Effective:
3 July 2017
Version 005

AUSTRALIAN PAYMENTS CLEARING ASSOCIATION LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 3
Acquirers Code

Commenced 1 July 2015

Australian Payments Clearing Association Limited
Level 6, 14 Martin Place, SYDNEY NSW 2000
Telephone: (02) 9216 4888 Facsimile: (02) 9221 8057

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 3
Acquirers Code

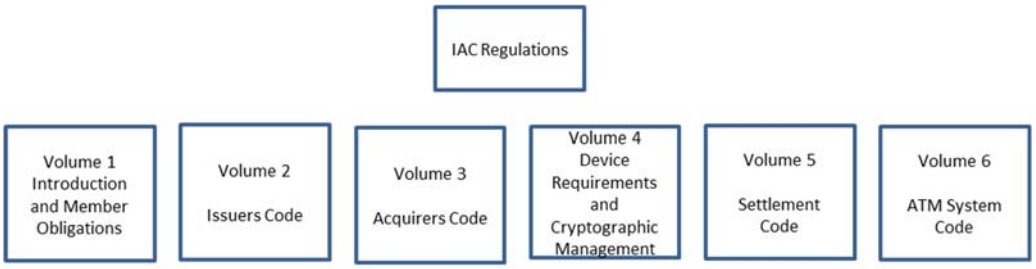
INDEX

PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this Code

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:



This volume of the IAC Manual is intended for Acquirers and when used in conjunction with Volumes 1 and 4, contains requirements for PIN and Transaction security and management that are considered mandatory for all Acquirers participating within the IAC. Part 2 of this volume covers the high level requirements for PIN security, device functionality and interchange requirements; Part 3 covers the applicable device security requirements as well as the device management requirements applying to all acquiring members participating in the IAC.

For application of the requirements, including the extent to which they apply, see Part 1 of IAC Code Set Volume 1 (Introduction and Member Obligations).

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**" means a Constitutional Corporation that in connection with a Transaction:

(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**" in relation to an Acquirer means a reference number which is unique to that Acquirer, allocated to it for identification purposes by the International Organisation for Standardization.

"**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**" has the meaning given in the IAC Regulations.

"**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**" means a testing laboratory that has been accredited by the Company to conduct SCD security compliance testing.

"**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 this Code. Inserted effective 1.1.16

"**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 this Code pursuant to Part 2, clause 2.2 of the IAC Code Set Volume 6 (ATM System Code) and includes, for the avoidance of doubt, each: Inserted effective 1.1.16

(a) IA Participant;

(b) ATM Operator Member; and

(c) ATM Affiliate.

"**ATM Interchange**" 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. Inserted effective 1.1.16

"**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 this Code. Inserted effective 1.1.16

"**ATM System**" 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. Amended effective 1.1.16

"**ATM Transaction**" 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). Amended effective 1.1.16

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

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

"**Cardholder**" 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: Inserted effective 1.1.16

(a) Primary Account Number;

(b) Cardholder Name;

(c) Service Framework; and

(d) Expiration Date.

"**Card Payment**" means an electronic funds transfer or cash withdrawal initiated by a Cardholder using a Card in Australia, under the rules of an Approved Card Payment System or any other Card-based Transactions approved from time to time for the purposes of this definition by the IAF, and irrespective of the infrastructure or network used to process the transfer or withdrawal, and includes as the context requires, ATM Transactions, point of sale Transactions, a card-not-present payment and reversals or refunds of any such Transaction.

"**Card Payment System**" 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.

"**Cash**" means Australian legal tender.

"**Certification**" in relation to an IA Participant means initial certification or re-certification, in either case to the extent required by and in accordance with, Regulation 5.1(b) and Part 3 of the IAC Code Set Volume 1 (Introduction and Member Obligations).

"**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. Inserted effective 1.1.16

"**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. Inserted effective 1.1.16

"**Clearing System**" 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.

"**Commencement Date**" means, subject to IAC Regulation 1.6(b), 1 July 2015.

"**Committee of Management**" means the committee constituted under Part 7 of the Regulations.

"**Company**" means APCA.

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

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

"**Constitution**" means the constitution of the Company as amended from time to time.

"**Core Code**" has the meaning given in the IAC Regulations. Inserted effective 1.1.16

"**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] Deleted effective 3.7.17

"**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). Amended effective 3.7.17

"**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**" includes all credit payment instructions, usually electronically transmitted, which give rise to Interchange Activity, except as may be specifically excluded by the IAC Regulations or this IAC Code Set.

