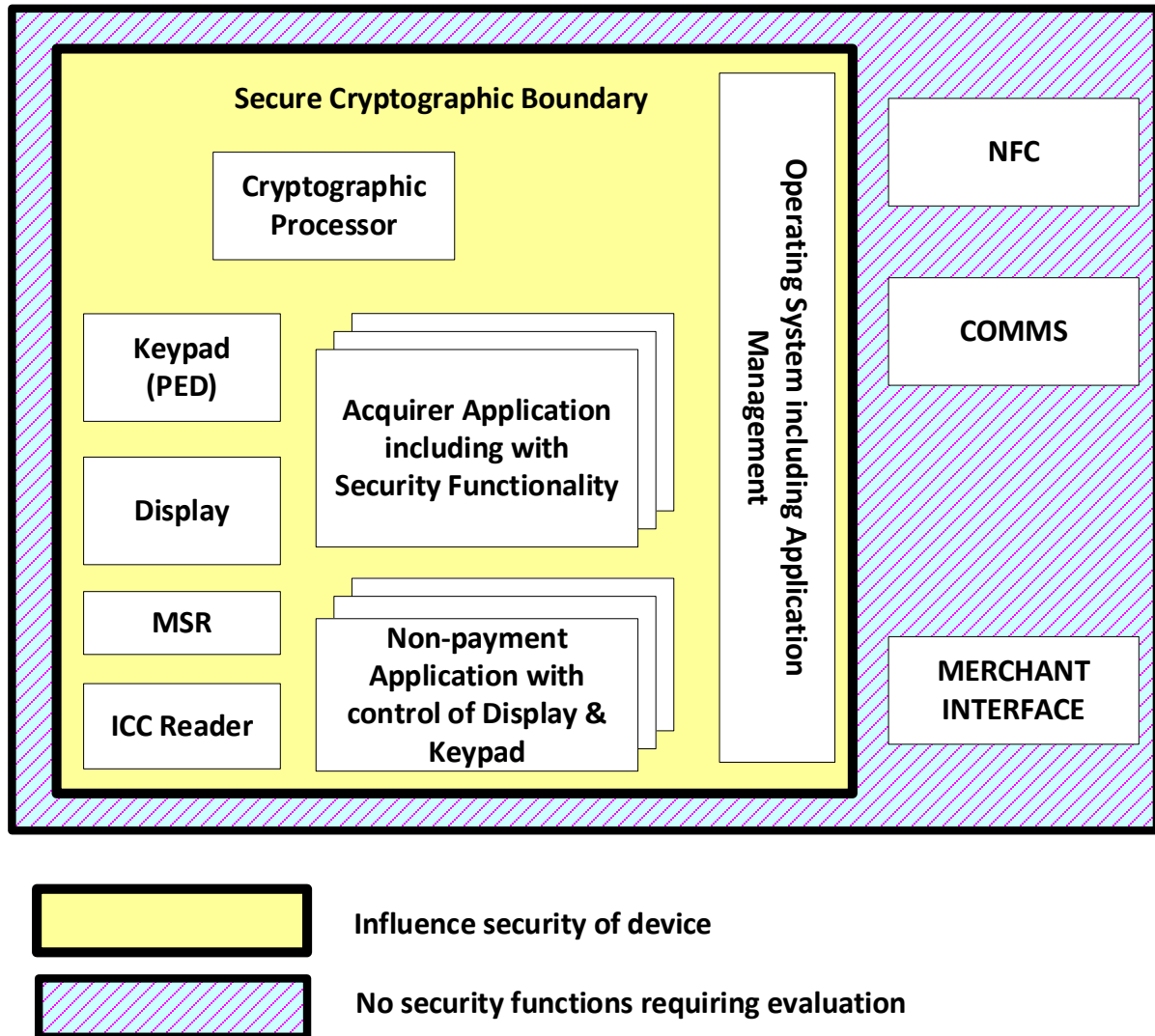


**Figure 3: SCD & EFTPOS (Financial) Terminal Relationship – Type 2**

To be granted a Type-2 classification, the device must have met all of the applicable security criteria and the manufacturer must be capable of shipping the device with mechanisms in place for controlling the display and its use. These mechanisms can be employed to unlock the device, using proper cryptographically controlled processes, to allow the Acquirer to update the prompts. The Acquirer application would typically have un-moderated access to the device's display, keyboard and prompts. As prompt presentment is part of the Acquirer application, devices meeting the Type-2 specifications require individual approval for each different Acquirer application to be deployed. Updates to approved Acquirer applications will only require further approval as described in Question 9 below.

Additionally, where the device is capable of running multiple applications, including non-payment applications, the manufacturer must be capable of shipping the device with cryptographic mechanisms in place for controlling the deployment of all applications running on the device.

Non-payment applications must be subject to a cryptographic mechanism which authenticates and authorises each application before each execution on the device. The details of these mechanisms must be addressed in the device evaluation report.

Non-payment applications require individual evaluation and authorisation by the Acquirer, or a party explicitly trusted by the Acquirer, for each application to be deployed or updated.

**C.12   Can the EFTPOS Terminal hardware be approved for use without an application?**

Amended
effective 20.8.18

Only a complete functioning Terminal can be approved for deployment under the IAC Code Set. If an application is required to perform transactions, then an application must be part of the approved Terminal. The Terminal will be identified on the Approved Device Lists by hardware, firmware and application identifiers.

Last amended
effective 20.8.18

EFTPOS Terminals achieving a type 1 classification do not require re-approval if deployed with other Acquirer applications than that listed. Type 2 EFTPOS Terminal devices require re-evaluation (delta evaluation) and approval for each unique instance of the Acquirer application.

Last amended
effective 20.8.18

**C.13   Component Approval**

Where a device consists of a number of components, each individually meeting the requirements for a secure cryptographic device, and intended for use where the inter-connections between the components provide the necessary level of either physical and/or logical protection, then such devices may be individually evaluated and listed in the approved device lists.

Irrespective of whether all individual components making up a financial Terminal are themselves approved, an evaluation-report and approval of the complete device is still necessary before deployment within IAC. Such a final evaluation need not re-examine approved components.

Where the individual components of a device host public keys or PIN-security related cryptographic keys, and/or key components and residues, then the device component must be evaluated against those values of "Not Feasible" (clause 2.3.1 of the IAC Code Set, Volume 4) required protecting for attacks against keys as well as the device component specific requirements.

Amended
effective 29.4.16

### C.14 Can a device's hardware be approved separately?

Hardware only evaluations can be accommodated and devices so approved will be listed, suitably annotated in the approved device lists. However, only fully approved, complete devices can be deployed within IAC. As complex interactions can occur between the hardware and software, an evaluation report covering the entire device (hardware and software) will be required before full approval is given.

### C.15 Do changes to the Acquirer application require re-approval?

For type 1 EFTPOS Terminals, no change to the Acquirer application can affect the security components so re-approval is not required.

*Last amended effective 20.8.18*

For type 2 EFTPOS Terminals, any changes to the device's cryptographic processes, PIN handling (including cardholder prompts relating to security data collection), and cryptographic key management will require re-evaluation and re-approval. The evaluation may not need to be a complete review but go only to the changes and any consequential effects (i.e., a delta evaluation). The determination, as to the areas impacted by a change, is the responsibility of the Acquiring Member supported by advice from the equipment vendor. It is a requirement of IAC that only devices meeting the IAC security requirements be deployed within the system.

*Last amended effective 20.8.18*

New non-payment applications or updates to existing non-payment applications are required to be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer, and must be authenticated by the same cryptographic mechanism that was part of the device approval.

All **ATM payment applications** other than those identified as approved payment applications on the AusPayNet approved devices list are required to be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer, and must be authenticated by the same cryptographic mechanism that was part of the original device approval. AusPayNet approval of an ATM payment application is applicable to only the specific device with which it is listed, that is approved ATM payment applications are not transferable to other ATM types and/or models.

*Inserted effective 20.8.18*

ATM certification includes the requirement that a payment application be approved for use prior to deployment. If an Acquirer wishes to deploy an ATM payment application not listed as approved for that ATM model on the Approved Devices List then that application must be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer by the same cryptographic mechanism that was part of the original device approval, prior to being deployed.

*Inserted effective 1.7.19*

Additionally, any update or modifications to the payment application must also be re-evaluated and authorised prior to deployment. AusPayNet approval of an ATM payment application applies to only the specific device with which it is listed, that is approved ATM payment applications are not transferable to other ATM types and models.

*Inserted effective 1.7.19*

---

**C.16    Do changes to the device's hardware require re-approval?**

Any changes to a device's physical characteristics that impact on its security features including protection mechanisms, PIN handling (including prompt presentment relating to security data collection), cryptographic processing and cryptographic key storage require re-examination and re-approval. The determination, as to the areas impacted by a change, is the responsibility of the Acquiring Member supported by advice from the equipment vendor. It is a requirement of IAC that only devices meeting the IAC security requirements be deployed within the system.

**C.17    How strong must tamper evidence be?**

Because merchants and cardholders are not trained to identify tamper-evidence and it is not expected that there will be frequent inspections by qualified inspectors, any tamper-evidence must be very effective. The typical uninformed cardholder and merchant must recognise that the device has been tampered with. This means damage that is ambiguous or can be hidden, or the use of tamper-evident seals are not sufficient. No device can be approved relying solely on tamper evidence for protection, (ISO 9564-1)

*Last amended effective1.7.19*

**C.18    When is an "N/A" response to a requirement acceptable?**

An "N/A" response is acceptable in three cases: first, if compliance is achieved by meeting another requirement option, such as meeting B2, but not B18; second, if the characteristics governed by the requirement are absent in the EFTPOS Terminal, (such as requirement B4 if the EFTPOS Terminal does not emit any audible tones); and last where a requirement relates to device management tasks which are the responsibility of the Acquirer. The evaluation laboratory must verify that all responses are appropriate.

*Last amended effective 1.7.19*

**C.19    What is required to adequately identify a device?**

EFTPOS Terminals submitted for testing must be properly identified so that AusPayNet Members can be certain of acquiring a Terminal that has been approved by AusPayNet. The EFTPOS Terminal Identifier is used by AusPayNet to denote all relevant information, consisting of the: Make (manufacturer), Model Name, Hardware Identifier and Version, Firmware Identifier and Version, and, if applicable, Application Identifier and Version. In order to ensure that the EFTPOS Terminal has been approved, Acquiring Members are advised to purchase and deploy only those Terminal models with the information that matches exactly the designations given in the components of the EFTPOS Terminal Identifier. (This is subject to the qualifications described in Question 12 and Question 13.)

*Last amended effective 20.8.18*

For self-certification purposes, the Acquirer's auditor must be able to confirm the device identification. This necessitates the use of tamper-proof labels and/or device functionality capable of displaying the relevant data for examination and confirmation.

Example of an EFTPOS Terminal Identifier (four components):

| | |
|---|---|
| Terminal Manufacturer: | Acme |
| Terminal Model Name: | PIN Pad 600 |
| Hardware Identifier & Version: | 600-NN-421-000-AB |
| Firmware Identifier & version: | NOS-FW ver. 1.01 |
| Application Identifier & Version: | AusPayNet 4.53 |

### Hardware Identifier

The Hardware Identifier represents the specific Hardware component set used in the approved EFTPOS Terminal. The fields that make up the Hardware identifier may consist of a combination of fixed and variable alphanumeric characters. A lower case "x" is used by AusPayNet to designate all variable fields. The "x" represents fields in the Hardware identifier that the vendor can change at any time to denote a different EFTPOS Terminal configuration, such as country usage code, customer code, language, device colour. The AEF has assessed the "x" field(s) as to not impact EFTPOS Terminal's security requirements or the device's approval. To ensure that the EFTPOS Terminal has been approved, Acquiring Members are advised to purchase and deploy only those EFTPOS Terminals with the Hardware Identifier whose fixed alphanumeric characters match exactly the Hardware identifier depicted on the Approval List or the vendor's approval letter from AusPayNet. (This is subject to the qualifications described in Question 13.)

Examples on the use of Hardware Identifier:

| Listed Hardware Identifier | Comments |
|---|---|
| NN-421-000-AB | Hardware identifier NN-421-000-AB of the Device Identifier does not employ the use of the variable "x." Hence, the EFTPOS Terminal being deployed must match the Hardware identifier exactly in order for the device to be considered an approved EFTPOS Terminal (Hardware component). |
| NN-4x1-0x0-Ax | Hardware identifier NN-4x1-0x0-Ax of the Device Identifier does employ the use of the variable "x." Hence, the EFTPOS Terminal being deployed must match the Hardware Identifier exactly in only those position(s) where there is no "x." |
| Vendor Hardware Identifier | Comments |
| NN-421-090-AC | If the Approved Device List lists NN-421-000-AB as the Hardware identifier in the Device Identifier, then the EFTPOS Terminal with the Hardware identifier NN-421-090-AC cannot be considered an approved device (Hardware component). However, if the IAC List of Approved Devices lists NN-4x1-0x0-Ax as the Hardware Identifier in the PED Identifier, then the Terminal with Hardware Identifier NN-421-090-AC can be considered an approved Terminal (Hardware component) |
| NN-421-090-YC | If the Approved Device List lists NN-4x1-0x0-Ax as the Hardware identifier in the Device Identifier, then the EFTPOS Terminal with the Hardware identifier NN-421-090-YC cannot be considered an approved Terminal (Hardware component). |

Last amended effective 20.8.18

The EFTPOS Terminal Identifier will be included in the approval letter and on the IAC List of Approved Devices. If an identical EFTPOS PED is used across a family of devices, vendors are cautioned against using a Hardware Version Number that may restrict approval only to that EFTPOS Terminal model.

Last amended effective 20.8.18

### C.20    What is classified as firmware?

For the purposes of the security evaluation, all EFTPOS Terminal software that is fixed and unchangeable across differing Acquirer payment applications is considered firmware.

Last amended effective 20.8.18

This includes boot loaders, operating systems and in most cases cryptographic libraries. As noted in Question 8, the controls over the loading and/or modification of Firmware must be distinct from those used to control end-user application loading. Where cryptographic controls are employed the mechanism must be such as to ensure that only the equipment manufacturer has the ability to authorize and implement firmware changes. Firmware must be fully identified by name/number and version information. Changes in firmware that impact the security of a device require re-examination and separate approval.

AEF's should particularly note that this definition is not the same as that used in the PCI approval process, which classifies, as firmware any code within a device that provides security protections needed to comply with the PCI PTS device security requirements or can impact compliance to those security requirements, including code necessary to meet PCI PTS Core, OP or SRED security requirements.

**C.21    Which Message Authentication Methods are acceptable?**

The only acceptable methods of MAC generation are those contained within AS 2805.4, which currently consists of two parts. Part 4.1 addresses methods using a block cipher and part 4.2 addresses methods using hash functions. It is important to note that only one block cipher algorithm, MAC algorithm 1, is specified consisting of a full triple-DES encryption of the message. MAC algorithm 3, commonly known as the ANSI Retail MAC as specified in ANSI X9.19, may only be used when the entire process, including the key decomposition, is executed within the confines of a Secure Cryptographic Device from which no intermediate results are ever released. Approved Evaluation Facilities should monitor activity within Standards Australia for changes in this area.

**C.22    Which Terminal key management schemes are acceptable?**

Terminal key-management schemes acceptable to IAC are those specified in the sub-parts of AS 2805.6, namely transaction key management conformant to AS 2805.6.2 or master/session key management conformant to AS 2805.6.4. or Derived Unique Key Per Transaction key management conformant to AS 2805.6.7.

Importantly, fixed key is not currently acceptable for use with IAC. Approved Evaluation Facilities should monitor activity within AusPayNet for changes in this area. However individual acquirers may request specific permission to use other key-management schemes (e.g., ATMs) from the IAC Management Committee. Question 20 provides further guidance on the requirements for the approval of a Terminal key management scheme.

**C.23    Terminal Key Management approval requirements**

IAC requires that all key-management comply with AS 2805.6.1 (similar to ISO 11568-1).  Additionally, for Terminals, it requires master/session or transaction key-management that complies with one of the Australian standards AS 2805 parts 6.2, 6.4 or 6.7, or alternatively with other approved mechanisms.  IAC also provides for the approval of other key-management mechanisms. <span style="font-size:small">Amended effective 29.4.16</span>

The following minimum requirements will be used by AusPayNet in evaluating the suitability of Terminal key-management mechanisms.  These are in addition to the key-management principles contained in the various parts of ISO 11568. <span style="font-size:small">Amended effective 1.7.19</span>

(a)    Minimum symmetric key size and algorithm

   (i)    PIN encipherment must use DEA-3 with either a 128 or 192-bit key length (clause 4.4.2 of the IAC Code Set, Volume 4). <span style="font-size:small">Amended effective 29.4.16</span>

   (ii)    Message Authentication must be achieved by using either of the MAC algorithms from AS 2805.4.1 using a 128-bit key length (clause 4.5.1(f) of the IAC Code Set, Volume 4). <span style="font-size:small">Amended effective 29.4.16</span>

   (iii)    Message encipherment must use DEA-3 with either a 128 or 192-bit key length (clause 4.4.2 of the IAC Code Set, Volume 4). <span style="font-size:small">Amended effective 29.4.16</span>

(b)    Minimum asymmetric key size and algorithms

   (i)    Only DEA-2 is approved for use within IAC.

   (ii)    In accordance with clause 4.2.2 of the IAC Code Set, Volume 4, the minimum size for DEA-2 keys is 2048-bits.  This key-size requirement may be waived for EMV compliant Terminals, where the requirements of EMV must apply. <span style="font-size:small">Amended effective 29.4.16</span>

(c)    Key encipherment

A key used to protect other keys must offer the equivalent or greater cryptographic strength to the key it is protecting.

(d)    Message encipherment

As message encipherment, conformant to AS 2805.9, is required for EFTPOS Terminals after January 2009, the key-management mechanism must provide for a data-protection key. <span style="font-size:small">Last amended effective 20.8.18</span>

(e)    Message Authentication

Bi-directional message authentication is mandatory using an approved MAC algorithm from AS 2805.4.1.

(f)     Session key backtracking

Any session based key-management scheme must be designed to make backtracking of key enciphering keys as difficult as exhaustive key determination.

(g)     Master key roll-over

A mechanism for updating the top-level symmetric key should be provided where a unique key per transaction mechanism is not used.    This mechanism needs to ensure that the requirement for the non-disclosure of future keys is met.

(h)     Session key roll-over

A mechanism that provides for the regular updating of session keys is required.

(i)     Key separation

Either variants or key-tags are acceptable mechanisms for providing key-separation.  It is preferable that distinct keys be used for each direction of communications.

(j)     Remote Terminal initialization (if supported)

The IAC requirements for remote Terminal initialization are those in AS 2805.6.5.2 (symmetric) and AS 2805.6.5.3 (asymmetric) and ANSI X9.24 Part 2 (asymmetric).  Other mechanisms may be approved, provided the basic principles of AS 2805.6.5.1 are met.

As ATM's do not typically support either of the approved Terminal key managed mechanisms, evaluation reports covering ATM devices should contain full details of the device's key-management including initialization and key-change to enable its evaluation.

**C.24     What support is required for privacy of communications?**

For EFTPOS Terminals, the AEF is required to confirm that the device can support data encryption in line with the requirements of AS 2805.9.   The management of the key(s) used for data encryption must comply with AS 2805.6.1.

All application level data elements, including but not limited to fields P-45 (Track 1 data) and P-35 (Track 2 data), as defined in AS 2805.2, must be protected except those fields necessary to indicate the origin of the transaction and information required to correctly reconstruct the message.   The latter may include the data required to derive the privacy key.

Where the EFTPOS Terminal relies upon DUKPT for the management of keys for Privacy of Communications the device must conform to AS 2805.6.7 including the normative appendix, Appendix C.

*Amended effective 20.8.18*

### C.25 How should device evaluation reports be formatted?

The exact layout of evaluation reports is not particularly important; the device that is the subject of the report should be clearly and fully identified in the opening sections of the report.  In particular, complete identification of the physical device and all firmware and software is required.  Revision levels of all components should be clearly revealed.

The contents of the report must include:

(a)     The list of all pertinent documentation used in the evaluation;

(b)     A completed list of all successful or failed tests;

(c)     For failed tests, any compensating factors that mitigate the severity and/or impact of the non-compliance;

(d)     The name of the sponsor;

(e)     The name of the AEF;

(f)     The date of the evaluation;

(g)     Identification of the device (e.g., manufacturers name, model, revision, software version etc.);

(h)     Completed SCD checklists;

(i)     Advised deployment environment (as advised by the Sponsor);

(j)     Details of the examination and testing process followed in developing the report, and

(k)     An indication as to how the device meets the specification of "not-feasible" defined in clause 2.3.1 of the IAC Code Set, Volume 4.  Evidence should be given into the derivation of the cost and time calculations.

*Last amended effective 1.7.19*

**C.26    What is the relationship between Australian and ISO standards?**

For the purposes of an IAC evaluation, Australian standards take precedence over ISO or other national standards bodies or PCI-SSC.  This is particularly important when working with Australian Standards that are clones of ISO standards.  Examples include AS 2805.14 the text of which is identical to ISO 13491:2005.   In these cases, as referenced standards are not necessarily functionally equivalent, references within the body of the standard to other ISO standards should be replaced with the Australian standard equivalent.   For example all references to ISO 11568 should be replaced with AS 2805.6, similarly ISO 9807 is replaced with AS 2805.4.  It should not be assumed that all algorithms, process and procedures appearing in ISO standards have equivalents within Australian standards.  It should also not be assumed that the Australian standard is a replica of the latest version of an ISO standard as some significant delay can occur before a revision is adopted.