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

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

"**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). Inserted effective 1.1.16

"**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. Inserted effective 1.1.16

"**Direct Connection**" means a direct communications link between two IA Participants for the purposes of: Inserted effective 1.1.16

(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: Inserted effective 1.1.16

(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: Amended effective 1.1.16

(a) which the Cardholder denies having initiated; or Inserted effective 1.1.16

(b) where the ATM Transaction amount is claimed to be incorrect; or Inserted effective 1.1.16

(c) in respect of which the ATM Operator Fee is claimed to be incorrect. Inserted effective 1.1.16

"**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. Last amended effective 21.11.16

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

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

"**EFTPOS PED**" means a whole approved device which provides for the secure entry and encryption of PINs in processing and completing a Transaction.

"**EFTPOS Transactions**" means Transactions cleared pursuant to the rules prescribed for the EFTPOS Card Payment System by eftpos Payments Australia Limited as the administrator of that system.

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

"**EMV@ATM Terminal Standards**" means the standards and requirements set out in Annexure G.

"**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. Amended effective 3.7.17

"**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 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**" in relation to the approval of a Secure Cryptographic Device for:

(a) an Acquirer, means an entity approved by the Committee of Management in accordance with, and for purposes of, IAC Code Set Volume 4 (Device Requirements and Cryptographic Management); and

(b) an Issuer, means an entity approved by the Committee of Management in accordance with, and for purposes of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

"**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.

"**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**" means a Constitutional Corporation:

(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.

"**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**" means a Framework Participant which is either:

(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**" means the Issuers and Acquirers Community constituted by the IAC Regulations.

"**IAC Card Standards**" means the standards for Cards set out in the IAC Code Volume 2 (Issuer Code). Inserted effective 1.1.16

"**IAC Code Set**" has the meaning given in the IAC Regulations.

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

"**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 the IAC Code Volume 5 (Settlement Code). Inserted effective 1.1.16

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

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

"**Institutional Identifier Change Date**" means one of at least three dates in each calendar year specified by the Committee of Management 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**" 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**" 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:

(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 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**" means Credit Items or Debit Items.

"**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 delivers goods or services to a Cardholder at point of sale and which, in the normal course, is reimbursed by the Acquirer to which, from the Terminal that it operates, it electronically transmits that Transaction.

"**Message Authentication Code**" and "**MAC**" 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.

"**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.

"**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). Inserted effective 1.6.17

"**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**" has the meaning given in the IAC Regulations. Inserted effective 1.1.16

"**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.

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

"**PCI Evaluation Report**" means an evaluation report, prepared by an Approved Evaluation Facility, which evidences the compliance of a device submitted for approval under Part 3 of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) with the requirements set out in PCI PTS version 3.x. (PCI standards can be found at https://www.pcisecuritystandards.org).

"**PCI Plus Evaluation Report**" means an evaluation report, prepared by an Approved Evaluation Facility, which evidences the compliance of a device submitted for approval under Part 3 of Volume 4 with the PCI Plus Requirements, and if applicable, includes any delta report prepared in respect of the device.

"**PCI Plus Requirements**" means the requirements set out in Annexure B of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), being requirements for device approval in accordance with AS 2805.14.2 Annexes A, B and D, which are determined by the Company to be additional to the requirements of PCI PTS v 3.x. Amended effective 29.4.16

"**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", version 3.0, 2011.

"**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**" 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.

"**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

"**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.

"**Recognised APS**" has the meaning given in the Constitution.

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

"**Regulations** or the "**IAC Regulations**" means the regulations for IAC, as prescribed by the Company.

"**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.

"**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).

"**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).

"**SCM**" means a Security Control Module sometimes referred to as a host security module (HSM).

"**Secretary**" means a person appointed by the Chief Executive Officer to perform the duties of secretary of the IAF under Regulation 7.14.

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

"**Security Control Module**" and "**SCM**" means a physically and logically protected hardware device that provides a 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**" 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).

"**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 PED 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). Inserted effective 1.1.16

"**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 □ 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."*

"**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 containing a PED which can be used to complete a Transaction.

"**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**" 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**" means any Card Payment or other transaction initiated by a Cardholder 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 trussted 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 REQUIREMENTS FOR PIN-BASED TRANSACTIONS

(a) To ensure the security and integrity of the Australian payments environment, Acquirers must ensure that the following requirements are met at all times for PIN-based Card transactions completed within the IAC.

(b) The Acquirer is wholly responsible for ensuring that all Third Party Providers who are involved in processing PIN-based Card transactions within the IAC comply with the relevant provisions of this volume of the IAC Code.

2.1 Functional requirements

2.1.1 *Account Selection*

At a minimum, device account selection should provide for cheque, savings and credit accounts.

2.1.2 *Record of Transaction*

(a) A Record of Transaction generated by a Terminal must be laid out in a clear manner, with all printed items shown in an unambiguous fashion. It must comply, at a minimum, with the standards detailed in the ePayments Code published by the Australian Securities and Investments Commission (ASIC).

(b) In addition to these requirements, any Card number included on the Record of Transaction must have at least four (4) digits excluded. The preferred method of truncation is to print the first six (6) digits and the last (3) digits of the Card number on the Record of Transaction.

(c) Card expiry dates should be excluded from Cardholder's Record of Transaction.

(d) For ATM Transactions, the Acquirer must be clearly identified on the Record of Transaction.

*(**Note**: IAC Code Set Volume 6 (ATM System Code) contains additional requirements concerning a Record of Transaction for Transactions which involve an ATM Operator Fee).*

2.2 PIN Security

Acquirers must ensure that:

(a) only approved SCDs are employed in Interchange, including but not limited to ATM, PED, SCM and Key Loading and Transfer Devices;

(b) the management of the SCD meets the applicable device management standards (see Part 3);

(c) the key management practices employed comply with current AS 2805.6 series requirements;

(d) PIN management procedures and practices comply with current AS 2805.3.1 requirements; and

(e) where a Transaction contains PIN data (bit 52), that PIN data must be formatted in accordance with one of the PIN block formats specified in ISO 9564.1 with the exception of formats 1and 2; Amended effective 21.11.16

as further detailed below.

2.3 Secure Cryptographic Devices (SCDs)

(a) All devices involved in the production, distribution, selection, entering and transmission of plaintext Cardholder PINs, or associated cryptographic keys used to protect Cardholder PINs, in the Interchange environment must meet the requirements set out in Part 3 and must be approved for use, using the process described in the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

(b) Only approved devices may be attached to the Interchange networks.

(c) Any Issuer or Acquirer, which proposes to:

(i) implement any new SCD (not currently covered by an existing Letter of Approval); or

(ii) continue to employ a SCD which has reached or is about to reach its 'Letter of Approval' sunset date, unless the Company has renewed the device's Approval Period; or

(iii) implement any changes to an existing SCD's cryptographic devices, PIN or cryptographic key handling and management processing,

(iv) must apply for approval of the device as required by clause 2.3 as if each device is a new device for the purposes of that section.

2.4 Cryptographic standards

2.4.1 *General*

(a) Acquirers must ensure that all cryptographic operations associated with the processing of IAC transactions satisfy current IAC cryptographic standards (see IAC Code Set Volume 4 (Device Requirements and Cryptographic Management). These include requirements regarding:

(i) PIN encryption and Message Authentication across Interchange Links;

(ii) message encryption across Interchange Lines;

(iii) PIN encryption and Message Authentication from Terminals and across Acquirer links; and

(iv) Key management practices.

2.4.2 *Message Authentication (for Interchange Links)*

(a) Message Authentication must apply to all Interchange Links.

(b) 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.

(c) All interchange PIN and MAC cryptographic functions must be performed within a Tamper responsive SCM.

2.4.3 *Message Authentication (for Terminals)*

(a) Message Authentication must apply to all Terminal to Acquirer Links for all financial and key management messages.

(b) The 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.

2.4.4 *Privacy of Communication (for Interchange Lines)*

Interchange Lines shall 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.

2.4.5 *Privacy of Communication (for Terminals)*

(a) This clause applies to links between an EFTPOS Terminal and an Acquirer.

(b) For all Terminal to Acquirer links, Acquirers must ensure that privacy of communication complies with AS 2805.9 or any other privacy of communication standard approved by the Management Committee.

(c) 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. Inserted effective 1.1.15

(d) 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.

2.4.6 *Key Management Practices – Interchange Links*

Clause 2.4.6 is Confidential

2.4.7 *Key Rolling Process for Interchange Key Encrypting Keys (KEKs).*

The procedures to be adopted for the exchange of Interchange KEKs are detailed in the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

2.4.8 *Key Management Practices Interchange Lines*

In accordance with clause 2.4.4 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.