*Amended effective 1.7.19*

**C.27    What mode of operation, other than Output Feedback Mode (OFB) are allowed to use as part of message encipherment in AS 2805.9?**

*Inserted effective 1.7.19*

Both OFB and CBC mode of operation as specified in AS 2804 5.2 is allowed for message encipherment in AS 2805.9.

**C.28    Does Key Loading Devices which are compliant with PCI-PTS HSM V3 satisfy the IAC Code Set Requirements?**

*Inserted effective 1.7.19*

Yes, based on a gap analysis conducted by AusPayNet in 2016, the PCI-PTS HSM V3 requirements satisfy the IAC Code Set requirements for KLD's.

**C.29    Who may authorise non-payment applications on devices?**

*Inserted effective 1.7.19*

Acquirers are responsible for evaluating non-payment applications, and are required to maintain a register for the Annual Acquirer Audit as per Volume 1 – Acquirer Audit Part 1 (1.2(e)).

**C.30    Do the PCI-PTS HSM V3 satisfy the IAC Code Set Requirements for Acquiring?**

*Inserted effective 1.7.19*

The PCI+ approach for HSM is to certify compliance with Clause 2.4.10 of Volume 4 of the IAC Code Set which defines the limited set of functions allowable on an AusPayNet approved HSM plus any specific IAC Code requirements, such as the ability to disable support of single DES and Format 1 PIN Blocks.

---

## LOGICAL SECURITY CHARACTERISTICS

**C.31     Is source code evaluation necessary?**

To form a true opinion as to compliance with the logical security requirements it is necessary that all source code associated with security, cryptographic key-management and PIN handling including all display output (e.g., prompts) be reviewed by an AEF. This includes the acquirer application to the extent that the acquirer application and/or payment application hosted by the ATM controller, participates in security related functions including message authentication.

Exception is available for low level code such as boot loaders and operating systems where those systems are not providing security related functionality. See Question 25.

**C.32     What is acceptable practice regarding the use of diagnostic features in source code?**

The AS 2805.14.2 security characteristics A16, A18 and A21 impose requirements that ensure the absence of diagnostic and test features within the EFTPOS Terminal application that could be misused to reveal sensitive information. It is highly preferable that source code provided to an AEF for evaluation is free from such functions. <sub>Last amended effective 20.8.18</sub>

However, where the removal of the diagnostic code from the source code would impose significant difficulty for the manufacturer, then the presence of such code during an AEF evaluation is acceptable provided that:

(a)     all such code is conditionally compiled to ensure diagnostic features are not included in versions of the application used in production;

(b)     when debug features are enabled there is an unambiguous display of that fact that would be clearly evident to a cardholder or other user of that device; and

(c)     the manufacturer/software developer must impose auditable quality control processes covering the compilation and release of production level application code.

**C.33     Are vendor assertions acceptable in evaluating logical security?**

In the event that the inspection of a source code relating to logical security by an Approved Evaluation Facility (AEF) is not practical, any vendor assertions:

(a)     are acceptable but only for low level firmware such as boot loaders and operating systems; and

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(b)    must be accompanied by sufficient evidence to fully satisfy the AEF as to the veracity of assertions and must include:

(i)    sufficient documentation, including design specifications, Application Program Interfaces (APIs), etc., to confirm the assertion;

(ii)    evidence of the vendor's internal security review processes, and

(iii)    evidence of the vendor's quality assurance programs and processes; and

(c)    must be confirmed through full evaluation testing of affected, external APIs.

## DEVICE MANAGEMENT REQUIREMENTS A40 THROUGH A43 : (AS2805.14.2)

Amended effective 29.4.16

### C.34    How are these requirements to be evaluated?

It is sufficient for an AEF to obtain vendor assertions on these requirements and for the AEF to reasonably satisfy themselves that the evidence provided provides a high likelihood that the Manufacturer is capable of and does meet these device management requirements.  Such vendor assertions must be accompanied by sufficient evidence to fully satisfy the AEF as to the veracity of those assertions and must be accompanied by evidence of the vendor's quality control processes and programs.

## DEVICE MANAGEMENT REQUIREMENTS A44 THROUGH A52

### C.35    Are these requirements to be evaluated?

No, these requirements are an Acquirer responsibility and are the subject of other processes within IAC.  The correct response to these questions in a device evaluation report is Not Applicable.

## DEVICE MANAGEMENT REQUIREMENTS B23 THROUGH B26 (CLAUSE B3)

### C.36    Are these requirements to be evaluated?

No, these requirements are an Acquirer responsibility and are the subject of other processes within IAC.  The correct response to these requirements is Not Applicable.

---

## PERMISSIBLE DEVIATIONS

### C.37    Must a PED include a privacy shield?

Yes, under normal circumstances, in accordance with the relevant clauses of AS 2805.14.2, the device must provide a means to deter the visual observation of PIN values as they are being entered by the cardholder.  As an alternative, it is permissible for a device to rely on the external physical environment in which it is to be installed to provide such protection.

Such an alternative is only permissible where the manufacturer supplies rules and guidance as to how the visual observation is to be deterred by the installation environment of the PED.  These rules must be evaluated along with the device during the approval process and subsequently provided to all purchasers and prospective purchasers.

Amended effective 1.7.19

These rules and instructions provided by the manufacturer must clearly state that the acquirer must meet the implementation criteria.  These rules must be binding for any acquirers placing the PED into service.

### C.38    Which PIN Block formats are permitted for PEDs and SCMs use within IAC?

Clause 2.7 of the IAC Code Set, Volume 4, requires that PEDs may use any PIN Block format as defined in ISO9564.1:2017, except format 1 and that format 3 is preferred.  Therefore a device must support more than ISO PIN Block format 1 in order to be approved for use within IAC.

### C.39    May an Approved Evaluation Facility rely on the FIPS 140-2 certification when evaluating a Secure Cryptographic Module for use in a KIF?

Inserted effective 9.11.16

Yes, only where the device in question has been deployed prior to 1 January 2012 and where the device is no longer produced or supported by the original device vendor (i.e. it is past "end-of-life" for production).  The FIPS 140-2 certification, the device's security policy and the content of the original FIPS test report, which must be made available by the vendor, may be used by the AEF to inform the findings for the security requirements as required by clause 3.1 of the IAC Manual, Volume 4: Device Requirements and Cryptographic Management.

The evaluation report must clearly show the origin of the data considered in the report, whether it is generated from tests or observations performed by the AEF or whether it is sourced from the FIPS 140-2 documentation.  The AEF shall confirm that data sourced from a FIPS 140-2 report is fit for purpose when drawing conclusions as to the result for each security characteristic of the device.

**Next page is D.1**

## ANNEXURE D.     DEVICE APPROVAL PROCESS [DELETED]

Deleted effective
1.1.19

## Next page is E.1

## ANNEXURE E.    IAC LABORATORY ACCREDITATION CHECKLIST

This self-assessment questionnaire specifies the accreditation criteria that a laboratory must meet in order to become accredited to conduct SCD security testing to the Companies requirements. Labs approved by the Company according to these criteria are allowed to conduct testing of Secure Cryptographic Devices for conformance to the Companies SCD security requirements. The criteria were derived using the National Institute of Standards and Technology Handbook 150 as a basis.

### E.1    Organisation

Legal name of laboratory ownership: _____

(a)    The laboratory or the organisation of which it is part must be an entity that can be held legally responsible.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)    It is the responsibility of the laboratory to carry out its testing and calibration activities in such a way as to meet the requirements of this handbook and to satisfy the needs of the client, the regulatory authorities or organisations providing recognition.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)    The laboratory management system must cover work carried out in the laboratory's permanent facilities, at sites away from its permanent facilities, or in associated temporary or mobile facilities.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)    If the laboratory is part of an organisation performing activities other than testing and/or calibration, the responsibilities of key personnel in the organisation that have an involvement or influence on the testing and/or calibration activities of the laboratory must be defined in order to identify potential conflicts of interest.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:    Where a laboratory is part of a larger organisation, the organisational arrangements should be such that departments having conflicting interests, such as production, commercial marketing, or financing do not adversely influence the laboratory's compliance with the requirements of this handbook.*

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

*Note 2:*    *If the laboratory wishes to be recognized as a third-party laboratory, it should be able to demonstrate that it is impartial and that it and its personnel are free from any undue commercial, financial, and other pressures that might influence their technical judgment. The third-party testing or calibration laboratory should not engage in any activities that may endanger the trust in its independence of judgment and integrity in relation to its testing or calibration activities.*

(e)     The Laboratory must:

(i)     have managerial and technical personnel with the authority and resources needed to carry out their duties, to identify the occurrence of departures from the quality system or from the procedures for performing tests and/or calibrations, and to initiate actions to prevent or minimise such departures (see also E.12);

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(ii)     have arrangements to ensure that its management and personnel are free from any undue internal and external commercial, financial, and other pressures and influences that may adversely affect the quality of their work;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iii)     have policies and procedures to ensure the protection of its clients' confidential information and proprietary rights, including procedures for protecting the electronic storage and transmission of results;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iv)     have policies and procedures to avoid involvement in any activities that would diminish confidence in its competence, impartiality, judgment, or operational integrity;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(v)     define the organization and management structure of the laboratory, its place in any parent organization, and the relationships between quality management, technical operation, and support services;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(vi) specify the responsibility, authority, and interrelationships of all personnel who manage, perform, or verify work affecting the quality of the tests and/or calibrations;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii) provide adequate supervision of testing and calibration staff, including trainees, by persons familiar with methods and procedures, the purpose of each test and/or calibration, and the assessment of the test or calibration results;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii) have technical management who has overall responsibility for the technical operations and who will provide the resources needed to ensure the required quality of laboratory operations:

Name of Person: _____

Area of Responsibility: _____

Repeat as necessary: _____

(ix) appoint a member of the staff as quality manager (however named) who, irrespective of other duties and responsibilities, must have defined responsibility and authority for ensuring that the quality system is implemented and followed at all times. The quality manager must have direct access to the highest level of management at which decisions are made on laboratory policy or resources;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(x) appoint deputies for key managerial personnel (see note).

Name(s): _____

*Note:* *Individuals may have more than one function and it may be impractical to appoint deputies for every function.*

(f) Staff members must be knowledgeable in the following areas:

(i) General requirements of the test methods;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    Familiarity with classes of hardware platforms (for software-based cryptographic algorithms;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)    Voltage and temperature measurement (EFP/EFT);

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)    Computer security concepts;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v)    Finite state machine model analysis;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi)    Production grade, tamper evident, and tamper detection and response techniques;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii)    Software design specifications, including high-level languages and formal models;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii)    Key management techniques and concepts;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ix)    EMI/EMC techniques;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(x)    Cryptographic self-test techniques;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xi)    IAC-approved cryptographic algorithms;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xii)   Operating system concepts;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xiii)  Familiarity with cryptographic terminology and families of cryptographic algorithms; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xiv)   Familiarity with the Common Criteria (ISO/IEC 15408:2005).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

## E.2    Quality Systems

(a)    The laboratory must establish, implement, and maintain a quality system appropriate to the scope of its activities.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)    The laboratory must document its policies, systems, programs, procedures and instructions to the extent necessary to ensure the quality of the test and/or calibration results.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)    The system's documentation must be communicated to, understood by, available to, and implemented by the appropriate personnel.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)    The laboratory's quality system policies and objectives must be defined in a quality manual (however named).  The overall objectives must be documented in a quality policy statement, which must be issued under the authority of the chief executive.  It must include at least the following:

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(i)    the laboratory management's commitment to good professional practice and to the quality of its testing and calibration in servicing its clients;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(ii)    the management's statement of the laboratory's standard of service;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iii)    the objectives of the quality system;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iv)    a requirement that all personnel concerned with testing and calibration activities within the laboratory familiarize themselves with the quality documentation and implement the policies and procedures in their work; and

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(v)    the laboratory management's commitment to compliance with this Manual.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

*Note:    The quality policy statement should be concise and may include the requirement that tests and/or calibrations must always be carried out according to stated methods and clients' requirements.  When the test and/or calibration laboratory is part of a larger organization, some quality policy elements may be in other documents.*

(e)    The quality manual must include or make reference to the supporting procedures including technical procedures.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(f)     It must outline the structure of the documentation used in the quality system.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(g)     It must contain or reference procedures for software handling and integrity.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(h)     It must contain or reference procedures for maintaining records of Quality System activities.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(i)     The roles and responsibilities of technical management and the quality manager, including their responsibility for ensuring compliance with this handbook, must be defined in the quality manual.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

## E.3     Document Control

### E.3.1     General

(a)     The laboratory must establish and maintain procedures (internally generated or from external sources) to control all documents that form part of its quality system, such as regulations, standards, other normative documents, test and/or calibration methods, as well as drawings, software, specifications, instructions, and manuals.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:     In this context, "document" could be policy statements, procedures, specifications, calibration tables, charts, textbooks, posters, notices, memoranda, software, drawings, plans, and so forth.  These may be on various media, whether hard copy or electronic, and they may be digital, analog, photographic, or written.*

*Note 2:     The control of data related to testing and calibration is covered in E.14.4(j). The control of records is covered in E.9.*

### E.3.2 Approving and issuing documents

(a) All documents issued to personnel in the laboratory as part of the quality system must be reviewed and approved for use by authorised personnel before being issued.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b) A master list or an equivalent document control procedure identifying the current revision status and distribution of documents in the quality system must be established and be readily available to preclude the use of invalid and/or obsolete documents.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c) The procedure(s) adopted must ensure that:

(i) authorized editions of appropriate documents are available at all locations where operations essential to the effective functioning of the laboratory are performed;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii) documents are periodically reviewed and, where necessary, revised to ensure continuing suitability and compliance with applicable requirements;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii) invalid or obsolete documents are promptly removed from all points of issue or use, or otherwise ensured against unintended use;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv) obsolete documents retained for either legal or knowledge preservation purposes are suitably marked;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)     Quality system documents generated by the laboratory must be uniquely identified.  Such identification must include:

(i)     the date of issue and/or revision identification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)     page numbering;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)     the total number of pages or a mark to signify the end of the document; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)     the issuing authority or authorities.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

**E.3.3     Document Changes**

(a)     Changes to documents must be reviewed and approved by the same function that performed the original review unless specifically designated otherwise.  The designated personnel must have access to pertinent background information upon which to base their review and approval.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)     Where practicable, the altered or new text must be identified in the document or the appropriate attachments.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)     If the laboratory's documentation control system allows for amending documents by hand pending the reissue of the documents, the procedures and authorities for such amendments must be defined.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)     Amendments must be clearly marked, initialled, and dated.  A revised document must be formally reissued as soon as practicable.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(e)     Procedures must be established to describe how changes in documents maintained in computerised systems are made and controlled.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

**E.4        Reviewing requests, tenders, and contracts**

(a)     The laboratory must establish and maintain procedures for reviewing requests, tenders, and contracts.  The policies and procedures for these reviews leading to a contract for testing and/or calibration must ensure that:

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(i)      the requirements, including the methods to be used, are adequately defined, documented, and understood (see E.14.4(e)); and

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(ii)     the appropriate test and/or calibration method is selected and capable of meeting the clients' requirements (see E.14.4(e)).

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note 1:     The request, tender, and contract review should be conducted in a practical and efficient manner, and the effect of financial, legal, and time schedule aspects should be taken into account.  For internal clients, reviews of requests, tenders, and contracts can be performed in a simplified way.*

*Note 2:     The review of capability should establish that the laboratory possesses the necessary physical, personnel, and information resources, and that the laboratory's personnel have the skills and expertise necessary for performing the tests and/or calibrations in question.  The review may also encompass results of earlier participation in inter-laboratory comparisons or proficiency testing and/or the running of trial test or calibration programs using samples or items of known value to determine uncertainties of measurement, limits of detection, confidence limits, and so forth.*

*Note 3:     A contract may be any written or oral agreement to provide a client with testing and/or calibration services.*

(b)  Records of reviews, including any significant changes, must be maintained.  Records must also be maintained of pertinent discussions with a client relating to the client's requirements or the results of the work during the period of execution of the contract.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note:*        *For review of routine and other simple tasks, the date and the identification (for example, the initials) of the person in the laboratory responsible for carrying out the contracted work are considered adequate.  For repetitive routine tasks, the review need be made only at the initial inquiry stage or on granting of the contract for ongoing routine work performed under a general agreement with the client, provided that the client's requirements remain unchanged.  For new, complex, or advanced testing and/or calibration tasks, a more comprehensive record should be maintained.*

(c)  The review must also cover any work that is subcontracted by the laboratory.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(d)  The client must be informed of any deviation from the contract.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(e)  If a contract needs to be amended after work has commenced, the same contract review process must be repeated and any amendments must be communicated to all affected personnel.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

## E.5        Subcontracting tests and calibrations

(a)  When a laboratory subcontracts work whether because of unforeseen reasons (for example, workload, need for further expertise or temporary incapacity) or on a continuing basis (for example, through permanent subcontracting, agency or franchising arrangements), this work must be placed with a competent subcontractor.  A competent subcontractor is one that, for example, complies with this handbook for the work in question.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(b)   The laboratory must advise the client of the arrangement in writing and, when appropriate, gain the approval of the client, preferably in writing.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(c)   The laboratory is responsible to the client for the subcontractor's work, except in the case where the client or a regulatory authority specifies which subcontractor is to be used.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(d)   The laboratory must maintain a register of all subcontractors that it uses for tests and/or calibrations and a record of the evidence of compliance with this handbook for the work in question.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

## E.6   Service to the client

(a)   The laboratory must afford clients or their representatives, cooperation to clarify the client's request and to monitor the laboratory's performance in relation to the work performed, provided that the laboratory ensures confidentiality to other clients.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note 1:     Such cooperation may include:*

*a)   Providing the client or the client's representative reasonable access to relevant areas of the laboratory for the witnessing of tests and/or calibrations performed for the client; and*

*b)   Preparation, packaging, and dispatch of test and/or calibration items needed by the client for verification purposes.*

*Note 2:     Clients value the maintenance of good communication, advice and guidance in technical matters, and opinions and interpretations based on results.  Communication with the client, especially in large assignments, should be maintained throughout the work.  The laboratory should inform the client of any delays or major deviations in the performance of the tests and/or calibrations.*

*Note 3:     Laboratories are encouraged to obtain other feedback, both positive and negative, from their clients (for example, client surveys).  The feedback should be used to improve the quality system, testing and calibration activities, and client service.*

### E.7    Complaints

(a)    The laboratory must have a policy and procedure for resolving complaints received from clients or other parties.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(b)    Records must be maintained of all complaints and of the investigations and corrective actions taken by the laboratory (see also E.9).