2.4.9 *Interchange Line Cryptographic Management*

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

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

(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;

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

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

(b) Where certificates are used consideration should be given to the use of the APCA signed, closed user-group certificate.

(c) 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.

2.4.10 *Key Management Practices for Interchange Lines*

Clause 2.4.10 is Confidential

2.5 Cardholder Data

All parties to the Interchange, including merchants, Acquirers, Third Party Providers and any intermediate network entities must maintain procedures and practices for preventing the unauthorised disclosure of Cardholder Data which, includes but is not necessarily limited to the:

(a) Primary Account Number;

(b) Cardholder Name;

(c) Service Code;

(d) Expiration Date.

(As an example, compliance with the Payment Card Industry (PCI) Data Security Standard would be sufficient to meet this requirement.)

2.6 Sensitive Authentication Data

Sensitive authentication data, including but not limited to:

(a) Full magnetic stripe (or equivalent);

(b) CVC2/CVV2/CID;

(c) PIN/PIN Block;

must not be stored, outside of an SCD, subsequent to Authorisation.

2.7 Unauthorised Access Prevention

All parties to the Interchange, including Acquirers, Issuers, Third Party Providers and any intermediate network entities must maintain procedures for avoiding any unauthorised access to or use of, the Interchange system through its own hardware, software, Interchange Lines and operational procedures which enable the exchange of authorisation and reconciliation of financial Transactions.

Next page is 3.1

PART 3 DEVICE SECURITY

3.1 Terminal security

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

(b) 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 SCD as defined in AS 2805.14.1 for on-line devices and be approved for use by the Company (see IAC Code Set Volume 4 (Device Requirements and Cryptographic Management). Amended effective 21.11.16

(c) SCDs must meet the requirements of AS 2805.14.2 (ISO 13491-2).

3.2 PIN Entry Devices

3.2.1 *Physical Characteristics and Key Management Protocols*

If PEDs employ key-management schemes not specifically permitted in AS 2805.6 series, Acquirers may seek approval for their deployment from the Company. Inserted effective 21.11.16

For the avoidance of doubt, a PIN entry device shall not reply on tamper evidence as its sole physical security characteristic (ISO 9564.1 clause 5.1). PEDs must also meet the following requirements: Amended effective 21.11.16

(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) they must meet, at a minimum, the requirements of a Physically Secure Device as defined in AS 2805.14.1; Amended effective 21.11.16

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

(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:

Inserted effective 21.11.16

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;

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.

3.2.2 *PIN Entry Devices*

(a) PIN entry devices must be managed in accordance with the requirements of AS 2805.14 series.

(b) The Sponsor will submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3 and B.3 of AS 2805.14.2 in respect of any PEDs employed in generating Interchange Transactions, Annexure B of IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.

3.2.3 *Privacy Shielding*

(a) Where a PED is approved subject to an optional privacy shield being installed, Acquirers must ensure that Merchants are advised of the importance of ensuring that the shield remains in place whilst the Terminal is operational.

(b) Where the device is designed and to be installed such that the device can be picked up and shielded from monitoring by the user's own body, or where the device, in itself, does not provide sufficient shielding and reliance is placed on the external physical environment, the Acquirer must ensure that the device is installed and managed in conformance with any vendor supplies rules and guidance as to how the visual observation is to be deterred.

3.2.4 *TCP/IP Terminal connectivity*

The following requirements apply to all Terminals where TCP/IP protocols are used for communications.

(a) Terminal identification is mandatory and may be implemented in part (at the financial message protocol level) by using a (Terminal resident) MAC address as a (Terminal) serial number or the PIN Pad Identification Definition (PPID).

(b) Mutual authentication is mandatory and may be implemented at the network / transport layer (e.g., SSL, IPSec, et al) or at financial message layer (e.g., AS2805.6.5 series).

(c) Transport level message encipherment must be applied to the entire datagram encapsulating the financial message unless the terminal is located on an Acquirer controlled private network. Amended effective 21.11.16

(d) End-to-end financial message encipherment must be provided using a method conformant to AS 2805.9.

(e) All operating systems must be hardened.

(f) The Terminal must contain a firewall if it is based on a ‘general purpose computer’.

(g) The Terminal must support a malware scanning application if it is based on a general purpose computer.

(h) No software on the Terminal will listen on any network service port, i.e., Terminal software may initiate "connect out" sessions only.

(i) The Terminal must support an active patch management process (to ensure that both the operating system and application environment is kept current and up to date to minimise exposure to any discovered flaws in those environments).

(j) The Terminal must comply with all applicable requirements of PCI-DSS

(k) The Terminal must, at a minimum, support 3DES encryption with full message encryption and authentication.

(l) Only unique key per Transaction or dynamic session keys are permitted for Terminal key management. Terminals with dynamic session key changes (application level) are required to change session keys every 256 Transactions or once per hour, whichever occurs first. Any remote support of merchant network and Terminals must be via a correctly configured and secured, remote access system, in accordance with all applicable requirements of PCI DSS security requirements.

(m) The Terminal application software must be secured against unauthorised changes or substitution.

3.2.5 *Terminals Running Multiple Applications*

Amended effective 1.7.15

The following requirements apply to all approved devices running multiple applications including non-payment applications.

(a) The terminal shall meet the requirements of clause 3.2.4(e) to 3.2.4(j).

(b) The terminal payment application software must be secured against unauthorised changes or substitution using cryptographic mechanisms.

(c) The terminal shall authenticate all applications using cryptographic mechanisms.

3.3 Security Control Modules

A Security Control Module (SCM) is a hardware device that provides an intentionally limited set of cryptographic services.

3.3.1 *Function set*

(a) The function set must be designed so 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., APCA 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.

3.3.2 *DEA-1*

From 1 January 2013 all symmetric encryption functionality weaker[1] than DEA-3 must have been disabled within every deployed SCM.

[1] See ISO TR14742 for an understanding of which algorithms are weaker than DEA-3

3.3.3 *Security Control Module Management (Host Security Modules)*

(a) SCMs must be managed in accordance with the requirements of AS 2805.14.2. The Sponsor must submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3, C.3, E.3 and either H.4 or H.5 in respect of any SCMs employed in the processing of Interchange Transactions. Annexure A of IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.

(b) SCMs should be configured in accordance with Section 0.3.5.2 of the APCA Specification for a Security Control Module Function Set such that all functions not required for the normal operation of the system are disabled. Additionally, where the SCM provides support for ISO format 1 PIN blocks, such functionality must be disabled in all Acquiring and switching systems.

3.3.4 *Remote Management of Security Control Modules*

The requirements of this clause apply to systems which support remote access for the management of SCMs.

(a) SCM Access Requirements:

(i) SCMs must be located in a secure, protected network, separate from generic internal or external access;

(ii) there must be no uncontrolled connections between general internal and external networks;

(iii) SCMs must be accessible only to authorised hosts and authorised applications;

(iv) for TCP/IP implementations:

(A) the SCM environment must be protected at a minimum by an IPS or IDS between the perimeter network firewall and the remote management device;

(B) stateful firewalls must protect all external entry points to the SCM environment; and

(C) such firewalls must log and monitor all inbound and outbound traffic to the SCMs;

(v) there must be a procedure, which is audited on a regular basis, for the rapid disablement of known/suspected compromised remote management devices.

(b) Management of SCM Remote Management Solutions:

(i) Remote Management Solutions may only be used with APCA approved SCMs.

(ii) All SCM Remote Management Solutions must be evaluated to the requirements specified in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and approved for use by the Company.

(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.

3.4 Key Loading and Transfer Devices

(a) Devices used in the initial cryptographic key loading of PEDs must be managed in accordance with the requirements of AS 2805.14.2.

(b) The Sponsor must submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3, E.3 and F.3 of AS 2805.14.2 in respect of any devices employed in the initial loading and transfer of PED cryptographic keys Annexure B of IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.

3.5 TCP/IP Host Requirements

The following requirements apply to host systems which support Terminals using the TCP/IP protocol for communications:

(a) stateful firewalls must protect all external entry points to the host environment;

(b) strong financial message protocol validation must be performed between Terminals and acquiring hosts;

(c) acquiring host must be located in a secure, protected network separate from generic internal or external access;

(d) production Security Control Modules must be accessible only to authorised production hosts and authorised production applications. Where connected via TCP/IP they must be on a separate, stand-alone network;

(e) there must be no uncontrolled connections between general internal and external networks and Terminal/SCM networks (assuming they are all TCP/IP);

(f) the host environment must provide, at a minimum, an IPS or IDS between the perimeter network firewall and acquiring host;

(g) the host system must support appropriate threat management techniques relevant to the host's operating platform, such as malware protection with up to date signatures and maintenance, vulnerability patching, etc.;

(h) all systems within the acquiring host environment must comply with all applicable requirements of PCI-DSS;

(i) the host must provide a mechanism for the rapid disablement of known/suspected compromised Terminals.