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

### E.8    Control of nonconforming testing and/or calibration work

(a)    The laboratory must have a policy and procedure that should be implemented when any aspect of its testing and/or calibration work, or the results of this work, do not conform to its own procedures or the agreed requirements of the client.  The policy and procedures must ensure that:

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(i)    the responsibilities and authorities for managing nonconforming work are designated and actions (including halting of work and withholding of test reports and calibration certificates, as necessary) are defined and taken when nonconforming work is identified;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(ii)    an evaluation of the significance of the nonconforming work is made;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(iii)    corrective actions are taken immediately, together with any decision about the acceptability of the nonconforming work;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(iv)    where necessary, the client is notified and work is recalled; and

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(v) the responsibility for authorising the resumption of work is defined.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note:       Identification of nonconforming work or problems with the quality system or with testing and/or calibration activities can occur at various places within the quality system and technical operations.  Examples are customer complaints, quality control, instrument calibration, checking of consumable materials, staff observations or supervision, test report and calibration certificate checking, management reviews and internal or external audits*

(b) Where the evaluation indicates that the nonconforming work could recur or that there is doubt about the laboratory's operations complying with its own policies and procedures, the corrective action procedures given in E.9 should be promptly followed.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

## E.9        Corrective action

### E.9.1        General

(a) The laboratory must establish a policy and procedure and must designate appropriate authorities for implementing corrective action when nonconforming work or departures from the policies and procedures in the quality system or technical operations have been identified.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note:       A problem with the quality system or with the technical operations of the laboratory may be identified through a variety of activities, such as control of nonconforming work, internal or external audits, management review, and feedback from clients or staff observations.*

### E.9.2        Cause analysis

(a) The procedure for corrective action must start with an investigation to determine the root cause or causes of the problem.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note:       Cause analysis is the key and sometimes the most difficult part in the corrective action procedure.  Often the root cause is not obvious, and thus a careful analysis of all potential causes of the problem is required.  Potential causes could include client requirements, the samples, sample specifications, methods and procedures, staff skills and training, consumables, or equipment and its calibration.*

---

**E.9.3    Selecting and implementing corrective actions**

(a)    Where corrective action is needed, the laboratory must identify potential corrective actions.  It must select and implement the action or actions most likely to eliminate the problem and to prevent recurrence.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)    Corrective actions must be to a degree appropriate to the magnitude and the risk of the problem.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)    The laboratory must document and implement any required changes resulting from corrective action investigations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

**E.9.4    Monitoring corrective actions**

(a)    The laboratory must monitor the results to ensure that the corrective actions taken have been effective.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

**E.9.5    Additional audits**

(a)    Where the identification of non-conformances or departures casts doubts on the laboratory's compliance with its own policies and procedures or on its compliance with this handbook, the laboratory must ensure that the appropriate areas of activity are audited according to E.12 as soon as possible.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:    Such additional audits often follow the implementation of the corrective actions to confirm their effectiveness.  An additional audit should be necessary only when a serious issue or risk to the business is identified.*

**E.10** **Preventive action**

(a) Needed improvements and potential sources of non-conformances, either technical or concerning the quality system, must be identified.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b) If preventive action is required, action plans must be developed, implemented, and monitored to reduce the likelihood of the occurrence of such non-conformances and to take advantage of the opportunities for improvement.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c) Procedures for preventive actions must include the initiation of such actions and application of controls to ensure that they are effective.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:* *Preventive action is a proactive process to identify opportunities for improvement rather than a reaction to the identification of problems or complaints.*

*Note 2:* *Apart from the review of the operational procedures; the preventive action might involve analysis of data, including trend and risk analyses and proficiency testing results.*

**E.11** **Controlling records**

**E.11.1** **General**

(a) The laboratory must establish and maintain procedures for identification, collection, indexing, access, filing, storage, maintenance, and disposal of quality and technical records. Quality records must include reports from internal audits and management reviews, as well as records of corrective and preventive actions.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b) All records must be legible and must be stored and retained in such a way that they are readily retrievable in facilities that provide a suitable environment to prevent damage or deterioration and to prevent loss.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)     Retention times of records must be established.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note:        Records may be in any media, such as hard copy or electronic media.*

(d)     All records must be held secure and in confidence.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(e)     The laboratory must have procedures to protect and back up records stored electronically and to prevent unauthorised access to or amendment of these records.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

### E.11.2     Technical records

(a)     The laboratory must retain records of original observations, derived data, and sufficient information to establish an audit trail, calibration records, staff records, and a copy of each test report or calibration certificate issued, for a defined period.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(b)     The records for each test or calibration must contain sufficient information to facilitate, if possible, identification of factors affecting the uncertainty and to enable the test or calibration to be repeated under conditions as close as possible to the original.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(c)     The records must include the identity of personnel responsible for the sampling, performance of each test and/or calibration, and checking of results.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note 1:        In certain fields it may be impossible or impracticable to retain records of all original observations.*

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

Note 2:     *Technical records are accumulations of data (see E.14.4(j)) and information that result from carrying out tests and/or calibrations and which indicate whether specified quality or process parameters are achieved. They may include forms, contracts, work sheets, workbooks, check sheets, work notes, control graphs, external and internal test reports and calibration certificates, clients' notes, papers, and feedback.*

(d)     Observations, data, and calculations must be recorded at the time they are made and must be identifiable to the specific task.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(e)     When mistakes occur in records, each mistake must be crossed out, not erased, made illegible or deleted, and the correct value entered alongside. All such alterations to records must be signed or initialled by the person making the correction.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(f)     In the case of records stored electronically, equivalent measures must be taken to avoid loss or change of original data.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(g)     Records covering the following are required:

(i)     Quality System;

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(ii)     Staff training dates and competency reviews;

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(iii)     Software versions and updates;

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(iv)     Test Equipment and instrument calibration (software documentation updates if applicable);

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(v)     Acceptance/rejection of modules submitted for test;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi)    Comprehensive logs for tracking samples and test activities;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii)   Problems with test systems and documentation for off-line until repair to restore status; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii)  Test data (including any diagrams, photos, and graphic images) and official reports.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(h)    Testing equipment or verification records should include, but are not limited to the following:

(i)     Equipment name or description;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    Model, style, serial number or other unique ID;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)   Manufacturer;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)    Date received and date placed in service;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v)     Current location, where appropriate;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi)  Condition when received (e.g., new, used, reconditioned);

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii)  Copy of manufacturer's instructions, where available;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii)  Notation of all equipment variables requiring verification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ix)  The range of verification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(x)  The resolution of the instrument and its allowable error;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xi)  Date of next calibration and/or verification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xii)  Date and result of last calibration and/or verification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xiii)  Details of maintenance carried out to date and planned for the future;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xiv)  History of any damage, malfunction, modification or repair;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xv)  Identity of the laboratory individual or external service responsible for calibration; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xvi)  Source of reference standard and traceability.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

### E.12    Internal audits

(a)    According to a predetermined schedule and procedure, the laboratory must periodically conduct internal audits of its activities to verify that its operations continue to comply with the requirements of the quality system and this handbook.  The internal audit program must address all elements of the quality system, including the testing and/or calibration activities.  It is the responsibility of the quality manager to plan and organize audits as required by the schedule and requested by management.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(b)    Such audits must be carried out by trained and qualified personnel who are, wherever resources permit, independent of the activity to be audited.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note:         The cycle for internal auditing should normally be completed in one year.*

(c)    When audit findings cast doubt on the effectiveness of the operations or on the correctness or validity of the laboratory's test or calibration results, the laboratory must take timely corrective action, and must notify clients in writing if investigations show that the laboratory results may have been affected.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(d)    The area of activity audited, the audit findings and corrective actions that arise from them must be recorded.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

(e)    Follow-up audit activities must verify and record the implementation and effectiveness of the corrective action taken.

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

### E.13    Management reviews

(a)    According to a predetermined schedule and procedure, the laboratory's executive management must periodically conduct a review of the laboratory's quality system and testing and/or calibration activities to ensure their continuing suitability and effectiveness, and to introduce necessary changes or improvements.

(b)    The review must take account of:

(i)    the suitability of policies and procedures;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    reports from managerial and supervisory personnel;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)    the outcome of recent internal audits;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)    corrective and preventive actions;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v)    assessments by external bodies;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi)    the results of inter-laboratory comparisons or proficiency tests;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii)    changes in the volume and type of the work;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii)    client feedback;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(ix)   complaints; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(x)   other relevant factors, such as quality control activities, resources, and staff training.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*   *A typical period for conducting a management review is once every 12 months.*

*Note 2:*   *Results should feed into the laboratory planning system and should include the goals, objectives, and action plans for the coming year.*

*Note 3:*   *A management review includes consideration of related subjects at regular management meetings.*

(c)   Findings from management reviews and the actions that arise from them must be recorded.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)   The management must ensure that those actions are carried out within an appropriate and agreed timeframe.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

## E.14   Technical requirements for accreditation

### E.14.1   General

(a)   Many factors determine the correctness and reliability of the tests and/or calibrations performed by a laboratory.  These factors include contributions from:

(i)   human factors (E.14.2);

(ii)   accommodation and environmental conditions (E.14.3);

(iii)   test and calibration methods and method validation (E.14.4);

(iv)   equipment (E.14.5);

(v)   measurement trace ability (E.14.6);

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

     (vi)   sampling (E.14.8); and

     (vii)  the handling of test and calibration items (E.14.9).

(b)    The extent to which the factors contribute to the total uncertainty of measurement differs considerably between (types of) tests and between (types of) calibrations.  The laboratory must take account of these factors in developing test and calibration methods and procedures, in training and the qualification of personnel, and in selecting and calibrating the equipment it uses.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

### E.14.2    Personnel

(a)    The laboratory management must ensure the competence of all who operate specific equipment, perform tests and/or calibrations, evaluate results, and sign test reports and calibration certificates.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(b)    When using staff members, who are undergoing training, appropriate supervision must be provided.  Personnel performing specific tasks must be qualified on the basis of appropriate education, training, experience, and/or demonstrated skills, as required.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note 1:*    *In some technical areas (for example, non-destructive testing), it may be required that the personnel performing certain tasks hold personnel certification.  The laboratory is responsible for fulfilling specified personnel certification requirements.  The requirements for personnel certification might be regulatory, included in the standards for the specific technical field, or required by the client.*

*Note 2:*    *The personnel responsible for the opinions and interpretation included in test reports should, in addition to the appropriate qualifications, training, experience, and satisfactory knowledge of the testing carried out, also have:*

(c)    relevant knowledge of the technology used for manufacturing the items, materials, products, and others tested, or the way they are used or intended to be used, and of the defects or degradations which may occur during or in service;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(d)    knowledge of the general requirements expressed in the legislation and standards; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(e)    an understanding of the significance of deviations found with regard to the normal use of the items, materials, products, and others concerned.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(f)    The management of the laboratory must formulate the goals with respect to the education, training, and skills of the laboratory personnel.  The laboratory must have a policy and procedures for identifying training needs and providing training of personnel.  The training program must be relevant to the present and anticipated tasks of the laboratory.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(g)    The laboratory must use personnel who are employed by, or under contract to, the laboratory.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(h)    Where contracted and additional technical and key support personnel are used, the laboratory must ensure that such personnel are supervised and competent and that they work according to the laboratory's quality system.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(i)    The laboratory must maintain current job descriptions for managerial, technical, and key support personnel involved in tests and/or calibrations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:        Job descriptions can be defined in many ways.  As a minimum, the following should be defined:*

(i)    The responsibilities with respect to performing tests and/or calibrations;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(ii) The responsibilities with respect to the planning of tests and/or calibrations and evaluation of results;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii) The responsibilities for reporting opinions and Interpretations;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv) The responsibilities with respect to modifying methods and developing and validating new methods;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v) Expertise and experience required;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi) Qualifications and training programs; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii) Managerial duties.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(j) The management must authorize specific personnel to perform particular types of sampling, test and/or calibration, to issue test reports and calibration certificates, to give opinions and interpretations, and to operate particular types of equipment.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(k) The laboratory must maintain records of the relevant authorizations, competence, educational and professional qualifications, training, skills, and experience of all technical personnel, including contracted personnel.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(I)    This information must be readily available and must include the date on which authorization and/or competence is confirmed.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

### E.14.3    Accommodation and environmental conditions

(a)    Laboratory facilities for testing and/or calibration, including but not limited to energy sources, lighting, and environmental conditions, must be such as to facilitate correct performance of the tests and/or calibrations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)    The laboratory must ensure that the environmental conditions do not invalidate the results or adversely affect the required quality of any measurement.  Particular care must be taken when sampling and tests and/or calibrations are undertaken at sites other than a permanent laboratory facility.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)    The technical requirements for accommodation and environmental conditions that can affect the results of tests and calibrations must be documented.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)    The laboratory must monitor, control, and record environmental conditions as required by the relevant specifications, methods and procedures or where they influence the quality of the results.  Due attention must be paid, for example, to biological sterility, dust, electromagnetic disturbances, radiation, humidity, electrical supply, temperature, and sound and vibration levels, as appropriate to the technical activities concerned.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(e)    Tests and calibrations must be stopped when the environmental conditions jeopardize the results of the tests and/or calibrations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

(f)     There must be effective separation between neighbouring areas in which there are incompatible activities.  Measures must be taken to prevent cross-contamination.

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

(g)     Access to and use of areas affecting the quality of the tests and/or calibrations must be controlled.  The laboratory must determine the extent of control based on its particular circumstances.

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

(h)     Measures must be taken to ensure good housekeeping in the laboratory. Special procedures must be prepared where necessary.

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

### E.14.4     Test and calibration methods and method validation

(a)     The laboratory must use appropriate methods and procedures for all tests and/or calibrations within its scope.  Methods and procedures to be used include sampling, handling, transport, storage, and preparation of items to be tested and/or calibrated, and, where appropriate, an estimation of the measurement uncertainty as well as statistical techniques for analysis of test and/or calibration data.

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

(b)     The laboratory must have instructions on the use and operation of all relevant equipment, and on the handling and preparation of items for testing and/or calibration, or both, where the absence of such instructions could jeopardize the results of tests and/or calibrations.

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

(c)     All instructions, standards, manuals, and reference data relevant to the work of the laboratory must be kept up-to-date and must be made readily available to personnel (see E.3).

| Yes | No | N/A |
|-----|----|----|
|     |    |     |

(d) Deviation from test and calibration methods must occur only if the deviation has been documented, technically justified, authorized, and accepted by the client.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:* *International, regional, or national standards or other recognized specifications that contain sufficient and concise information on how to perform the tests and/or calibrations do not need to be supplemented or rewritten as internal procedures if these standards are written in a way that they can be used as published by the operating staff in a laboratory. It may be necessary to provide additional documentation for optional steps in the method or additional details.*

(e) Selecting methods

(i) The laboratory must use test and/or calibration methods, including methods for sampling, that meet the needs of the client and which are appropriate for the tests and/or calibrations it undertakes. Methods published in international, regional, or national standards must preferably be used. The laboratory must ensure that it uses the latest valid edition of a standard unless it is not appropriate or possible to do so.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii) When necessary, the standard must be supplemented with additional details to ensure consistent application.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii) When the client does not specify the method to be used, the laboratory must select appropriate methods that have been published either in international, regional, or national standards, or by reputable technical organizations, or in relevant scientific texts or journals, or as specified by the manufacturer of the equipment. Laboratory-developed methods or methods adopted by the laboratory may also be used if they are appropriate for the intended use and if they are validated.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv) The client must be informed as to the method chosen.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(v) The laboratory must confirm that it can properly operate standard methods before introducing the tests or calibrations. If the standard method changes, the confirmation must be repeated.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

(vi) The laboratory must inform the client when the method proposed by the client is considered to be inappropriate or out-of-date.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

(f) Laboratory-developed methods

(i) The introduction of test and calibration methods developed by the laboratory for its own use must be a planned activity and must be assigned to qualified personnel equipped with adequate resources.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

(ii) Plans must be updated as development proceeds and effective communication among all personnel involved must be ensured.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

(g) Non-standard methods

(i) When it is necessary to use methods not covered by standard methods, these must be subject to agreement with the client and must include a clear specification of the client's requirements and the purpose of the test and/or calibration.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

(ii) The method developed must have been validated appropriately before use.

| **Yes** | **No** | **N/A** |
|---|---|---|
| | | |

*Note:* *For new test and/or calibration methods, procedures should be developed prior to the tests and/or calibrations being performed and should contain at least the following information:*

(A)  appropriate identification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)  scope;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)  description of the type of item to be tested or calibrated;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(D)  parameters or quantities and ranges to be determined;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(E)  apparatus and equipment, including technical performance requirements;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(F)  reference standards and reference materials required;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(G)  environmental conditions required and any stabilization period needed;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(H)  description of the procedure, including;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(I)     affixing of identification marks, handling, transporting, storing, and preparing of items;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(J)     checks to be made before the work is started;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(K)     checks that the equipment is working properly and, where required, calibration and adjustment of the equipment before each use;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(L)     the method of recording the observations and results;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(M)     any safety measures to be observed;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(N)     criteria and/or requirements for approval or rejection;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(O)     data to be recorded and method of analysis and presentation; and

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(P)     the uncertainty or the procedure for estimating uncertainty.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(h)     Validating methods

Validation means to confirm by examination and to provide objective evidence that the particular requirements for a specific intended use are fulfilled.

---

(i)     The laboratory must validate non-standard methods, laboratory-designed or developed methods, standard methods used outside their intended scope, and amplifications and modifications of standard methods to confirm that the methods are fit for the intended use. The validation must be as extensive as is necessary to meet the needs of the given application or field of application.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    The laboratory must record the results obtained, the procedure used for the validation, and a statement as to whether the method is fit for the intended use.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*    *Validation may include procedures for sampling, handling, and transporting.*

*Note 2:*    *The techniques used for determining the performance of a method should be one of, or a combination of, the following:*

(A)     calibration using reference standards or reference materials;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)     comparison of results achieved with other methods;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)     inter-laboratory comparisons;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(D)     systematic assessment of the factors influencing the result; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(E)     assessment of the uncertainty of the results based on scientific understanding of the theoretical principles of the method and practical experience.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

*Note 3:*      *When some changes are made in the validated non-standard methods, the influence of such changes should be documented and, if appropriate, a new validation should be carried out.*

(i)      The range and accuracy of the values obtainable from validated methods (for example, the uncertainty of the results, detection limit, selectivity of the method, linearity, limit of repeatability and/or reproducibility, robustness against external influences and/or cross-sensitivity against interference from the matrix of the sample/test object), as assessed for the intended use, must be relevant to the clients' needs.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*      *Validation includes specifying the requirements, determining the characteristics of the methods, checking that the requirements can be fulfilled by using the method, and issuing a statement on the validity.*

*Note 2:*      *As method development proceeds, regular review should be carried out to verify that the needs of the client are still being fulfilled. Any change in requirements requiring modifications to the development plan should be approved and authorized.*

*Note 3:*      *Validation is always a balance between costs, risks, and technical possibilities. There are many cases in which the range and uncertainty of the values (for example, accuracy, detection limit, selectivity, linearity, repeatability, reproducibility, robustness, and cross-sensitivity) can only be given in a simplified way due to lack of information.*

(j)      Estimating the uncertainty of measurement

       (i)      A calibration laboratory, or a testing laboratory performing its own calibrations, must have and must apply a procedure to estimate the uncertainty of measurement for all calibrations and types of calibrations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii) Testing laboratories must have and must apply procedures for estimating the uncertainty of measurement.  In certain cases, the nature of the test method may preclude rigorous, metrologically and statistically valid calculation of the uncertainty of measurement.  In these cases, the laboratory must at least attempt to identify all the components of uncertainty and make a reasonable estimate, and must ensure that the form of reporting of the result does not give a wrong impression of the uncertainty.  A reasonable estimate must be based on knowing how the method performs and on the measurement scope and must make use of, for example, previous experience and validation data.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*     *The degree of rigour needed in estimating the uncertainty of measurement depends on factors such as:*

*a)     the requirements of the test method;*

*b)     the requirements of the client; and*

*c)     the existence of narrow limits on which decisions on conformance to a specification are based.*

*Note 2:*     *In those cases where a well-recognized test method specifies limits to the values of the major sources of uncertainty of measurement and specifies the form of presentation of calculated results, the laboratory is considered to have satisfied this clause E.14.4(j) by following the test method and reporting instructions (see E.14.11).*

(iii) When estimating the uncertainty of measurement, all uncertainty components that are of importance in the given situation must be taken into account using appropriate methods of analysis.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*     *Sources contributing to the uncertainty include, but are not necessarily limited to, the reference standards and reference materials used, methods and equipment used, environmental conditions, properties and condition of the item being tested or calibrated, and the operator.*

*Note 2:*     *The predicted long-term behaviour of the tested and/or calibrated item is not normally taken into account when estimating the measurement uncertainty.*

*Note 3:*     *For further information, see ISO 5725 series and the Guide to the Expression of Uncertainty in Measurement.*

(k)  Safe guarding of data:

(i)  Calculations and data transfers must be subject to appropriate checks in a systematic manner.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(ii)  When computers or automated equipment are used for acquiring, processing, recording, reporting, storing or retrieving of test or calibration data, the laboratory must ensure that:

(A)  computer software developed by the user is documented in sufficient detail and is suitably validated as being adequate for use;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(B)  procedures are established and implemented for protecting the data; such procedures must include, but not be limited to, integrity and confidentiality of data entry or collection, data storage, data transmission, and data processing; and

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(C)  computers and automated equipment are maintained to ensure proper functioning and are provided with the environmental and operating conditions necessary to maintain the integrity of test and calibration data.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note:*  *Commercial off-the-shelf software (for example, word processing, database, and statistical programs) in general use within their designed application range may be considered to be sufficiently validated. However, laboratory software configuration or modifications should be validated as in E.14.4(k)(ii)(A)).*

### E.14.5 Equipment

(a) The laboratory must be furnished with all items of sampling, measurement and test equipment required for the correct performance of the tests and/or calibrations (including but not limited to standard laboratory bench equipment, digital storage oscilloscope or logical analyser (to view outputs from ports), tools to perform physical security conformance tests, sampling, preparing of test and/or calibration items, processing, and analysis of test and/or calibration data).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b) In those cases where the laboratory needs to use equipment outside its permanent control, it must ensure that the requirements of this handbook are met.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c) Equipment and its software used for testing, calibration, and sampling must be capable of achieving the accuracy required and must comply with specifications relevant to the tests and/or calibrations concerned.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d) Calibration programs must be established for key quantities or values of the instruments where these properties have a significant effect on the results.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(e) Before being placed into service, equipment (including that used for sampling) must be calibrated or checked to establish that it meets the laboratory's specification requirements and that it complies with the relevant standard specifications. It must be checked and/or calibrated before use (see E.16).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(f) Equipment must be operated by authorized personnel. Up-to-date instructions on the use and maintenance of equipment (including any relevant manuals provided by the manufacturer of the equipment) must be readily available for use by the appropriate laboratory personnel.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(g) Each item of equipment and its software used for testing and calibration and significant to the result must, when practicable, be uniquely identified.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(h) Records must be maintained of each item of equipment and its software significant to the tests and/or calibrations performed. The records must include at least the following:

   (i) the identity of the item of equipment and its software;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

   (ii) the manufacturer's name, type identification, and serial number or other unique identification;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

   (iii) checks that equipment complies with the specification (see E.14.5(c) to E.14.5(e));

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

   (iv) the current location, where appropriate;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

   (v) the manufacturer's instructions, if available, or reference to their location;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

    (vi)    dates, results and copies of reports and certificates of all calibrations, adjustments, acceptance criteria, and the due date of next calibration;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

    (vii)    the maintenance plan, where appropriate, and maintenance carried out to date; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