3.6 Key Injection Facility Assessment

3.6.1 *Request Assessment*

An Acquirer may request the Company conduct an assessment of a Key Injection Facility for the purposes of verifying compliance with certification requirements under IAC Code Set Volume 1 (Introduction and Member Obligations). This clause broadly outlines the process for assessment of a Key Injection Facility by the Company on an Acquirer's behalf. In this clause, "Applicant" means the Acquirer on whose behalf the Company agrees to conduct an assessment of a Key Injection Facility.

3.6.2 *Nomination for Assessment*

An Applicant should initiate the assessment process by submitting to the Company:

(a) a written request that the Company assess a nominated Key Injection Facility on its behalf;

(b) evidence of the consent of the Key Injection Facility to the conduct of the assessment by the Company in accordance with this clause 3.6.2, such consent to be evidenced by a Key Injection Facility Assessment Agreement executed by the Key Injection Facility; and

(c) all relevant additional information, including technical materials and evidentiary matters relevant to the Applicant's certification requirements with respect to key injection practice.

3.6.3 *Assessment Process*

(a) The Company will assess the performance of the Key Injection Facility in relation to the Company's standards and the Applicant's requirements. The Key Injection Facility must comply with the standards and requirements set out in Annexure B, together with such additional requirements as may be applicable to the Applicant's circumstances or requirements.

(b) The Key Injection Facility assessment process comprises such business reviews, technical reviews and on-site visits as may be necessary to enable the Company to properly assess the compliance of the Key Injection Facility with applicable requirements.

(c) Once a Key Injection Facility has been assessed by the Company as compliant with the applicable requirements, the Acquirer may rely on the assessment only for the purposes of certification under IAC Code Set Volume 1 (Introduction and Member Obligations). The Company may require, at its sole discretion, a Key Injection Facility to provide evidence of its continued compliance with assessment requirements triennially. The Company in its sole discretion may determine whether any other person, including any other Acquirer, may rely on the assessment for certification purposes.

Next page is A.1

ANNEXURE A KEY INJECTION FACILITY REQUIREMENTS

[Informative]

This Annexure will be used by the company in carrying out an assessment of a Key Injection Facility as set out in clause 3.6 of this Code. It provides the assumptions, scope references and definitions in support of the Key Injection Facility Requirements provided in Annexure B.

A.1 Assumptions

(a) As only APCA approved SCDs are used for key handling, i.e., HSMs, KLDs and PEDs, it is assumed that these devices will only perform in their accredited manner. Therefore, no requirements have been included here that would have been checked during the SCD approval process (i.e., key lengths, algorithms, randomness and uniqueness of keys). This also applies to the tamper responsiveness of the PEDs after key injection.

(b) KLDs have their own set of requirements which will not need to be rechecked by the facility. This includes how the device is handled once it has been securely dispatched from the facility, i.e., requirements on how keys are transferred from the KLD into a PED.

A.2 Scope

(a) The Key Injection Facility is considered to be the entire facility that is responsible for generation of the keys for injection into a PED through to loading of these keys into the PED.

(b) Annexure B, sets out the minimum requirements for protecting these keys; however it is understood that the environment in which the KIF operates may provide suitable mitigation in the event the requirements are not fully achieved.

(c) The scope of this part is limited to those requirements (both physical and operational) necessary for a KIF to meet. It covers:

(i) the generation of the initial cleartext keys or key components to be loaded into a PED or a KLD (used to transfer keys from the KIF to a PED);

(ii) the secure loading of cleartext keys or components into PEDs or KLDs within the KIF;

(iii) the secure management of any key generation device, PED or KLD during the time it is under the control of the KIF;

(iv) the loading of a keys, as part of the manufacturing process, which are subsequently used by the KIF;

(v) key management between KIF and manufacturer, if required;

(vi) key management between the KIF and acquirer, if required; and the secure receipt and dispatch of PEDs or KLDs to and from the KIF; and

(vii) CAs and RAs which operate under a PKI scheme and may be used as part of a remote key initialisation scheme.

(d) The types of keys subject to the requirements outlined in this part are application-level keys used by, or injected by, the KIF into a PED as part of injection and initialisation process associated with the device. Such key types include:

(i) Asymmetric initialisation master keys, such as manufacturer, sponsor, and TCU public & private keys;

(ii) Symmetric initialisation master keys, such as manufacturer, sponsor, and TCU master and derived keys;

(iii) the initial keys that the KIF is responsible for are any keys generated by the KIF, or received and managed by the KIF, which lead up to the establishment in the PED of the initial key common to the acquirer and PED.

(e) This part does not cover:

(i) the manufacturing process of PEDs, including any loading of firmware etc. by the manufacturer, except where the manufacturer generates and loads a key as part of the manufacturing process. In the latter case, the manufacturer's key injection facility must comply with these requirements;

(ii) any subsequent storage or dispatch of the device by the manufacturer to the KIF;

(iii) the manual loading of the initial keys into remote PEDs by a KLD;

(iv) network or transport-layer keys, such as those used to provide full stream encipherment of traffic independent from the devices payment application (e.g., SSL/TLS, IPSec, etc.,), nor does it address any application signing keys used to secure the payment application on the device.

(f) There are three phases for a device from manufacture through to installation for its intended use. The first is the manufacturing process itself. The first phase is not covered by these requirements. The second is the phase is post-manufacturing, from the time that the manufacturing process has been completed until the installation of the first key into the device. The third phase is pre-use, the period from the time the device is loaded with its initial key until it is installed for use. These requirements only cover the device from the post-manufacturing phase through to the pre-use phase when it is dispatched from the KIF plus any device returned from the field for reinjection.

(g) The intention of these requirements is to ensure that no PED goes into operation with compromised keys which could lead to a loss of customers' PINs. Although facilities whose processes and systems meet these requirements may not be able to prevent the compromise of keys used in the facility, any such compromise should be detected with a high degree of certainty before the compromised keys can be used. This can be achieved by utilizing appropriate factors of:

(i) device characteristics;

(ii) device management; and

(iii) environment.

A.3 Key Injection Facility Audit Guide

The Key Injection Facility Audit Guide, v3.0[1] should be used in conjunction with this document and provides additional information on how certain of the requirements are to be met.

A.4 References

(a) The following documents were used in the development of these requirements:

(i) AS 2805.6.1;

(ii) ANSI X9.24 2004;

(iii) ISO 11568-2;

(iv) ISO 13491-2 2005;

(v) CECS Manual – 2008;

[1] available on the APCA Extranet at https://extranet.apca.com.au/extranet/cs0corpdocs.nsf/NDX/KIF_AUDITGUIDE_CURRENT?OpenDocument&Login

(vi) Visa PCI-PIN Security Requirements (Annex B) – Jan 2008;

(vii) ANSI X9 TG-3 – 2006;

(viii) AS 2805.14.1;

(ix) Visa Cryptographic Key Injection Facility: Auditor's Guide v1.0, Jan 2008;

(x) ISO 11568-4;

(xi) ISO 11770-3;

(xii) MasterCard PCI-PIN Security Requirements – March 2008.

(b) Appendix A of the KIF Audit Guide provides a cross reference table indicating how the requirements in the reference documents are covered by the requirements in this document. The original documents can be used to clarify the intention behind the requirements however, where a discrepancy might exist, this part will take precedence.

A.5 Definitions

For the purposes of this part, the following definitions apply.

"**Approved Device**" means an approved SCD is one that has been evaluated in accordance with the requirements provided in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) of the IAC manual.

"**Asymmetric Key Pair**" means the two related keys, called the public key and the private key that are used with the DEA 2 asymmetric algorithm.

Note: DEA 2 is specified in AS 2805.5.3.

"**Certification Authority**" and "**CA**" means an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

"**Cipher Text**" means plain text that has been enciphered.

"**Cleartext Key**" has the same meaning as Plaintext Key.

"**Digital Certificate**" means a digital certificate is used to bind together a public key with an identity in the form of a public key certificate. It contains information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

"**Dual Control**" means the process of utilizing two or more entities (usually persons) operating in concert to protect sensitive functions or information whereby no single entity is able to access or use the materials.

"**Key Injection Device**" and "**KID**" means an approved SCD which is loaded with keys for injection into devices within the KIF, e.g., is used to inject acquirer supplied keys into a PED.

"**Key Injection Facility**" and "**KIF**" means a secure facility which contains an SCD for key generation and/or injection. The level of security will be determined by the security requirements of the SCD(s) used within the facility.

"**Key Pair**" has the same meaning as Asymmetric Key Pair.

"**Local Registration Authority**" and "**LRA**" means an optional part of a PKI that maintains users' identities from which CAs can issue digital certificates.