    (viii)   any damage, malfunction, modification or repair to the equipment.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(i)    The laboratory must have procedures for safe handling, transport, storage, use and planned maintenance of measuring equipment to ensure proper functioning and to prevent contamination or deterioration.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:*    *Additional procedures may be necessary when measuring equipment is used outside the permanent laboratory for tests, calibrations, or sampling.*

(j)    Equipment that has been subjected to overloading or mishandling, gives suspect results, or has been shown to be defective or outside specified limits, must be taken out of service. It must be isolated to prevent its use or clearly labelled or marked as being out of service until it has been repaired and shown by calibration or test to perform correctly.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(k)    The laboratory must examine the effect of the defect or departure from specified limits on previous tests and/or calibrations and must institute the "Control of nonconforming testings and/or calibration work" procedure (see E.7).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(l)    Whenever practicable, all equipment under the control of the laboratory and requiring calibration must be labelled, coded, or otherwise identified to indicate the status of calibration, including the date when last calibrated and the date or expiration criteria when recalibration is due.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(m)    When, for whatever reason, equipment goes outside the direct control of the laboratory, the laboratory must ensure that the function and calibration status of the equipment are checked and shown to be satisfactory before the equipment is returned to service.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(n)    When intermediate checks are needed to maintain confidence in the calibration status of the equipment, these checks must be carried out according to a defined procedure.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(o)    Where calibrations give rise to a set of correction factors, the laboratory must have procedures to ensure that copies (for example, in computer software) are correctly updated.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(p)    Test and calibration equipment, including both hardware and software, must be safeguarded from adjustments that would invalidate the test and/or calibration results.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

### E.14.6    Measurement traceability

(a)    General

(i)    All equipment used for tests and/or calibrations, including equipment for subsidiary measurements (for example, for environmental conditions) having a significant effect on the accuracy or validity of the result of the test, calibration, or sampling must be calibrated before being put into service.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)   The laboratory must have an established program and procedure for the calibration of its equipment.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:      Such a program should include a system for selecting, using, calibrating, checking, controlling, and maintaining measurement standards, reference materials used as measurement standards, and measuring and test equipment used to perform tests and calibrations.*

(b)   Specific requirements

(i)   Calibration

(A)   For calibration laboratories, the program for calibration of equipment must be designed and operated so as to ensure that calibrations and measurements made by the laboratory are traceable to the International System of Units (SI) (Système international d'unités).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)   A calibration laboratory establishes traceability of its own measurement standards and measuring instruments to the SI by means of an unbroken chain of calibrations or comparisons linking them to relevant primary standards of the SI units of measurement.   The link to SI units may be achieved by reference to national measurement standards.   National measurement standards may be primary standards, which are primary realizations of the SI units or agreed representations of SI units based on fundamental physical constants, or they may be secondary standards which are standards calibrated by another national metrology institute.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)   When using external calibration services, trace-ability of measurement must be assured by the use of calibration services from laboratories that can demonstrate competence, measurement capability, and traceability.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(D)  The calibration certificates issued by these laboratories must contain the measurement results, including the measurement uncertainty and/or a statement of compliance with an identified metrological specification (see also E.14.11(d)(iv) to E.14.11(d)(vii)).

| **Yes** | **No** | **N/A** |
|---------|--------|---------|
|         |        |         |

*Note 1:*    *Calibration laboratories fulfilling the requirements of this handbook are considered to be competent. A calibration certificate bearing an accreditation body logo from a calibration laboratory accredited to this handbook, for the calibration concerned, is sufficient evidence of traceability of the calibration data reported.*

*Note 2:*    *Traceability to SI units of measurement may be achieved by reference to an appropriate primary standard (see VIM:1993, 6.4) or by reference to a natural constant, the value of which in terms of the relevant SI unit is known and recommended by the General Conference of Weights and Measures (CGPM) and the International Committee for Weights and Measures (CIPM).*

*Note 3:*    *Calibration laboratories that maintain their own primary standard or representation of SI units based on fundamental physical constants can claim trace-ability to the SI system only after these standards have been compared, directly or indirectly, with other similar standards of a national metrology institute.*

*Note 4:*    *The term "identified metrological specification" means that it must be clear from the calibration certificate which specification the measurements have been compared with, either by including the specification or by giving an unambiguous reference to the specification.*

*Note 5:*    *When the terms "international standard" or "national standard" are used in connection with traceability, it is assumed that these standards fulfil the properties of primary standards for the realization of SI units.*

*Note 6:*    *Traceability to national measurement standards does not necessarily require the use of the national metrology institute of the country in which the laboratory is located.*

*Note 7:*    *If a calibration laboratory wishes or needs to obtain traceability from a national metrology institute other than in its own country, this laboratory should select a national metrology institute that actively participates in the activities of BIPM either directly or through regional groups.*

*Note 8:*    *The unbroken chain of calibrations or comparisons may be achieved in several steps carried out by different laboratories that can demonstrate traceability.*

(c)    There are certain calibrations that currently cannot be strictly made in SI units. In these cases, calibration must provide confidence in measurements by establishing traceability to appropriate measurement standards such as:

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(i)    the use of certified reference materials provided by a competent supplier to give a reliable physical or chemical characterization of a material;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(ii)    the use of specified methods and/or consensus standards that are clearly described and agreed on by all parties concerned; and

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(iii)    Participation in a suitable program of inter-laboratory comparisons is required where possible.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(d)    For testing laboratories, the requirements given in E.14.6(b)(i) apply for measuring and test equipment with measuring functions used, unless it has been established that the associated contribution from the calibration contributes little to the total uncertainty of the test result. When this situation arises, the laboratory must ensure that the equipment used can provide the uncertainty of measurement needed.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note:*    *The extent to which the requirements in E.14.6(b)(i) should be followed depends on the relative contribution of the calibration uncertainty to the total uncertainty. If calibration is the dominant factor, the requirements should be strictly followed.*

(e)    Where traceability of measurements to SI units is not possible and/or not relevant, the same requirements for traceability to, for example, certified reference materials, agreed methods, and/or consensus standards, are required as for calibration laboratories (see E.14.6(c)).

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

**E.14.7    Reference standards and reference materials**

(a)    Reference standards

(i)    The laboratory must have a program and procedure for the calibration of its reference standards.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    Reference standards must be calibrated by a body that can provide traceability as described in E.14.6(b)(i).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)    Such reference standards of measurement held by the laboratory must be used for calibration only and for no other purpose, unless it can be shown that their performance as reference standards would not be invalidated.  Reference standards must be calibrated before and after any adjustment.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)    Reference materials

(i)    Reference materials must, where possible, be traceable to SI units of measurement or to certified reference materials.  Internal reference materials must be checked as far as is technically and economically practicable.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(c)    Intermediate checks

(i)    Checks needed to maintain confidence in the calibration status of reference, primary, transfer, or working standards and reference materials must be carried out according to defined procedures and schedules.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)     Transport and storage

(i)     The laboratory must have procedures for safe handling, transporting, storing, and using reference standards and reference materials to prevent contamination or deterioration and to protect their integrity.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note:          Additional procedures may be necessary when reference standards and reference materials are used outside the permanent laboratory for tests, calibrations, or sampling.*

### E.14.8     Sampling

(a)     The laboratory must have a sampling plan and procedures for sampling when it carries out sampling of substances, materials, or products for subsequent testing or calibration.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(b)     The sampling plan, as well as the sampling, procedure, must be available at the location where sampling is undertaken.  Sampling plans must, whenever reasonable, be based on appropriate statistical methods.  The sampling process must address the factors to be controlled to ensure the validity of the test and calibration results.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:          Sampling is a defined procedure whereby a part of a substance, material, or product is taken to provide for testing or calibration of a representative sample of the whole.  Sampling may also be required by the appropriate specification for which the substance, material, or product is to be tested or calibrated.  In certain cases (for example, forensic analysis), the sample may not be representative but is determined by availability.*

*Note 2:          Sampling procedures should describe the selection, sampling plan, withdrawal, and preparation of a sample or samples from a substance, material, or product to yield the required information.*

(c)     Where the client requires deviations, additions, or exclusions from the documented sampling procedure, these must be recorded in detail with the appropriate sampling data, included in all documents containing test and/or calibration results, and communicated to the appropriate personnel.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)    The laboratory must have procedures for recording relevant data and operations relating to sampling that forms part of the testing or calibration that is undertaken.  These records must include the sampling procedure used, the identification of the sampler, environmental conditions (if relevant) and diagrams or other equivalent means to identify the sampling location as necessary and, if appropriate, the statistics upon which the sampling procedures are based.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

### E.14.9    Handling of test and calibration items

(a)    The laboratory must have procedures for the transportation, receipt, handling, protection, storage, retention, and/or disposal of test and/or calibration items, including all provisions necessary to protect the integrity of the test or calibration item, and to protect the interests of the laboratory and the client.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(b)    The laboratory must have a system for identifying test and/or calibration items.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(c)    The identification must be retained throughout the life of the item in the laboratory.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(d)    The system must be designed and operated so as to ensure that items cannot be confused physically or when referred to in records or other documents.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(e)    The system must, if appropriate, accommodate a sub-division of groups of items and the transfer of items within and from the laboratory.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(f)     Upon receipt of the test or calibration item, abnormalities or departures from normal or specified conditions, as described in the test or calibration method, must be recorded.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(g)     When there is doubt as to the suitability of an item for test or calibration, or when an item does not conform to the description provided, or the test or calibration required is not specified in sufficient detail, the laboratory must consult the client for further instructions before proceeding and must record the discussion.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(h)     The laboratory must have procedures and appropriate facilities for avoiding deterioration, loss, or damage to the test or calibration item during storage, handling, and preparation.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(i)     Handling instructions provided with the item must be followed.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(j)     When items have to be stored or conditioned under specified environmental conditions, these conditions must be maintained, monitored, and recorded.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(k)     Where a test or calibration item or a portion of an item is to be held secure, the laboratory must make arrangements for storing and protecting the condition and integrity of the secured items or portions concerned.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*     *Where test items are to be returned into service after testing, special care is required to ensure that they are not damaged or injured during the handling, testing, or storing and waiting processes.*

*Note 2:*     *A sampling procedure and information on storage and transport of samples, including information on sampling factors influencing the test or calibration result, should be provided to those responsible for taking and transporting the samples.*

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

*Note 3:*      *Reasons for keeping a test or calibration item secure can be for reasons of record, safety or value, or to enable complementary tests and/or calibrations to be performed later.*

**E.14.10**      **Assuring the quality of test and calibration results**

(a)      The laboratory must have quality control procedures for monitoring the validity of tests and calibrations undertaken.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(b)      The resulting data must be recorded in such a way that trends are detectable and, where practicable, statistical techniques must be applied to the reviewing of the results.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(c)      This monitoring must be planned and reviewed and may include, but not be limited to, the following:

(i)      regular use of certified reference materials and/or internal quality control using secondary reference materials;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(ii)      participation in inter-laboratory comparison or proficiency-testing programs;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iii)      replicate tests or calibrations using the same or different methods;

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iv)      retesting or recalibration of retained items; and

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(v)      correlation of results for different characteristics of an item.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

*Note:* *The selected methods should be appropriate for the type and volume of the work undertaken.*

### E.14.11    Reporting the results

(a)    General

(i)    The results of each test, calibration, or series of tests or calibrations carried out by the laboratory must be reported accurately, clearly, unambiguously and objectively, and according to any specific instructions in the test or calibration methods.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    The results must be reported, usually in a test report or a calibration certificate (see note 1).  It must include all the information requested by the client, and necessary for the interpretation of the test or calibration results, and required by the method used.  This information is normally that required by E.14.11(b) and E.14.11(c) or E.14.11(d).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)    In the case of tests or calibrations performed for internal clients, or in the case of a written agreement with the client, the results may be reported in a simplified way.  Any information listed in E.14.11(b) to E.14.11(d) that is not reported to the client must be readily available in the laboratory which carried out the tests and/or calibrations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)    The laboratory has the capability to digitally sign or apply an integrity mechanism to electronic copies of test reports.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v)    If a test report is digitally signed, the laboratory provides a secure means of conveying the necessary information to AusPayNet for signature verification.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi) The laboratory uses confidentiality mechanisms to prevent unauthorized disclosure of electronic copies of test reports delivered by any of the available means.

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

*Note 1:*     *Test reports and calibration certificates are sometimes called test certificates and calibration reports, respectively.*

*Note 2:*     *The test reports or calibration certificates may be issued as hard copy or by electronic data transfer provided that the requirements of this handbook are met.*

(b) Test reports and calibration certificates

Each test report or calibration certificate must include at least the following information, unless the laboratory has valid reasons for not doing so:

(i) a title (for example, "Test Report" or "Calibration Certificate");

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(ii) the name and address of the laboratory, and the location where the tests and/or calibrations were carried out, if different from the address of the laboratory;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(iii) unique identification of the test report or calibration certificate (such as the serial number), and on each page an identification to ensure that the page is recognized as a part of the test report or calibration certificate, and a clear identification at the end of the test report or calibration certificate;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(iv) the name and address of the client;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(v) identification of the method used;

| **Yes** | **No** | **N/A** |
|---|---|---|
|  |  |  |

(vi) a description of, the condition of, and unambiguous identification of the item or items tested or calibrated;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii) the date of receipt of the test or calibration item or items where this is critical to the validity and application of the results, and the date or dates when the test or calibration were performed;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(viii) reference to the sampling plan and procedures used by the laboratory or other bodies where these are relevant to the validity or application of the results;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ix) the test or calibration results with, where appropriate, the units of measurement;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(x) the names, functions, and signatures or equivalent identification of persons authorizing the test report or calibration certificate; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(xi) where relevant, a statement to the effect that the results relate only to the items tested or calibrated.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:*     *Hard copies of test reports and calibration certificates should also include the page number and total number of pages.*

*Note 2:*     *It is recommended that laboratories include a statement specifying that the test report or calibration certificate must not be reproduced except in full, without written approval of the laboratory.*

(c)     Test reports

(i)     In addition to the requirements listed in E.14.11(b), test reports must, where necessary for the interpretation of the test results, include the following:

(A)     deviations from, additions to, or exclusions from the test method, and information on specific test conditions, such as environmental conditions;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)     where relevant, a statement of compliance or non-compliance with requirements and/or specifications;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)     where applicable, a statement on the estimated uncertainty of measurement; information on uncertainty is needed in test reports when it is relevant to the validity or application of the test results, when a client's instruction so requires, or when the uncertainty affects compliance to a specification limit;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(D)     where appropriate and needed, opinions and interpretations (see E.14.11(e)); and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(E)     additional information that may be required by specific methods, clients, or groups of clients.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    In addition to the requirements listed in E.14.11(b) and E.14.11(c), test reports containing the results of sampling must include the following, where necessary, for the interpretation of test results:

(A)     the date of sampling;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)     unambiguous identification of the substance, material, or product sampled (including the name of the manufacturer, the model or type of designation and serial numbers as appropriate);

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)     the location of sampling, including any diagrams, sketches or photographs;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(D)     a reference to the sampling plan and procedures used;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(E)     details of any environmental conditions during sampling that may affect the interpretation of the test results; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(F)     any standard or other specification for the sampling method or procedure, and deviations, additions to, or exclusions from the specification concerned.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(d)     Calibration certificates

(i)     In addition to the requirements listed in E.14.11(b), calibration certificates must include the following, where necessary, for the interpretation of calibration results:

(A)     the conditions (for example, environmental) under which the calibrations were made that have an influence on the measurement results;

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(B)     the uncertainty of measurement and/or a statement of compliance with an identified metrological specification or clauses thereof; and

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(C)     evidence that the measurements are traceable (see note 2 in E.14.6(b)(i)).

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii)    The calibration certificate must relate only to quantities and the results of functional tests.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iii)   If a statement of compliance with a specification is made this must identify which clauses of the specification are met or not met.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(iv)    When a statement of compliance with a specification is made omitting the measurement results and associated uncertainties, the laboratory must record those results and maintain them for possible future reference.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(v)     When statements of compliance are made, the uncertainty of measurement must be taken into account.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vi)    When an instrument for calibration has been adjusted or repaired, the calibration results before and after adjustment or repair, if available, must be reported.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(vii) A calibration certificate (or calibration label) must not contain any recommendation on the calibration interval except where this has been agreed with the client. This requirement may be superseded by legal regulations.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(e) Opinions and interpretations

(i) When opinions and interpretations are included, the laboratory must document the basis upon which the opinions and interpretations have been made. Opinions and interpretations must be clearly marked as such in a test report.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

*Note 1:* *Opinions and interpretations should not be confused with inspections and product certifications as intended in AS/NZS ISO/IEC 17020 and ISO/IEC Guide 65.*

*Note 2:* *Opinions and interpretations included in a test report may comprise, but not be limited to, the following:*

  *a)* *an opinion on the statement of compliance/non-compliance of the results with requirements;*

  *b)* *fulfilment of contractual requirements;*

  *c)* *recommendations on how to use the results; and*

  *d)* *guidance to be used for improvements.*

*Note 3:* *In many cases it might be appropriate to communicate the opinions and interpretations by direct dialogue with the client. Such dialogue should be written down.*

(f) Testing and calibration results obtained from subcontractors

(i) When the test report contains results of tests performed by subcontractors, these results must be clearly identified.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

(ii) The subcontractor must report the results in writing or electronically.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(iii)  When a calibration has been subcontracted, the laboratory performing the work must issue the calibration certificate to the contracting laboratory.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(g)  Electronic transmission of results

(i)  In the case of transmission of test or calibration results by telephone, telex, facsimile, or other electronic or electromagnetic means, the requirements of this handbook must be met (see also E.14.4(k)).

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(h)  Format of reports and certificates

(i)  The format must be designed to accommodate each type of test or calibration carried out and to minimize the possibility of misunderstanding or misuse.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

*Note 1:*    *Attention should be given to the layout of the test report or calibration certificate, especially with regard to the presentation of the test or calibration data and ease of assimilation by the reader.*

*Note 2:*    *The headings should be standardized as far as possible.*

(i)  Amendments to test reports and calibration certificates

(i)  Material amendments to a test report or calibration certificate after issue must be made only in the form of a further document, or data transfer, which includes the statement: "Supplement to Test Report [or Calibration Certificate], serial number … [or as otherwise identified]," or an equivalent form of wording.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(ii)  Such amendments must meet all the requirements of this handbook.

| Yes | No | N/A |
|---|---|---|
|  |  |  |

(iii) When it is necessary to issue a complete new test report or calibration certificate, this must be uniquely identified and must contain a reference to the original that it replaces.

| Yes | No | N/A |
|-----|-----|-----|
|     |     |     |

**The next page is F.1**

## ANNEXURE F.   INTRODUCTION TO DEVICE SUPPORT AND SCM FUNCTIONALITY

*[Informative]*

### F.1   Introduction

This annexure illustrates how the functionality provided by the AusPayNet SCM may be used to provide device driving support for ATMs and POS Terminals including remote initialisation.

It is based on the use of the approved triple-DES SCM specification referred to as AusPayNet SCM specification which is at revision V5.0 at the time of writing (January 2015) This annexure illustrates a method of implementing both ATM and POS device support using AusPayNet specification Security Control Modules.  Only a limited subset of the possible key management schemes and associated SCM functions are described, in particular, transaction based key management schemes are not addressed.

Description of transactions and messages is confined to cryptographic items such as keys, PIN blocks, and MACs, and excludes financial and other items.

### F.2   References and Related Documentation

1.   SCM Spec Specification for a Security Control Module Function Set, AusPayNet Technical Security Sub-Committee, Version 5.0, June 25th, 2013.    <span style="font-size:small">Amended effective 20.8.18</span>

2.   AS 2805.3-2000 Electronic funds transfer - Requirements for interfaces - PIN management and security.

3.   AS 2805.4.1/Amdt 1/2006   Electronic funds transfer - Requirements for interfaces - Message authentication - Mechanisms using a block cipher.

4.   AS 2805.5.1-1992   Electronic Funds Transfer - Requirements for Interfaces, Part 5.1: Ciphers - Data encipherment algorithm 1 (DEA 1).

5.   AS 2805.5.3-2004   Electronic funds transfer - Requirements for interfaces - Ciphers - Data encipherment algorithm 2 (DEA 2).

6.   AS 2805.5.4-2000   Electronic Funds Transfer - Requirements for Interfaces, Part 5.4: Ciphers - Data encipherment algorithm 3 (DEA 3) and related techniques.

7.   AS 2805.6.2-2002   Electronic funds transfer - Requirements for interfaces - Key management - Transaction keys.

8.   AS 2805.6.4-2001   Electronic funds transfer - Requirements for interfaces - Key management - Session keys - Terminal to acquirer.

9.    AS 2805.6.5.3-2004    Electronic funds transfer - Requirements for interfaces - Key management - TCU initialization - Asymmetric.

10.    NCR NDC+ Programmer's Reference Manual.

## F.3    Overview

Section F.4 describes the key specifiers which the AusPayNet SCMs use to manage keys with different lengths and attributes.  It also describes the key variants that are used.

Section F.5 shows how AusPayNet SCM functions can be used to perform 3DES ATM key management with double-length keys, MACing, and remote initialisation.  *The AusPayNet SCM functions currently only provide support for NCR's NDC+ 3DES ATMs.  Details of other ATM manufacturer's 3DES functionality are covered.*

Section F.6 shows how AusPayNet SCM functions can be used to perform 3DES POS key management (double-length session keys) with remote initialisation.

The scheme described in section F.6 is AS 2805.6.4 key management (session keys) and AS 2805.6.5.3 remote initialisation.  The AusPayNet SCM also provides 3DES functions to support AS 2805.6.2 key management (transaction keys).  This is not covered in this document.

For both ATM and EFTPOS Terminals, there are associated new or upgraded remote initialisation standards and associated SCM functions, which interface with the 3DES session key management functions.  The IAC Manual should be consulted to determine the appropriate key lengths to be used when implementing any remote key initialisation scheme. <span style="float:right">Amended effective 20.8.18</span>

For ATM devices, section F.5.6 describes how double-length master keys can be loaded manually instead of by remote initialisation.

For EFTPOS Terminals, section F.6.5 describes how it is possible to combine 3DES session key management with remote initialisation using the existing 512-bit RSA keys.[1] <span style="float:right">Amended effective 20.8.18</span>

## F.4    Key Specifiers and Variants

The AusPayNet SCM specification introduces a new data structure: the key specifier.  A key specifier allows various attributes to be associated with a key:

• key length: single, double, triple, etc.;

• keyblock encipherment algorithm: DEA, AES, etc.;

---

[1] It is a challenge for POS Terminals with 8-bit hardware to perform signing and ciphering with 1024-bit keys. It is not unknown for a Terminal to take 11-12 minutes to perform this calculation with 512-bit keys after being sent the sponsor's public key (see F.6.4).

- keyblock encipherment mode: ECB, CBC, etc. ;

- storage mode: host or SCM.

These attributes are encoded as different hexadecimal values of a one-byte key specifier format code. Thus format code 21, for example, specifies a key with the following attributes:

- key length: double (128-bit);

- keyblock encipherment algorithm: DEA;

- keyblock encipherment mode: CBC;

- storage mode: host (because this format includes an index of the KM under which the key is enciphered for storage on the host.

Many AusPayNet SCM functions allow more than one key specifier format to be used in the request or the response.

The following key specifier formats are applicable to the host-stored keys used for ATM and EFTPOS Terminal key management:

Amended
effective 20.8.18

| Format 21 DEA CBC Enciphered key - 128-bit with KM index | | | |
|---|---|---|---|
| Length | Attrib | Content | Description |
| 1 | h | 21 | Format Code |
| 1 | x | i | KM index (Range 00-FF) |
| 16 | x | eKMi(K) | Enciphered key |

| Format 23 DEA ECB Enciphered key - 128-bit with KM index | | | |
|---|---|---|---|
| Length | Attrib | Content | Description |
| 1 | h | 23 | Format Code |
| 1 | x | i | KM index (Range 00-FF) |
| 16 | x | eKMi(K) | Enciphered key |

| Format 31 DEA CBC Enciphered key - 128-bit | | | |
|---|---|---|---|
| Length | Attrib | Content | Description |
| 1 | h | 31 | Format Code |
| 16 | x | eKEK(K) | Enciphered key |

---

| Format 41 Cleartext key - DEA 2 | | | |
|--------|--------|---------|-------------|
| **Length** | **Attrib** | **Content** | **Description** |
| 1 | h | 41 | Format Code |
| 1 | x | n | Number (n) of 8-byte blocks in modulus |
| 16*n | x | PK | Clear text DEA 2 public key |

| Format 42 Enciphered key - DEA 2 with KM index | | | |
|--------|--------|---------|-------------|
| **Length** | **Attrib** | **Content** | **Description** |
| 1 | h | 42 | Format Code |
| 1 | x | n | Number (n) of 8-byte blocks in modulus |
| 1 | x | i | KM index (Range 00-FF) |
| 16*n | x | eKMi(PK) or eKMi(SK) | DEA CBC Enciphered DEA 2 key. Either the public key or the private key. |

Each SCM function implicitly requires keyblocks in a predetermined format.
In an SCM Spec function, the key specifier is preceded by a length prefix, which adds one or more bytes to each of the above formats.  The value of the length prefix does not include its own length.  It is not necessary to store or transmit the length prefix, as its value is implied by the format code.  The lengths of each of the above key specifiers are as follows:

| **Length** | **Format code** | **Key specifier** |
|--------|--------|-------------|
| | 21 | DEA CBC Enciphered key - 128-bit with KM index |
| 18 | 23 | DEA ECB Enciphered key - 128-bit with KM index |
| | | |
| 17 | 31 | DEA CBC Enciphered key - 128-bit |
| 16n + 2 | 41 | Cleartext DEA 2 public key - n 8-byte blocks |
| 16n + 3 | 42 | DEA CBC Enciphered DEA 2 key - n 8-byte blocks |

The following figures reflect the different way of representing key variants in the AMB and SCM Spec specifications. SCM Spec function specifications represent the repeated byte of each hexadecimal variant constant, as shown below:

| AMB variant | SCM Spec variant | variant constant for ECB-enciphered keys | variant constant for CBC-enciphered keys (SCM Spec) |
|---|---|---|---|
| V1 | V24 | 2424242424242424242424242424242424 | 24C024C024C024C024C024C024C024C0 |
| V2 | V28 | 282828282828282828282828282828282828 | 28C028C028C028C028C028C028C028C0 |
| V3 | V22 | 222222222222222222222222222222222222 | 22C022C022C022C022C022C022C022C0 |
| V4 | V48 | 4848484848484848484848484848484848 | 48C048C048C048C048C048C048C048C0 |
| V5 | V42 | 424242424242424242424242424242424242 | 42C042C042C042C042C042C042C042C0 |
| V6 | V44 | 444444444444444444444444444444444444 | 44C044C044C044C044C044C044C044C0 |
| V7 | V82 | 828282828282828282828282828282828282 | 82C082C082C082C082C082C082C082C0 |
| V8 | V84 | 8484848484848484848484848484848484 | 84C084C084C084C084C084C084C084C0 |
| N/A | VA0 | A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0A0 | A0C0A0C0A0C0A0C0A0C0A0C0A0C0A0C0 |
| V10 | VAA | AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | AAC0AAC0AAC0AAC0AAC0AAC0AAC0AAC0 |
| N/A | VAC | ACACACACACACACACACACACACACACACAC | ACC0ACC0ACC0ACC0ACC0ACC0ACC0ACC0 |

In subsequent figures, a box such as 21 in front of a key indicates the key specifier format.

## F.5 ATM Terminal - 3DES

AusPayNet have defined an ATM 3DES solution that matches to the NCR ATM NDC+ 3DES specifications. Accordingly the following sections are based on this solution.

For remote initialisation, three RSA key pairs are used. The modulus of each key pair is 2048 bits in size:

- The manufacturer's key (SK-NCR, PK-NCR);

- The host's key (SK-HSM, PK-HSM);

- The Encrypting PIN pad's key (SK-EPP, PK-EPP).

Signatures are created by signing a hash of the target key or data, allowing all of the above keys to be the same size (unlike RSA keys for POS - see F.6).

NCR nomenclature for RSA key usage is as follows:

- (key) * SKsignature of key (or data) with secret key;

- [key] PK encryption of key (or data) with public key.

---

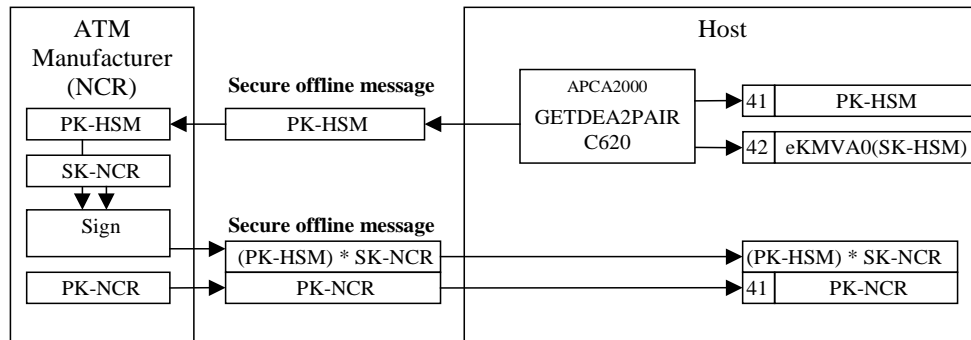### F.5.1 Exchange of Public Keys between Manufacturer and Host



**Figure 1 Exchange of RSA Public Keys between ATM Manufacturer and Host**

This is a one-off offline procedure, which precedes installation of any of the manufacturer's Encrypting PIN Pads on the host's network. The keys exchanged will be used in common for all ATMs on the network (unless either party needs to replace their RSA keys in the future).

1.  The host uses SCM function C620 to generate a general-purpose RSA key pair. This function is called with the size of the modulus set to 32 8-byte blocks and the public key exponent set to 65537.

2.  The host sends the host's public key to the manufacturer in a secure offline message (encrypted with PGP, for example).

3.  The host stores the host's public key for sending to ATMs (see F.5.3).

4.  The host stores the host's encrypted secret key for signing ATM master keys (see F.5.4).

5.  The manufacturer signs the host's public key with the manufacturer's secret key, and returns the signature in a secure offline message (encrypted with PGP, for example), along with the manufacturer's public key.

6.  The host appends the fixed exponent 65537 to the manufacturer's public key and stores it for checking the signature of EPP public keys (see F.5.3).

7.  The host stores the signed host's public key for sending to ATMs (see F.5.3).

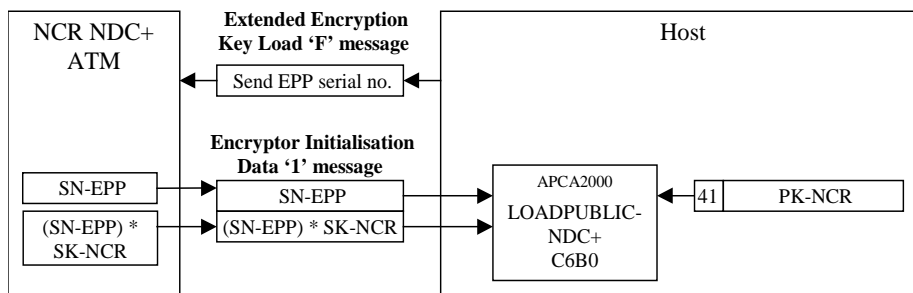### F.5.2 Authentication by Host of ATM's EPP Serial Number



**Figure 2 Authentication by Host of ATM's EPP Serial Number**

1. The host requests the serial number of the ATM's EPP using an Extended Encryption Key Load Message (Message Class 3, Message Sub-class 4) with Modifier 'F' - 'Send EPP serial number and signature'.

2. The ATM returns the EPP's serial number and its signature, which were loaded into the EPP during manufacture. They are sent in an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '1' - 'EPP serial number and signature'.

3. There is no function in the AusPayNet SCM specifically designed to verify the signature on an EPP serial number. The signature can be verified, however, by making it look like a public key.

4. The host pads the EPP serial number and appends the fixed exponent 65537 to produce a format 41 key for sending to the SCM.

5. The host decodes the EPP's serial number signature from base-94 for sending to the SCM.

6. The host uses SCM function C6B0 to verify the EPP's serial number, using the manufacturer's public key provided by the manufacturer (see F.5.1).

7. If function C6B0 indicates that the EPP's serial number signature is invalid, the host displays a console message[2].

---

[2] ATM sent invalid EPP serial number. Master key load will be unsuccessful

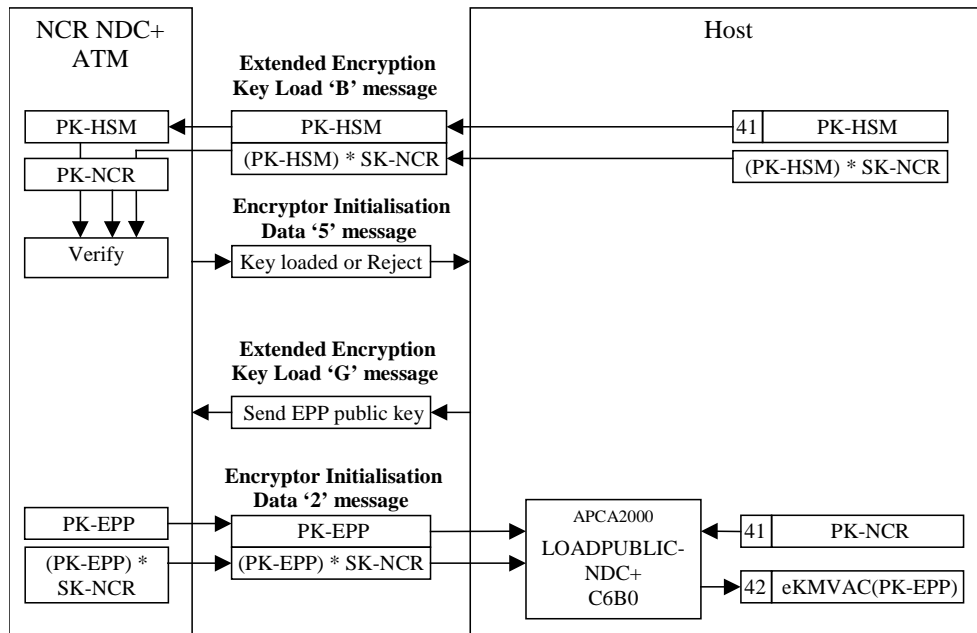## F.5.3  Exchange of RSA Public Keys between ATM and Host



**Figure 3 Authentication by Host of ATM's EPP Serial Number**

1.  The host sends the host's public key to the ATM, along with the signature provided by the manufacturer (see F.5.1). They are sent in an Extended Encryption Key Load message (Message Class 3, Message Sub-class 4) with Modifier 'B' - 'Load HSM public key and signature'. For the message, the host removes the exponent from the host's public key, and encodes the host's public key modulus and the signature to base-94.

2.  The ATM's EPP verifies the signature of the host's public key, using the manufacturer's public key which was loaded into the EPP during manufacture.

3.  The ATM sends an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '5' - 'Key Loaded'.

4.  If the host does not receive this 'Key Loaded' message, it displays a console message[3] and does not proceed with the key exchange.

5.  The host requests the public key of the ATM's EPP using an Extended Encryption Key Load Message (Message Class 3, Message Sub-class 4) with Modifier 'G' - 'Send EPP public key and signature.

6.  The ATM returns the EPP's public key and its signature, which were loaded into the EPP during manufacture. They are sent in an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '2' - 'EPP public key and signature'.

---

[3] The key exchange failed and no keys were loaded. Master key load will be unsuccessful.

7.   The host decodes the EPP's public key modulus from base-94 and appends the fixed exponent 65537 to produce a format 41 key for sending to the SCM.

8.   The host decodes the EPP's public key signature from base-94 for sending to the SCM.

9.   The host uses SCM function C6B0 to verify the EPP's public key, using the manufacturer's public key provided by the manufacturer (see F.5.1)

10.  If function C6B0 indicates that the EPP's public key signature is valid, it encrypts the EPP's public key under a variant of the domain master key, and the host stores it for encrypting an ATM master key (see F.5.4).

11.  If function C6B0 indicates that the EPP's public key signature is invalid, the host displays a console message[4] and does not store an encrypted EPP's public key.

## F.5.4    Generation of double-length ATM Master Key
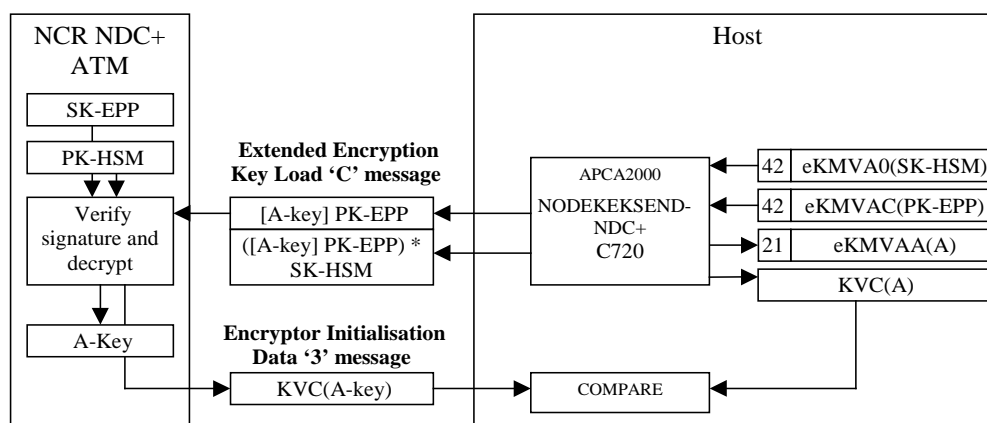


**Figure 4 Generation of double-length ATM Master Key**

## F.5.5    Remote Initialisation

1.   The host uses SCM function C720 to generate a random double-length master key.  The SCM function pads the master key to 256 bytes and encrypts it with the EPP's public key received earlier (see F.5.3) and signs it with the HSM's secret key generated earlier (see F.5.1).

2.   The hosts sends the encrypted master key and signature to the ATM in an Extended Encryption Key Load message (Message Class 3, Message Sub-class 4) with Modifier 'C' - 'Load initial master key (A-key) with RSA key'.  For the message, the host encodes the encrypted public key and the signature to base-94.

---

[4] Host's public key loaded on ATM but ATM's public key not loaded on host.  Master key load will be unsuccessful.

3.    The host saves the master key, encrypted under a variant of the domain master key, for encrypting session keys (see F.5.7)

4.    The ATM's EPP verifies the signature using the HSM's public key received earlier (see F.5.3).

5.    The ATM's EPP decrypts the master key using the EPP's secret key which was loaded into the EPP during manufacture.

6.    The ATM's EPP stores the A-key for decrypting session keys (see F.5.7).

7.    The ATM sends the KVC (aka KVV) of the master key to the host in an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '3' - 'New KVV for key just loaded'.

8.    The host compares the KVC with the KVC returned by SCM function C720. If they do not match, the host displays a console message[5].

## F.5.6    Manual Load

As an alternative to remote initialisation, items F.5.1 - F.5.5 can be replaced by a manual load of the double-length ATM Master Key in two double-length components:
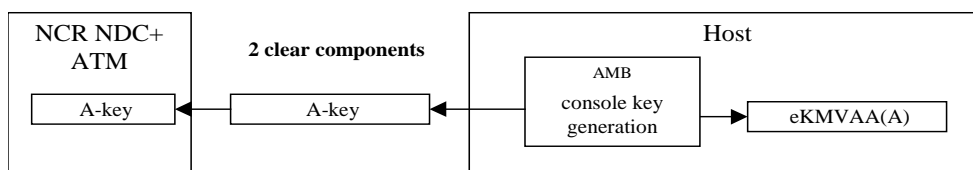


**Figure 5 Generation of double-length master key for manual loading**

1.    The host uses a custom key generation command on the SCM console to generate a random double-length ATM master key.

2.    The host stores the ATM master key, encrypted under a variant of the domain master key, for encrypting session keys (see F.5.7).

3.    The host prints two clear double-length components of the ATM master key in sealed key mailers.

4.    The clear components of the ATM master key are loaded into the ATM as the A-key.

---

[5] The master key has been loaded incorrectly on the ATM. Session key loads will be unsuccessful.

### F.5.7 Generation of double-length session keys
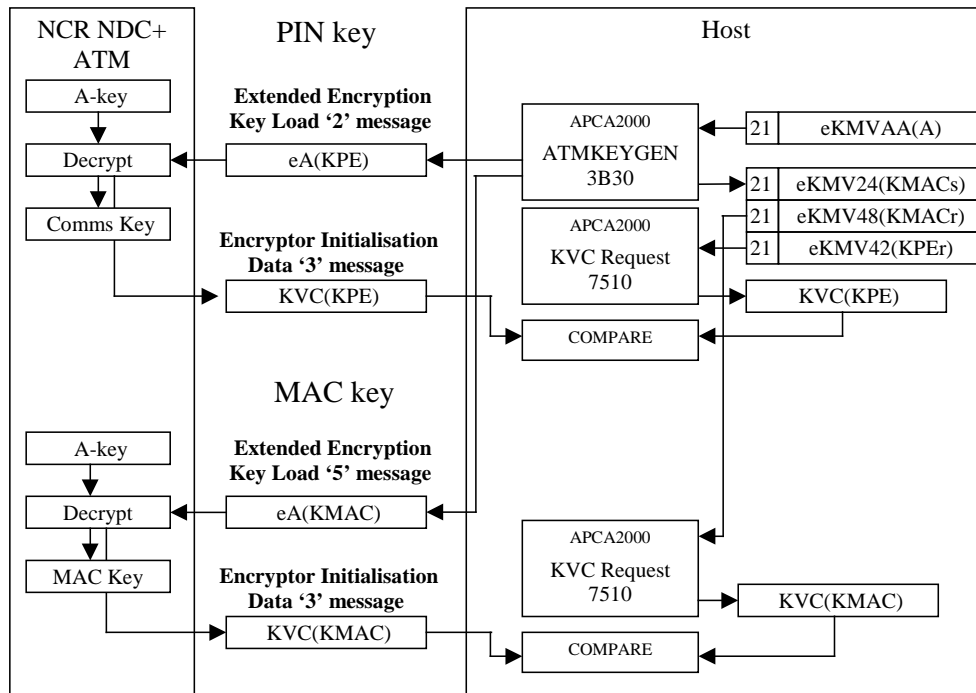


**Figure 6 Generation of double-length session keys**

### F.5.8 PIN and MAC keys

1. The host uses SCM function 3B30 to generate random double-length PIN encryption and MAC keys. This function is called with the key length set to 2 (double) and the cipher mode set to 0 (ECB). It encrypts the session keys with the master key generated earlier (see F.5.4).

2. The host stores the PIN encryption key, encrypted under a variant of the domain master key, for decrypting PIN blocks (see F.5.11).

3. The host stores the MAC key, encrypted under variants of the domain master key, for generating and verifying MACs (see F.5.12 and F.5.13).

4. The host uses SCM function 7510 to calculate the KVCs of the PIN encryption key and the MAC key.

### F.5.9 PIN key

1. The host sends the encrypted PIN encryption key to the ATM in an Extended Encryption Key Load message (Message Class 3, Message Sub-class 4) with Modifier '2' - 'Decipher new communications key with current master key'.

2. The ATM's EPP decrypts the communications key and stores it for encrypting PIN blocks see (F.5.11).

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

3.  The ATM sends the KVC of the communications key to the host in an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '3' - 'New KVV for key just loaded'.

4.  The host compares the KVC of the communications key with the KVC returned by SCM function 7510.  If they do not match, the host displays a console message[6].

## F.5.10     MAC key

1.  The host sends the encrypted MAC key to the ATM in an Extended Encryption Key Load message (Message Class 3, Message Sub-class 4) with Modifier '5' - 'Decipher new MAC key with current master key'.

2.  The ATM's EPP decrypts the MAC key and stores it for generating and verifying MACs (see F.5.12 and F.5.13).

3.  The ATM sends the KVC of the MAC key to the host in an Encryptor Initialisation Data message (Message Class 2, Message Sub-class 3) with Information Identifier '3' - 'New KVV for key just loaded'.

4.  The host compares the KVC of the MAC key with the KVC returned by SCM function 7510.  If they do not match, the host displays a console message[7].

## F.5.11     PIN translation with double-length session key
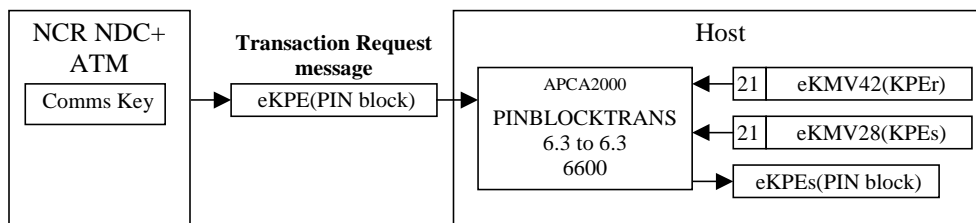


**Figure 7 PIN translation with double-length session key**

1.  The ATM is configured to encrypt the PIN block with the ATM Comms key. Prior to encryption, the ATM's EPP formats the PIN in an AS 2805.3.1 format 0 PIN block (same as ISO format 0). <sub>Amended effective 29.4.16</sub>

2.  The ATM sends the encrypted PIN block in a Transaction Request message (Message Class 1, Message Sub-class 1).

---

[6] The communications key has been loaded incorrectly on the ATM. PIN decryption will be unsuccessful.
[7] The MAC key has been loaded incorrectly on the ATM. MAC verification will be unsuccessful.

---

3. The host uses SCM function 6600 to translate the PIN block from encryption under the PIN encryption receive key to encryption under the PIN encryption send key. The PIN encryption receive key is the same as the ATM's Communications key (see F.5.7). The PIN encryption send key is the host's Switch Working Key[8].

4. For an 'on us' transaction, the host uses the translated PIN block to verify the PIN. For a 'not on us' transaction, the host performs a second PIN translation to encrypt it under the issuer's PIN encryption key.

### F.5.12   MAC generation with double-length session key
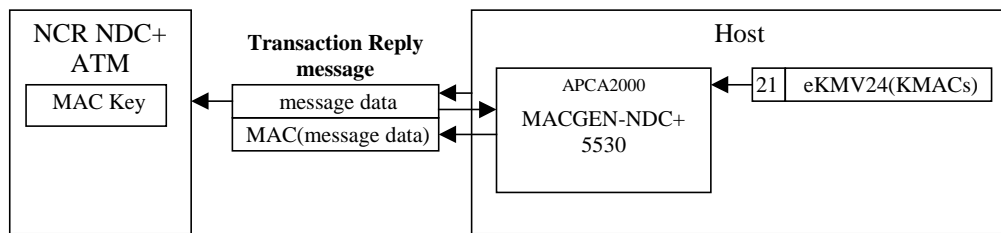


**Figure 8 MAC generation with double-length session key**

1. The host uses SCM function 5530 to generate the MAC. The MAC send key is the same as the ATM's MAC key (see F.5.7). The MAC algorithm used by SCM function 5530 will be standardised as MAC algorithm 3 in the amendment to AS 2805.4.1 which is under preparation by the IT-5-4 committee. The MAC is calculated over the entire message.

2. The host sends the MAC in a Transaction Reply message (Message Class 4).

3. The ATM is configured to verify the MAC in the message data with the ATM MAC key.

### F.5.13   MAC verification with double-length session key



**Figure 9 MAC verification with double-length session key**

1. The ATM is configured to MAC the message data with the ATM MAC key.

---

[8] Assuming the host uses a SWK to encrypt all PIN blocks during internal processing on the switch.

2.  The ATM sends the MAC in a Transaction Request message (Message Class 1, Message Sub-class 1).
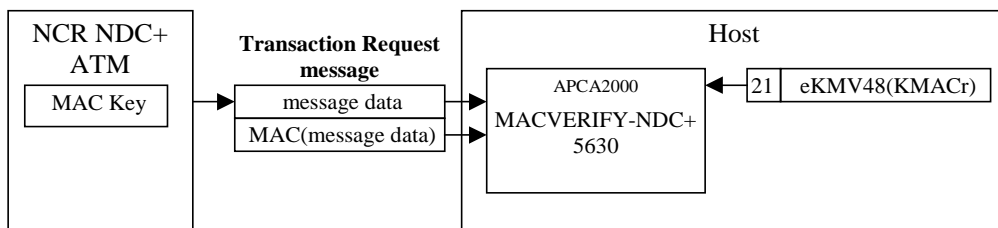
3.  The host uses SCM function 5630 to verify the MAC.  The MAC receive key is the same as the ATM's MAC key (see F.5.7).  The MAC algorithm used by SCM function 5630 is MAC algorithm 2 from AS 2805.4.1 (functionally equivalent to MAC algorithm 3 in ISO 9797-1).  The MAC is calculated over the entire message.

## F.6     EFTPOS Terminals - 3DES

Key management is accomplished by the exchange of messages between Terminal and host system(s), and the execution of complementary cryptographic functions by the Terminal and host application software.  The following diagrams and descriptions are indicative of the messages and functions needed to support remote initialisation and session key management.  Only those message fields relevant to key management are shown.

For remote initialisation, three RSA key pairs are used.  The modulus of each key pair is nominally 1024 bits in size, but the actual sizes are constrained to prevent reblocking for operations involving more than one key pair:

1.  The manufacturer's key (SKman, PKman) is 1024 bits, stored on the host as 16 8-byte blocks ($1024 = 16 \times 8 \times 8$).

2.  The Terminal's key (SKtcu, PKtcu) is 960 bits, so that its modulus or exponent can be signed by SKman, which is one block bigger ($960 = 15 \times 8 \times 8$).

3.  The sponsor's key (SKsp, PKsp) is 896 bits, so that data (*KI, etc) enciphered with this key can be signed by SKtcu, which is one block bigger ($896 = 14 \times 8 \times 8$).

### F.6.1     Key Loading of a Terminal by the Manufacturer
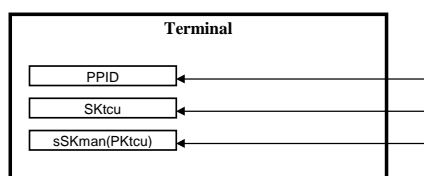


**Figure 10 Key Loading of a Terminal by the Manufacturer**

The following items are loaded into the Terminal by manufacturer in a secure area before the Terminal is installed in the field:

1.  PPID: a unique PIN pad identifier consisting of 16 decimal digits.  The PPID includes a manufacturer code, year and month of manufacturer, and a unique PIN pad serial number.

---

2.  SKtcu: the secret key of the TCU.  The modulus of this key contains 960 significant bits.

3.  sSKman(PKtcu): the public key of the TCU, signed with the secret key of the manufacturer.

The TCU key pair is statistically unique for each Terminal manufactured.

### F.6.2    Key Loading and Generation by the Sponsor
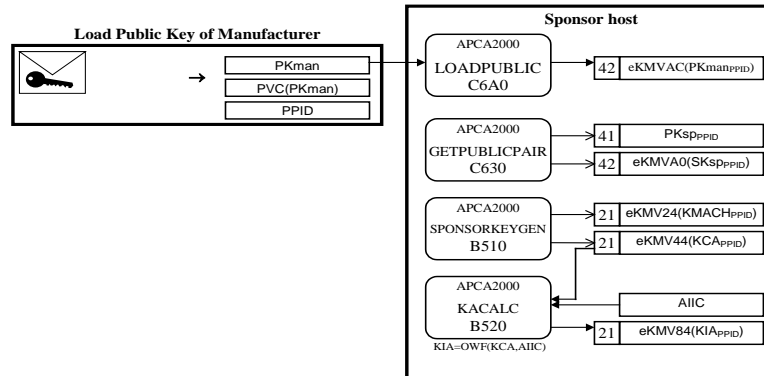


**Figure 11 Key Loading and Generation by the Sponsor**

1.  The PPID of the Terminal and the manufacturer's public key are communicated to the sponsor in a secure manner.  The sponsor loads the manufacturer's public key on the host system.  The manufacturer can use the same public key for all Terminals for this sponsor, or for batches of Terminals for this sponsor, but it must not be disclosed to any other party. The modulus of this key contains 1024 significant bits.

2.  The sponsor generates a public and secret key pair.  The same key pair may be used for all Terminals or for batches of Terminals.  The modulus of these keys contains 896 significant bits.

3.  The sponsor generates a random cross acquirer key (KCA) and MAC housekeeping key (KMACH).

4.  The sponsor uses the KCA to derive the sponsor's acquirer initialisation key (KIA) using the sponsor's Acquiring Institution Identification Code (AIIC).

These are all off-line procedures performed by the sponsor before the Terminal is installed.

---

### F.6.3 Key Transmission to an Acquirer
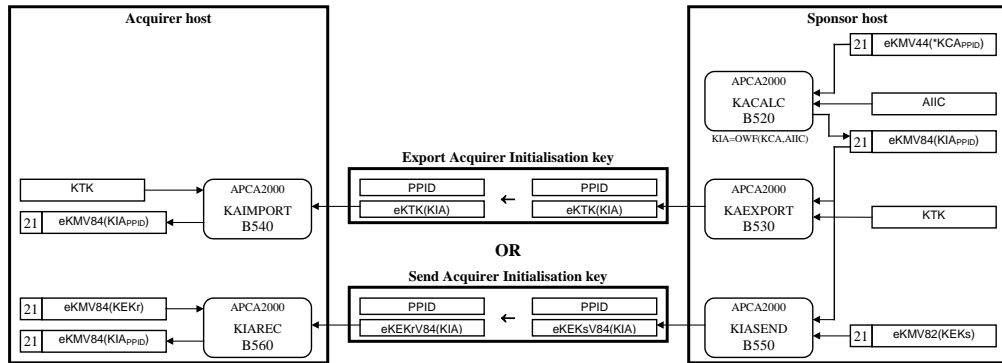


**Figure 12 Key Transmission to an Acquirer**

For multi-acquirer Terminals, the sponsor conveys the acquirer initialisation key (KIA) for each Terminal to each acquirer. The KIA is encrypted for transmission using either a key transport key (KTK) or a Key encrypting Key (KEK). The KTK or KEK will have been previously loaded into the SCM of sponsor and acquirer. These are off-line procedures performed by the sponsor and acquirer(s) before the Terminal is installed.

### F.6.4 Remote Initialisation of a Terminal by the Sponsor
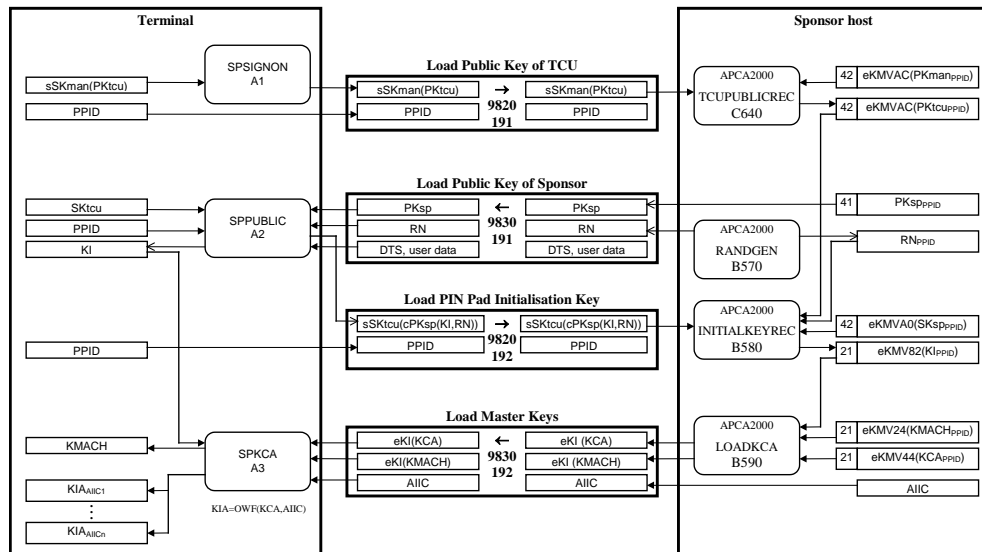


**Figure 13 Remote Initialisation of a Terminal by the Sponsor**

1. The Terminal sends the public key of the TCU, signed by the secret key of the manufacturer. The sponsor unsigns the TCU public key with the public key of the manufacturer.

2. The sponsor sends the public key of the sponsor, along with a random number (RN), a date time stamp (DTS), and user data.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

3. The Terminal generates a random Terminal initialisation key (KI), and enciphers it with the public key of the sponsor, along with the random number RN, the PPID, the DTS, and the user data. The cipher text is signed with the secret key of the TCU and sent to the sponsor.

4. The sponsor unsigns and deciphers the message, checks the RN, PPID, DTS, and user data, and saves the KI.

5. The sponsor sends the cross acquirer key (KCA) and MAC housekeeping key (KMACH) to the Terminal, encrypted under the KI.

6. The Terminal decrypts the KCA and KMACH with KI, which is then erased. The Terminal uses KCA to derive the acquirer initialisation key (KIA) for each acquirer in its acquirer table. The KCA is then erased.

Remote initialisation is performed when a Terminal is first installed in the field. It is initiated by a password-protected command entered on the Terminal. It will be necessary to repeat the remote initialisation if the Terminal cannot log on to an acquirer using either KEK1 or KEK2, implying that the values of KEK2 have become out of step between Terminal and acquirer. This is expected to be happen infrequently - no more than once per year.

## F.6.5 Remote Initialisation of a Terminal by an Acquirer
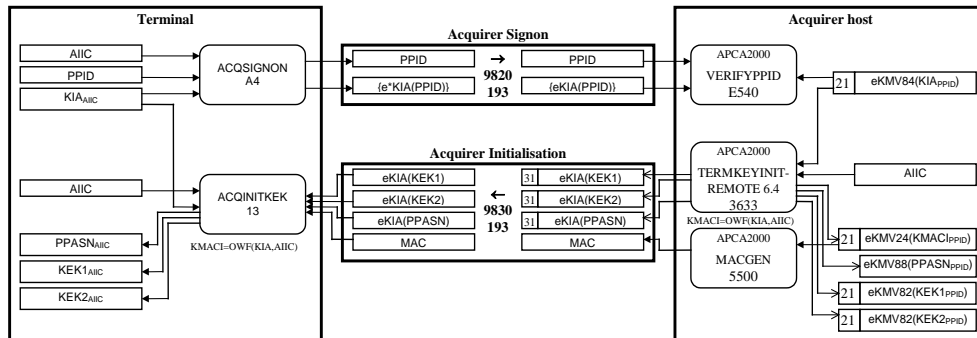


**Figure 14 Remote Initialisation of a Terminal by an Acquirer**

The Terminal performs this procedure for each acquirer in its acquirer table (the sponsor being the first acquirer).

1. The Terminal encrypts the PPID with the acquirer's KIA and sends the high-order 32 bits to the acquirer.

2. The acquirer verifies that the encrypted PPID is correct, thereby confirming that the Terminal is using a genuine KIA.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

3.  The sponsor generates random initial values for KEK1, KEK2, and the PIN pad acquirer security number (PPASN). These are encrypted under KIA and sent to the Terminal. The sponsor derives an initial MAC key (KMACI) from the KIA and the AIIC and uses it to generate a MAC for the message containing the encrypted keys.

4.  The Terminal also derives KMACI and uses it to verify the MAC on the message.

5.  The Terminal decrypts KEK1, KEK2, and PPASN and stores them in its key storage memory for the acquirer. The KIA for this acquirer is then erased.

Note that functions E540 and 3633 can both be supplied with the encrypted KIA eKMV84(KIA) in format 23 (ECB-encrypted) as well as format 21 (CBC-encrypted). A format 23 KIA can be constructed from the e*KMV8(*KIA) produced for 1DES POS Terminals. This would allow support of a hybrid POS Terminal which performed remote initialisation with 512-bit RSA keys but performed 3DES session key management. It is may be AusPayNet's intention, however, to discontinue support for a format 23 KIA when 3DES migration is complete.

## F.6.6    Logon by a Terminal to an Acquirer
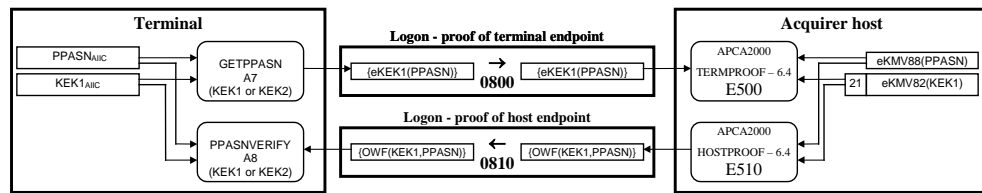


**Figure 15 Logon by a Terminal to an Acquirer**

1.  The Terminal sends the acquirer a cryptographic function of KEK1 and PPASN which the acquirer verifies to prove that the Terminal is genuine.

2.  The acquirer sends the Terminal a cryptographic function of KEK1 and PPASN which the Terminal verifies to prove that the acquirer is genuine.

This is just the cryptographic part of Terminal logon - other functions are performed by Terminal and acquirer at the same time. Proof of endpoint is normally performed with KEK1, as indicated by a flag in the messages. If proof of endpoint is unsuccessful with KEK1, suggesting that transformation of KEK1 has become out of step between Terminal and acquirer, proof of endpoint is attempted with KEK2.

A session key change, as described below, is performed immediately after a successful proof of endpoint.

### F.6.7 Session Key Change by an Acquirer
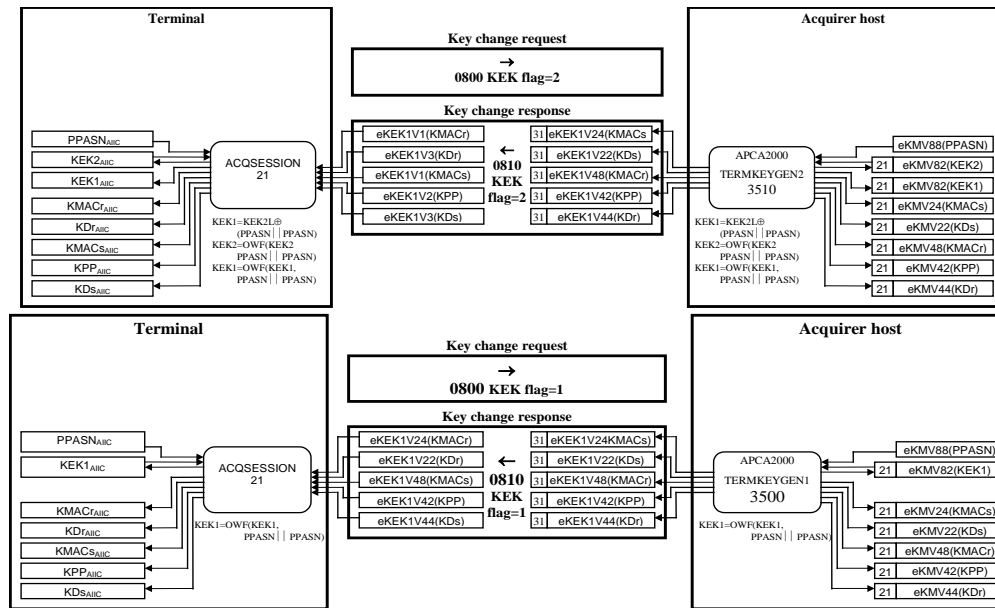


**Figure 16 Session Key Change by an Acquirer**

1.  The acquirer responds to a key change request by generating a set of random double-length session keys, encrypting them under variants of KEK1, and sending them to the Terminal. The KEK1 is transformed by a one way function before it is used.

2.  The Terminal transforms KEK1, and decrypts the session keys.

Note that the format 31 session keys generated by functions 3500 and 3510 are CBC-enciphered and that the variants of KEK1 or KEK2 are the ones shown in section F.4 (with C0 in alternate bytes).

Session key change is normally performed with KEK1, as indicated by a flag in the messages. If the key verification codes are incorrect, suggesting that transformation of KEK1 has become out of step between Terminal and acquirer, a session key change is attempted with KEK2. This causes both acquirer and Terminal to derive a new KEK1 from KEK2 and transform KEK2 with a one way function. A session key change with KEK2 is also requested after doing a KEK2 proof of endpoint during Terminal logon.

Although the key change request originates from the Terminal, each acquirer host can effectively control the frequency of session key changes by setting a "key change required" flag in a previous message to the Terminal, such as a financial transaction response.

---

### F.6.8 Financial Transaction from a Terminal to an Acquirer
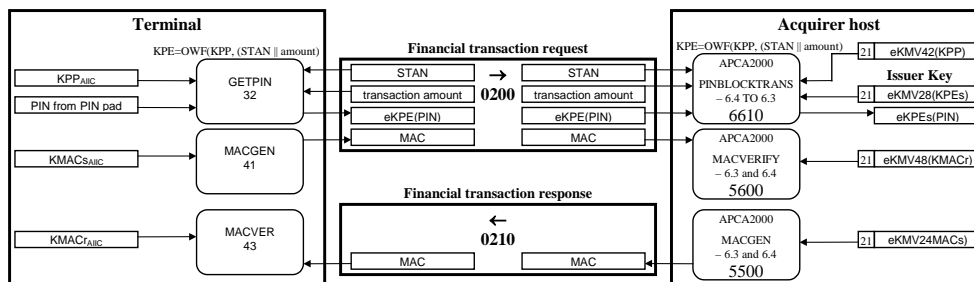


**Figure 17 Financial Transaction from a Terminal to an Acquirer**

1.  The Terminal encrypts the PIN (entered by the customer on the PIN pad) using a PIN encryption key KPE which is derived from the PIN protection key (KPP) combined with the STAN and amount of the transaction. A MAC is generated on the financial transaction request message using the MAC session key (KMACs).

2.  The acquirer verifies the MAC using the MAC session key (KMACr).

3.  If the acquirer is the card issuer for the transaction (or is standing in for the card issuer), the customer's PIN is verified using the issuer's PIN verification key. Otherwise the transaction is switched to the card issuer for PIN verification - this is the case illustrated above, where the PIN block is translated to encryption under the KPEs for the issuer. The KPE used to decrypt the incoming PIN block for verification or translation is derived from the KPP, STAN, and amount, as on the Terminal.

4.  The acquirer generates a MAC on the financial transaction response message using the MAC session key (KMACs).

5.  The Terminal verifies the MAC on the financial transaction response message using the MAC session key (KMACr).

### F.7 Glossary

**3DES** Triple DES encipherment, performed by **three** 56-bit DES operations. Same as DEA 3 if 112-bit keys are used (as they are in SCM Spec).

**AES** Advanced Encryption Standard - a new encryption algorithm which is the US standard to replace DES.

**AMB** Australian Major Banks - an industry standard set of SCM functions.

**AusPayNet** Australian Payments Network Limited - the industry body which regulates EFT interchange.

**AusPayNet TSSC** The AusPayNet Technical Security Sub-Committee - a committee of security experts from the Australian EFT industry.

Amended effective 20.8.18

---

**CBC** Cipher Block Chaining - a mode of operation of DEA 1 or DEA 3 in which each 64-bit block of enciphered data is dependent on the previous block.

**DEA 1** Data Encipherment Algorithm with 56-bit keys, same as DES.

**DEA 3** Data Encipherment Algorithm with 112-bit keys, performed by three 56-bit DEA 1 operations.

**DES** Data Encryption Standard algorithm with 56-bit keys.

**Double-length Key** A 128-bit cryptographic key of which 112-bits are used for encipherment, 16 bits for parity checking.

**ECB** Electronic Code Book - a mode of operation of DEA 1 and DEA 3 in which each 64-bit block of data is enciphered independently.

**EPP** Encrypting PIN Pad - the component of an ATM which captures PINs and performs cryptographic functions.

**Host** The processing system which drives ATM and EFTPOS Terminals. It runs EFT application software and sends function requests to an SCM.   <sub>Amended effective 20.8.18</sub>

**Interchange** The exchange of EFT messages between acquirers of EFT transactions and card issuers.

**Inversion** In the context of proof-of-endpoint, inversion of a random number, shown by the symbol "~", means a ones complement operation, equivalent to exclusive OR with the hexadecimal constant FFFFFFFFFFFFFFFF.

**KEK** Key Encipherment Key - a cryptographic key used to encipher another cryptographic key.

**Key Management** The secure exchange and storage of cryptographic keys.

**Keyblock** A data structure used to store enciphered cryptographic keys.

**KM** A Master Key, stored in an SCM, which is used to encipher cryptographic keys stored on the host.

**KM index** The ordinal number of a particular master key (KM), in an SCM which can hold more than one master key.

**KVC** Key Verification Code. A value, derived from a cryptographic key, which is used to verify that the key is correct. Same as KVC.

**KVV** Key Verification Value. A value, derived from a cryptographic key, which is used to verify that the key is correct. Same as KVV.

**SCM** Security Control Module - a physically secure server which performs cryptographic functions.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

**SCM Spec** The SCM specification published by AusPayNet TSSC to support 3DES.

**SWK** Switch Working Key, key used to encrypt all PIN blocks during internal processing on an EFT switch.

**Session key** A cryptographic key used for a session of limited duration before being replaced, under dynamic key management.

**Single-length Key** A 64-bit cryptographic key of which 56-bits are used for encipherment, 8 bits for parity checking.

**Variant** A constant which is used to modify a KEK or KM before it is used to encipher another key, to enforce key separation. Different types of key are enciphered with different variants, so that they can only be used in the appropriate SCM functions.

**The next page is G.1**

## ANNEXURE G. DEVICE APPROVAL PROCESS

### G.1 Introduction

### G.1.1 Operation

This Annexure sets out the Company's process for device approval applications and the requirements for Device Approval Applicants and Approved Evaluation Facilities. The Annexure operates as follows:

(a) It does not form an operative provision of the IAC Code Set.

(b) By submitting a device approval application or a delta approval application, a Device Approval Applicant agrees to comply with the applicable terms of this Annexure.

(c) By applying to become an Approved Evaluation Facility, the evaluation facility agrees to comply with applicable terms of this Annexure.

### G.1.2 Interpretation

(a) The words defined in Part 1.3 of the IAC Code Set Volume 4 have the same meaning in this Annexure unless a contrary intention appears.

(b) In this Annexure, 'device approval application' and related 'device' and 'SCD' references include, when necessary and relevant:

(i) 'SPoC Solution', 'SPoC Solution approval application' and related 'SPoC Solution' references; and

(ii) 'CPoC Solution', 'CPoC Solution approval application' and related 'CPoC Solution' references; and

(iii) in considering an application for approval of a non-standard POI Technology, 'non-standard POI Technology approval application' and related 'non-standard POI Technology' references.

### G.1.3 Purpose

Part 1.1 of IAC Code Set Volume 4 states that the purpose of the IAC is to provide framework for participants in card payments in Australia to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. In the context of device approvals, that purpose includes balancing the interest of maintaining the security and integrity of Australian Card Payments with the interest of promoting innovation and competition.

**G.2      Device approval criteria**

The following are factors which the Company must consider in determining a device approval application under Part 3.1 of IAC Code Set Volume 4:

(a)    the Evaluation Report, including the results of the testing process;

(b)    the Device Security Standards in Part 2 of IAC Code Set Volume 4 as required under Part 3; and

(c)    in relation to a device containing non-standard technologies, also:

   (i)     any criteria referenced in Schedule 1 'Process for Considering Non-Standard Technologies at the Point of Interaction' (NST Process), as updated from time to time;

   (ii)    any other criteria agreed upon by the Company and Device Approval Applicant.

**G.3      Approved Evaluation Facilities**

**G.3.1    Introduction**

This Part G.3 documents the process for accreditation by the Company to perform Secure Cryptographic Device (SCD) security testing.  The following clauses identify the requirements a prospective Approved Evaluation Facility ("a Test Laboratory") must meet in order to qualify for accreditation by the Company for conducting device evaluations to the IAC security requirements.

**G.3.2    Initiation**

Test Laboratories applying for accreditation as Approved Evaluation Facilities should initiate the process by contacting the Senior Manager Operations, AusPayNet.  To minimise the associated time frames, Test Laboratories should submit all required materials and evidentiary matter in a single package. Subsequent to the receipt by the Company of all prerequisite materials, a minimum of six weeks is required for processing.  Where required, testing of device artefacts may result in more extended time frames.

**G.3.3    Accreditation Process**

(a)    To gain accreditation for SCD security testing, the Test Laboratory must successfully complete the Company's Evaluation Facility accreditation process described below.  The accreditation process has three components:

   (i)     Business Review;

   (ii)    Technical Review;

(iii)     On-site Visit.

(b)     The Company may require, at its sole discretion, that an Approved Evaluation Facility provide evidence of its continued compliance with the accreditation process requirements triennially.

(c)     Once a Test Laboratory has been approved by the Company to perform SCD security testing, it will be listed on the AusPayNet website as an Approved Evaluation Facility, and it can offer its services to Device Approval Applicants.   The Approved Evaluation Facility must perform testing as described in the following documents:

(i)     AS 2805.14.1 Secure Cryptographic Devices, concepts, requirements and evaluation methods;

(ii)     AS 2805.14.2 Secure Cryptographic Devices – Security Compliance Checklists; and

(iii)     Code Set Volume 4 Part 2 – Device Security Standards.

## G.3.4     Business Review

The Test Laboratory must complete a business review with the Company.  This review requires that the Test Laboratory meet a minimum required standard acceptable to the Company for conducting business with the highest ethical standards.  The business review covers areas including, but not limited to, Due Diligence and Independence.

### G.3.4.1     *Due Diligence*

Establishes the potential business relationship with the Company and its Members, the nature of services to be provided, a review of the last two years financial statements and a background check on the key executives within the organisation.  The purpose of this review is to provide the Company with a clear understanding of the Test Laboratory's capabilities and business practices.

### G.3.4.2     *Independence*

(a)     The Test Laboratory must demonstrate its independence from any SCD manufacturer or vendor.

(i)     The Test Laboratory must not be owned in whole or in part by any SCD manufacturer or vendor.

(ii)     Evaluations will not be accepted from any Approved Evaluation Facility if the customer whose products being evaluated represent more than 10% of the facility's prior two years annual revenue.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

(b)    The Test Laboratory must be able to demonstrate its independence of its review.  Evaluations will not be accepted from an Approved Evaluation Facility where the AEF designed the product being evaluated or was involved in its design.

### G.3.5    Technical Review

The Test Laboratory must complete a due diligence technical review with the Company.  This review requires that the Test Laboratory meet certain minimum technical requirements set forth by the Company.  The technical review covers areas such as Laboratory Accreditation, Personnel Requirements, Equipment Requirements, Reference Library and Demonstrated Ability.

### G.3.5.1    *Laboratory Accreditation Checklist*

(a)    The Test Laboratory must complete and submit the IAC Laboratory Accreditation Checklist (Volume 4- Annexure E).  This material addresses such areas as:

    (i)      Organisation and Management;

    (ii)     Quality Assurance function;

    (iii)    Skill sets of personnel;

    (iv)    Adequacy of the facilities;

    (v)     Appropriateness of equipment and reference materials;

    (vi)    Equipment and software configuration management;

    (vii)   Testing methodologies employed;

    (viii)  Records management; and

    (ix)    Qualities of reports issued.

(b)    In addition, the Test Laboratory must specifically provide the information in clauses G.3.5.2 to G.3.5.6.

### G.3.5.2    *Accreditations and Certifications*

(a)    The Test Laboratory must provide current evidence of all accreditations claimed.  These may include accreditation under the relevant national implementation of AS ISO/IEC 17025 (Criteria for the competence of testing and calibration laboratories), AS/NZS ISO 9000 (Quality management systems), AS ISO/IEC 15408 series (Common Criteria for IT security evaluations) or other similar international, national, or industry standards.

(b) The Test Laboratory must also provide evidence of sponsorship or endorsement by a recognized payment scheme engaged in the processing of PIN Transactions (either a global payment scheme or a multi-Member national debit network/network). The sponsorship or endorsement must include the testing of cryptographic devices to a prescribed set of security requirements.

### G.3.5.3 Personnel Requirements

The Test Laboratory must provide a listing of personnel who will work on evaluations submitted for the Company's consideration, along with their qualifications. Qualifications should include formal and informal training, length and type of experience in doing related evaluation work. The list should include their specific role(s) in the evaluation process. This listing should be updated annually and must be made available to the Company upon request.

### G.3.5.4 Equipment Requirements

The Test Laboratory must provide a listing of the relevant "standard" test equipment that is owned by the Test Laboratory, and any relevant "specialised" test equipment that is owned by the Test Laboratory or available for rent or contract service.

### G.3.5.5 Reference Library

The Test Laboratory must provide a listing of reference materials that are resident at the Test Laboratory. Reference materials should include, but not be limited to, books, articles and proceedings that relate to the testing of cryptographic devices (e.g., cryptography, threats and attacks, etc.). Reference materials should also include industry standards and specifications for testing cryptographic devices (e.g., ISO and National Standards).

### G.3.5.6 Demonstrated Ability

(a) The Test Laboratory must provide a test report for a cryptographic device completed by the Test Laboratory within twelve months of the application for accreditation. The test report must document the results of a security evaluation of a cryptographic device, preferably a PIN Entry Device. The test report submitted must be current, and demonstrate the Test Laboratory's ability to assess the cryptographic device against a defined set of security characteristics and assess the device's overall strengths and vulnerabilities from a physical and logical security perspective. This must be accompanied by documentation of the relevant standards and requirements that form the basis for the evaluation.

(b) The Company requires that the test report be accompanied by a letter of permission signed by the applicant for the evaluation. The letter of permission must state that the applicant permits the test report to be reviewed by the Company, and kept by the Company for its records.

(c)     The Company may also require the Test Laboratory to examine a test artefact (PED) with one or more features that are not in compliance with the IAC SCD Security Requirements. The Test Laboratory must discover the nonconformities, document them, and indicate which IAC SCD Security Requirements have failed due to the presence of the nonconformities. The Test Laboratory must bear the costs of this process and, in addition, compensate the Company for the costs of completing a concurrent evaluation of the same device via an Approved Evaluation Facility.

### G.3.6     On Site Visit

The Company, or a third party acting on behalf of the Company, may visit the Test Laboratory. The purpose of the visit is twofold:

(a)     to inspect the Test Laboratory and validate that the Test Laboratory is in compliance with the documentation provided to the Company under clauses G.3.4 and G.3.5; and

(b)     to discuss security-testing issues with the Test Laboratory's staff.

### G.3.7     Other Accreditations

The Company may, at its sole discretion, accept existing accreditations with other bodies, as meeting part or all of the accreditation process requirements of this Part G.3.

### G.4     Process for Standard Technology Device Approvals

This part sets out the device approval process for standard technologies. Device Approval Applicants (when submitting a device approval application) and AEFs (when preparing and submitting an Evaluation Report) must also follow the requirements in Annexure C 'Device Evaluation FAQs' to the IAC Code Set Volume 4.

### G.4.1     Engagement to AEF to produce Evaluation Report

(a)     The AEF and Device Approval Applicant must directly enter into a contract and any necessary non-disclosure agreements for the conduct of all testing to be carried out under clause G.4.2. If a device is submitted for examination under clause G.4.2(d) such contract must authorise the disclosure of any relevant PCI Evaluation Report by the AEF to the Company.

(b)     The costs and expenses incurred in securing approval for a device are the responsibility of the relevant Device Approval Applicant. The Company may levy a fee to cover its reasonable costs (if any) in supporting the evaluation of any particular device.

(c)     Documents to be provided by Device Approval Applicant to AEF:

Rules and guidance for privacy shielding using the external physical environment must be provided to the Approved Evaluation Facility, for evaluation.

**G.4.2**     **AEF review and preparation of Evaluation Report**

(a)     The AEF must evaluate and consider the compliance of the device with the standards at Part 2 and Part 3.1 of Code Set Volume 4.

(b)     Only those checklists appropriate to the characteristics and function of the device must be evaluated. In addition to these checklists the AEF must use such additional tests as its knowledge and experience dictate.

(c)     The Evaluation Report must contain:

(i)      the list of all pertinent documentation used in the evaluation;

(ii)     a completed list of all successful or failed tests;

(iii)    the name of the Device Approval Applicant;

(iv)     the name of the AEF;

(v)      the date of the evaluation;

(vi)     identification of the device (model name, hardware version, firmware version and application version);

(vii)    completed SCD checklists;

(viii)   advised deployment environment (as advised by the Applicant);

(ix)     details of the examination and testing process followed in developing the report; and

(x)      if the examination is conducted pursuant to clause G.4.2(d), a copy of the PCI Evaluation Report and PCI Plus Evaluation report.

(d)     Where conducting a PCI Plus evaluation, the AEF must submit:

(i)      a PCI Evaluation Report; and

(ii)     a PCI Plus Evaluation Report, which must explicitly state whether or not the device complies with the Company's feasibility requirements set out herein;

to the Company in support of the Device Approval Applicant's application for approval of such device under the IAC Code Set.

(e) The AEF must submit a copy of the Evaluation Report and any relevant PCI Evaluation Reports (if applicable), directly to the Company.

(f) The Device Approval Applicant must arrange with the AEF consent release forms so that it has permission to release the PCI Evaluation Report to the Company.

### G.4.3 Company review of device approval application

(a) The Company will review the device approval application in accordance with the device approval criteria at Part G.2 of this Annexure.

(b) If the Company cannot determine a device approval application for reasons of incomplete or inadequate documentation, the Company will request further clarification and/or documentation from the Device Approval Applicant and/or AEF.

(c) The Company will endeavour to complete its review and issue its decision on the device approval application, within 6 weeks of receiving the Evaluation Report. Matters which can increase the time it takes the Company to issue its decision include:

(i) whether the Company has further requests for information of the Approved Evaluation Facility and/or Device Approval Applicant, and if so, the speed with which appropriate responses are provided to the Company; and

(ii) whether the device contains new technology.

(d) The Company will determine whether to approve a device in accordance with Part G.8 of this Annexure, and if so, whether any conditions should be attached to the approval.

### G.5 Process for Non-Standard Technology Device Approvals

(a) The process for non-standard technology device approvals is described in 'Process for Considering Non-Standard Technologies at the Point of Interaction' (NST Process), which is Schedule 1 to this Annexure.

(b) The Company will review the device approval application in accordance with the device approval criteria at Part G.2 of this Annexure.

(c) The Company will determine whether to approve a device in accordance with Part G.8 of this Annexure.

---

**G.6 Delta approval of an approved device**

(a) Where there are proposed changes to the device software and/or minor hardware modifications to an Approved Device, the Device Approval Applicant must apply to the Company for delta approval of the Approved Device.

(b) To apply for delta approval, the Device Approval Applicant must follow the Process for Standard Technology Device Approvals in Part G.4 of this Annexure, save that the Evaluation Report need only address the software and/or minor hardware modifications to the approved device.

(c) The Company will review the delta approval application in accordance with the device approval criteria at Part G.2 of this Annexure.

(d) The Company will determine whether to approve a device in accordance with Part G.8 of this Annexure, and if so, whether any conditions should be attached to the approval.

**G.7 Term of Device Approval**

(a) Devices will be approved by the Company for the Approval Period contained at Part 3.2(c) of IAC Code Set Volume 4, being three years from the date of the Letter of Approval.

(b) Pursuant to Part 3.2(d) of IAC Code Set Volume 4, at the conclusion of the Approval Period, the Company may, at its sole discretion, extend the Approval Period for a further period of three years or such other period as it deems appropriate, having regard to changes in security technology, applicable standards, security threats and/or other knowledge in the security industry.

(c) Device approvals may only be revoked by the Company prior to the expiry of the Approval Period in accordance with Part 3.2(e) of IAC Code Set Volume 4, being if the Company determines that the device should no longer be approved because the device:

(i) no longer meets the applicable standards; or

(ii) approval of the device has been withdrawn or revoked by any other relevant security standards body; or

(iii) the device is vulnerable to a significant security threat which did not exist or was not apparent at the time the device approval was granted.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

**G.8** **Decisions on device approval application**

(a) Approval

In accordance with Part 3.2(a) of IAC Code Set Volume 4, if the Company approves a device (including delta approvals), the Company will issue a Letter of Approval to the Device Approval Applicant. The Letter of Approval will state any conditions which are attached to the approval.

(b) Decline

In accordance with Part 3.2(b) of IAC Code Set Volume 4, if the Company declines to approve a device, the Company must notify the Device Approval Applicant in writing of the reasons for its decision, including the details of the unacceptable results.

(c) Delay

If the Company requests further information pursuant to clause G.4.3(b) of this Annexure, and the Device Approval Applicant or AEF does not respond within two calendar months of the request, then the Company may decline the device approval application.

(d) Revocation

If the Company decides to revoke device approval prior to expiry of the Approval Period, in accordance with Part 3.2(e) of IAC Code Set Volume 4, the Company must notify the Device Approval Applicant in writing of the reasons for its decision.

(e) Re-certification

If the Company requires the re-certification of a device in accordance with Part 3.2(g) of IAC Code Set Volume 4, the Company must notify the Device Approval Applicant in writing of the reasons for its decision.

**G.9** **Review**

(a) The Device Approval Applicant may request review of a Company decision issued in accordance with Part G.8 of this Annexure.

(b) Any request for review must be made to the Company, in writing, within 30 days of the Company's notification to the Device Approval Applicant. The request must properly detail the reasons for the requested review, including by reference to the Company's reasons for its decision.

(c) The Company must review and respond in writing to the request for review within a reasonable time depending upon the subject matter of the review request. If, following the review, the Company approves a device, the Part G.8 of this Annexure will apply.

## SCHEDULE 1    PROCESS FOR CONSIDERING NON-STANDARD TECHNOLOGIES AT THE POINT OF INTERACTION

### PART 1    INTRODUCTION

### 1.1    Background

The card payment system is seeing a surge in new products and services due to the rapid changes in available technology and the growing number of organisations entering the payments market. Many of these innovations fit within the device security standards in Part 2 of IAC Code Set Volume 4; however, some proposed solutions employ a different paradigm for protecting payments information.

The process for considering non-standard technologies at Point of Interaction (POI) has been established in order to:

1.    allow and encourage innovation;

2.    quickly address emerging technologies while limiting the potential for fraud; and

3.    act as an industry and avoid potential inconsistencies from card schemes acting individually.

### 1.2    Purpose of this document

This document provides a description of the process for reviewing and approving non-standard technologies at Point of Interaction (POI).

### 1.3    Scope

This document supports the consideration of POI technologies that can be provided to a merchant to undertake card payments. POI technologies include attended and unattended Point of Sale (POS) devices and ATMs.

A proposed POI solution / technology will be considered under this process if it would normally be required to meet any of the following Australian or global payment standards but, by nature of its design, is unable to do so:

    i)    PCI PTS;

    ii)    PCI DSS;

    iii)    IAC requirements for PIN Entry Devices (IAC Code Volume 3 - Acquirers Code); and

    iv)    EMV.

---

Excluded from scope is any solution / technology that:

a) is not intended for use at POI;

b) is expected to be able to meet each of the standards listed above (where required) but has not yet completed the certification process; or

c) is a closed loop system.

## 1.4 Review of the process

The IAF will review the process for considering non-standard technologies at Point of Interaction from time to time and at least every two years.

## PART 2 HIGH LEVEL PROCESS

## 2.1 Stages for assessing non-standard technologies at POI

The high level joint industry process for assessing non-standard technology at POI is made up of 6 stages as follows:

1. Request Phase

   a) Request for consideration of a non-standard technology by an acquirer or the IAF

2. Identification Phase

   a) Identification of existing applicable or partially applicable standards and academic research

   b) Identification of laboratories best matched for testing the non-standard technology

   c) Identification of subject matter experts

3. Technical Examination Phase

   a) Review of the device by selected laboratories

4. Assessment Phase

   a) Review of reports and assessment by AusPayNet

   b) Development of a high level risk assessment by AusPayNet

   c) Development of a pass/fail/pilot decision by AusPayNet

5. Pilot Phase

   a) A controlled pilot with strictly defined parameters including number of devices and merchant is permitted and subject to close monitoring by the Company.

6. Decision Phase

   a) Development of a pass/fail decision by AusPayNet.

## 2.2 Timing

The goal is to complete the Assessment within approximately 6 months from the time the Device Approval Applicant first approaches AusPayNet Management with a request for consideration. However, the actual timing will depend largely on the complexity of the solution, the quality of documentation received from the Device Approval Applicant, the workload of the selected laboratories and the level of support from card schemes.

## 2.3 Request for consideration

Figure 1 below highlights the steps of the request for consideration stage:
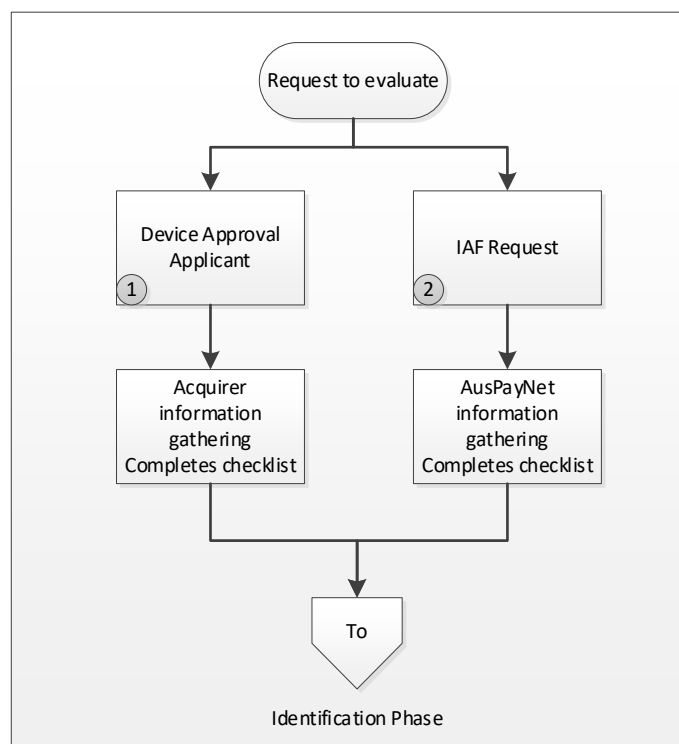


**Figure 1 – Request Phase**

1. A request for considering a non-standard technology evaluation is made to AusPayNet by the acquirer who wishes to use the device or technology (the Device Approval Applicant)[1].

2. Alternatively, the IAF may request that a non-standard technology be considered for assessment if they believe it to be beneficial to the Australian Card Payments industry as a whole.

3. The standard checklist to be completed by the Device Approval Applicant (or AusPayNet if the IAF is the Device Approval Applicant) contains information about the proposed technology (Part 3 - Initial assessment checklist).

Note: As part of the initial request, the Device Approval Applicant agrees to accept the external costs associated with the device evaluation. These costs usually need to cover technical security consulting, system testing by a specialised testing company, plus travel costs for members to attend meetings.[2] If the IAF requests that a technology should be assessed, then the costs associated with the process will be covered through AusPayNet's normal budgetary process.

The Device Approval Applicant must ensure that the Vendor is prepared to make the solution itself available to the lab for testing as part of the industry analysis.

## 2.4 Identification Phase

Figure 2 below highlights the steps of the identification phase
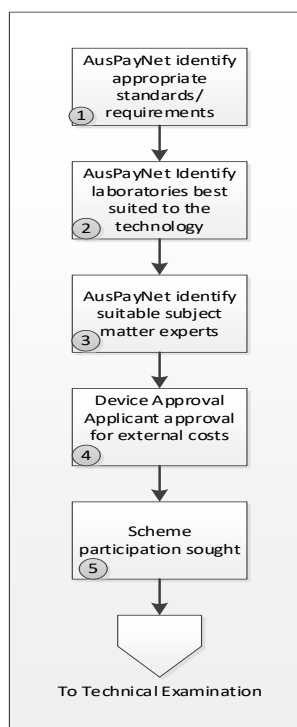


**Figure 2 – Identification Phase**

---

[1]- A primary Device Approval Applicant should be nominated if a solution has more than one acquirer.
[2]- An estimate of the expected costs will be advised to the Device Approval Applicant before any decision is made to spend the money.

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

1. AusPayNet will initially review the Initial assessment checklist and obtain the views of the card schemes with regards to the technology under consideration. AusPayNet will then identify any possible existing standards including partial or draft standards or requirements applicable to the technology involved. This research must also examine the current state of academic research in the technology being considered.

2. AusPayNet will identify any laboratories, not necessarily Approved Evaluation Facilities, with particular knowledge and/or skills in testing the technology involved.

3. AusPayNet will identify any subject matter experts willing to assist in the evaluation of the technology and estimate likely costs. Any consultants likely to be engaged must be willing to agree to AusPayNet's confidentiality requirements and any applicable terms of reference.

4. AusPayNet will advise the Device Approval Applicant of the selected laboratory (more than one laboratory is possible) and the likely estimate of external costs and obtain the Device Approval Applicant's agreement to bear those costs.

5. Having gained the Device Approval Applicant's approval for bearing the costs involved, AusPayNet may approach the card schemes requesting nominations for experts to attend and assist in the evaluation of the technology.

Prior to completing the Identification Phase, AusPayNet will ensure that appropriate contractual arrangements are in place, including:

a) Consent from the Vendor to authorise AusPayNet to access documents/personnel/premises as required by the scope of the assessment; and

b) A confidentiality undertaking between AusPayNet and the Device Approval Applicant/Vendor and any Subject Matter Experts.

## 2.5 Technical Examination Phase

Figure 3 below highlights the steps of the technical examination phase:
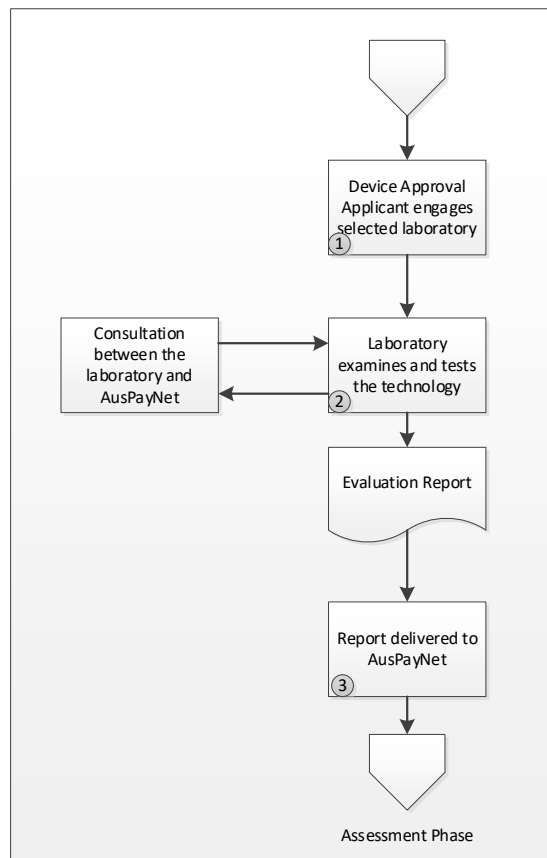


**Figure 3 – Technical Examination**

1. The Device Approval Applicant or vendor will engage the identified laboratory or laboratories if so required by AusPayNet and arrange for a review with the output report to be provided to AusPayNet. This engagement should permit an ongoing dialogue between the laboratory and AusPayNet to ensure that desired outcomes are met.

2. The laboratory will examine and test the device against standards and requirements as advised by AusPayNet and its own knowledge and skill set.

   a) The lab carries out the technical review/penetration testing[3] for any identified risks and writes a draft report including:

      i) Highlighting the risks and the effectiveness of any relevant mitigation measures in place; and

---

[3]- The card schemes may also choose to do their own testing in addition to the industry testing.

**Australian Payments Network Limited [ABN 12 055 136 519]**

ii) Areas of uncertainty and why they are not able to provide a clear statement.

3. The laboratory will provide the report to AusPayNet and the Device Approval Applicant/Vendor if required by AusPayNet:

a) Card schemes may carry out their own testing/analysis and provide AusPayNet with any additional risks that they consider as relevant for the device or technology under consideration.

## 2.6    Assessment Phase

Figure 4 below highlights the steps of the assessment phase:
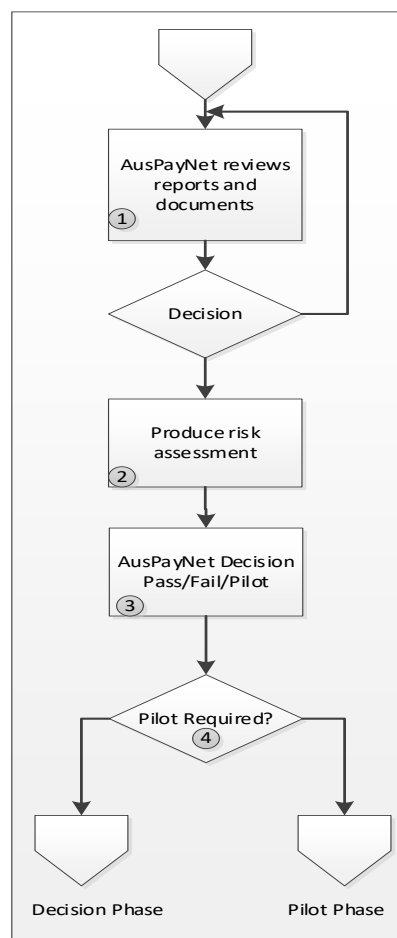


**Figure 4 – Assessment phase**

1.  AusPayNet convenes a meeting, which includes nominated experts from the schemes and the attendance of any nominated subject matter experts to review the laboratory's findings and other relevant documentation. A maximum of three meetings may occur if more information is required.

2.  AusPayNet produces a high level risk assessment of the device.

    a)  In order to facilitate the risk assessment, the Device Approval Applicant/Vendor should provide to AusPayNet any available technical documentation and/or results from previous testing, including relevant testing carried out by the card schemes in Australia or internationally.

    b)  In the risk assessment, AusPayNet will:

        •   Assess the solution against the current standards to confirm and potentially identify which requirements of the current standards are not met;

        •   Identify potential threats and risks to the payment system arising from the gaps to the current standards;

        •   Assess the controls applied by the Vendor against these potential threats and risks to the payment system;

        •   Assess the residual threats and risks to the payment system based on the combination of the potential threats and risks identified and the controls applied.

3.  AusPayNet will determine whether:

        •   to approve the device or decline to approve the device in accordance with Part 8 of the Device Approval Process; or

        •   a Pilot Phase is required and determined appropriate criteria.

## 2.7    Pilot Phase

If a pilot is recommended by AusPayNet, it can be run in line with pre-determined criteria[4] and the following assumptions:

1.  All agreed criteria are applicable to the Device Approval Applicant, not the Vendor;

2.  The Device Approval Applicant should report on performance against criteria at a pre-determined frequency;

---

[4] Such criteria (including success criteria) would be agreed with the Device Approval Applicant and card schemes.  Part 4 of this Schedule contains high level criteria for a pilot. The criteria for the pilot shall be strong enough to provide comfort to the industry that the technology is acceptable

3.  Anything that AusPayNet considers as having an impact on the suitability of the new technology whilst the pilot is running will be part of the considerations when running and assessing a pilot;

4.  The criteria may be amended by AusPayNet during the course of the pilot, although this should be a rare occurrence;

5.  Card schemes may withdraw from a pilot at any time at their own discretion if it is deemed that the pilot will create a liability or risk to their issuers, their brands or network;

6.  By undertaking the Pilot Phase, the Device Approval Applicant accepts the liability shift stated in 'Principles for Liability Shift' in Part 4 to this Schedule; and

7.  The Device Approval Applicant has the financial reserves to withstand the magnitude of liability described above.

Note:  it is acknowledged that a pilot, in and of itself, cannot be used to test whether a solution is secure.

During the course of the pilot, the Device Approval Applicant collects the data and provides it to AusPayNet in line with the agreed criteria. Card schemes receive the data in relation to their pre-determined individual criteria from the Device Approval Applicant directly.

The data provided by the Device Approval Applicant is assessed by AusPayNet Management against the pre-defined criteria.

If significant issues are identified during the course of the pilot it can be shut down prior to completion by the Device Approval Applicant, the Vendor or AusPayNet.

## 2.8     Decision Phase

Following any Pilot Phase, AusPayNet will:

*   review whether the criteria for the pilot have been met within the timeframe, and determine if the technology is suitable for broader rollout, and if a phased or full rollout is appropriate; and

*   approve or decline to approve the device, in accordance with Part 8 of the Device Approval Process.

## PART 3    INITIAL ASSESSMENT CHECKLIST

The initial assessment checklist should be completed by the Device Approval Applicant to request consideration for a non-standard technology at Point of Interaction and provided to AusPayNet in line with the process for consideration.

1- Date of submission: …../……/…..

2- Name of the Device Approval Applicant (acquirer):
.................................................................................................................................................
.................................................................................................................................................

3- Name of the Vendor (technology provider):
.................................................................................................................................................
.................................................................................................................................................

4- Name of the non-standard technology for consideration:
.................................................................................................................................................
.................................................................................................................................................

5- Software / hardware / firmware version numbers:
.................................................................................................................................................
.................................................................................................................................................

6- Provide details around the current and expected use of the technology:
.................................................................................................................................................
.................................................................................................................................................

7- Level of support from card schemes and names of contacts in Australia:
.................................................................................................................................................
.................................................................................................................................................

8- Information on markets where it is already running, for how long and the experience so far:
.................................................................................................................................................
.................................................................................................................................................

9- Incremental and economic benefits the solution delivers to stakeholders that existing solutions don't:
.................................................................................................................................................
.................................................................................................................................................

10- Description of the non-standard technology, including details around the equipment used, the security process and procedures used to manage the equipment and information about the system architecture where applicable:
.................................................................................................................................................
.................................................................................................................................................

11- What is required for merchants and/or other issuers and acquirer to adopt the solution?
.................................................................................................................................................
.................................................................................................................................................

12- Other technology that is relied upon to support the solution (e.g. mobile phone):
.................................................................................................................................................
.................................................................................................................................................

13- List (non-exhaustive) of standards that devices would be expected to be assessed against:
.................................................................................................................................................
.................................................................................................................................................

14- Details of the gap between the existing standard requirements and the new technology (why doesn't it comply with existing standard?)
.................................................................................................................................................
.................................................................................................................................................

15- Perceived risks of the non-standard technology and how can they be mitigated (impact on payment ecosystem):
.................................................................................................................................................
.................................................................................................................................................

16- How the Device Approval Applicant intends to mitigate the risks:
.................................................................................................................................................
.................................................................................................................................................

17- Evidence of any relevant certifications already obtained, failed or in progress:
.................................................................................................................................................
.................................................................................................................................................

18- Provide details of any previous independent testing that may have already been carried out:
.................................................................................................................................................
.................................................................................................................................................

19-Provide information (if available) on whether any process is already underway internationally or within Australia to establish new relevant standards:

....................................................................................................................................................

....................................................................................................................................

20- If a pilot is proposed, details of any existing plans for pilot including merchant base, numbers and target date for initiating the pilot:

....................................................................................................................................................

....................................................................................................................................

21- Any additional comments to be considered that the Device Approval Applicant deems relevant:

....................................................................................................................................................

....................................................................................................................................

## PART 4    HIGH LEVEL CRITERIA FOR PILOT

Once AusPayNet has agreed that the technology under consideration is appropriate for pilot, it will meet with the card schemes and agree on the industry criteria for pilot. It is important that the criteria for pilot are strong enough to provide comfort to the industry that the technology is acceptable for launch on the Australian market at the end of the pilot. This is because the expectation would be that if all the criteria for pilot are met within the timeframe, then the next step will be a phased or full rollout (depending on the size of the pilot).

Criteria for pilot include:

- Length of pilot (including tentative start and end dates)

- Pilot phases

- Frequency and content of reporting

- Restriction to specific states and/or concentration requirements

- Transaction types

- Eligible merchants (include anticipated number)

- Eligible devices

- Eligible cards

- Minimum number of transactions that need to be going through to consider that the technology was sufficiently tested

- % of active users that continue to use the solution throughout the pilot

---

**Australian Payments Network Limited [ABN 12 055 136 519]**

- Industry mix of merchants

- Compliance and fraud limits

- Communication (or no communication) to merchants and card holders about the risks of the technology they are piloting

- Broader communication plan for before, during and after the pilot is being run.

- Merchant training

- Fraud rate

- Surveys to users (merchant and card holders) on how comfortable they are in using the solution

- Social media response

- Any additional security testing to be done whilst the pilot is running

- Progress through relevant standards bodies or similar

- The Device Approval Applicant has the financial reserves to withstand the magnitude of liability inherent to the risk of running the pilot

Each of the criteria will be assigned a success measure for the Device Approval Applicant and AusPayNet to track during the course and at the completion of the pilot.

Note:  the card schemes may separately impose their own requirements to the Device Approval Applicant.

**Principles for Liability Shift**

- A Device Approval Applicant is responsible for card losses incurred by an Issuer, where such losses arise from the compromise of PIN and/or card data caused by the Device Approval Applicant's use of a non-standard POI technology in an approved IAC pilot during the pilot and for 2 years after the conclusion of the pilot.

- The definition of losses will be limited to chargebacks and chargeback fees associated with fraudulent use of PIN and/or card data, and costs associated with re-issuing Cards.

- Upon an Issuer identifying that the PIN and/or card data associated with the cards of two or more Issuers have been compromised at a pilot device (or group of pilot devices), the Issuer must immediately advise the Device Approval Applicant of the pilot and AusPayNet in writing.

- The standard of proof for all matters related to the pilot shall be on the balance of probabilities.

- Parties to any cost dispute shall attempt to resolve it by negotiating in good faith bilaterally prior to seeking to use AusPayNet's dispute resolution process (to be developed).

**END**