"**Plaintext Key**" means an unenciphered cryptographic key or key component, which is used in its current form.

"**Private Key**" means that key of an entity's asymmetric key pair, which can only be used by that entity. In the case of an asymmetric signature system, the private key defines the signature transformation.

Note: The term private key differentiates this key from the secret key of a symmetric algorithm.

"**Public Key**" means that key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system the public key defines the verification transformation.

"**Registration Authority**" has the same meaning as Local Registration Authority.

"**RSA**" means the name given to an algorithm for public-key cryptography.

"**Secret Key**" means a cryptographic key used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and must not be made public.

"**Split Knowledge**" means a condition under which two or more parties, separately and confidentially, have custody of components of a single key that, individually, convey no knowledge of the resultant key.

"**Symmetric Key**" means a secret key used with a symmetric cryptographic algorithm which uses the same key for encipherment and decipherment.

"**Tamper Evidence**" means a process that makes unauthorised modification to the device easily detected.

"**Tamper Responsiveness**" means a process that detects the intrusion attempt and destroys the sensitive contents of the device.

Next page is B.1

ANNEXURE B KEY INJECTION REQUIREMENTS

[Informative]

This Annexure, to be used in conjunction with Annexure A, contains the Key Injection Facility Requirements to be used by the Company in carrying out an assessment of a Key Injection Facility as set out in clause 3.6 of this Code.

B.1 Key Injection Facility (KIF)

This facility is a secure environment which encloses the key injection process, housing the key generation/injection device plus any PEDs and KLDs whilst they are being loaded and prior to securing for dispatch. The level of security afforded by this facility will depend on the minimum security requirements of the devices housed and used within that facility.

KIF Requirements		Ref[1]
B.1.1	Key Injection Facilities shall inject keys only into approved SCDs. This includes, but is not limited to, PEDs and KLDs. The SCDs shall be approved by APCA for their intended purpose.	5
B.1.2	Key Injection Facilities that include hardware devices/systems for managing keys (e.g., generation and storing) shall ensure those hardware devices/systems are approved by APCA or PCI as per these requirements or comply with the requirements of clause B.2.18. This includes HSMs and any associated system, such as a PC, to which the HSM is attached and that the cleartext keys or components pass through.	5
B.1.3	A KIF, including all processes related to key management (e.g., key generation and injection), shall be implemented securely within an environment which meets the definitions of a Controlled or a Secure environment in Annex H of Reference 4 (see KIF Audit Guide), and shall be operated under dual control.	3
B.1.4	The environment shall remain secure until all keys or other secret data and useful residue from such secret data and have been removed from the environment or destroyed.	2

[1] This reference number refers to numbers in the "Key Injection Requirements Cross Reference Table" document in the KIF Audit Guide (refer to clause A.3).

KIF Requirements	Ref[1]
B.1.5 Any hardware used in the key injection process shall be monitored and a log of all key-loading activities maintained for audit purposes. This log must be protected from unauthorised modification.	34
B.1.6 Auditable records shall be maintained on all SCDs processed by the facility, from the time of receipt through to dispatch to ensure detection of lost or stolen equipment. The record (which must be protected from unauthorised modification) should contain but is not limited to the following information: (a) sender; (b) receipt note number; (c) manufacturer; (d) serial number of the device; (e) operations carried out on device. (f) recipient; (g) confirmation of receipt; and (h) dispatch note number.	
B.1.7 All SCDs received by the facility shall be accounted for and any discrepancy between the quantity and serial numbers of the devices sent and of those received shall be notified to the sender and owner and investigated.	
B.1.8 All SCDs dispatched from the facility shall be accompanied by an itemized record of the devices dispatched. The recipient shall notify the KIF of any discrepancy between the record of items sent by the facility and the SCDs actually received.	
B.1.9 The KIF operator shall ensure that any new staff involved within the KIF or who have access to keys or key components, are subject to appropriate probity checking (e.g., identity verification, reference check, criminal record check) such as those required for Australian Financial Services License holders for employment of Responsible Officers (RO) as outlined in ASIC policy statement (PS 146) or equivalent.	
B.1.10 Documented procedures exist and are demonstrably in use for all processes related to the operation of the KIF, including key injection, and all involved staff shall be trained and competent in the use of these procedures.	33,82 & 88

KIF Requirements		Ref[1]
B.1.11	No wireless network connectivity is allowed to or from the KIF.	
B.1.12	Where the KIF participates in remote key establishment and distribution applications the following additional requirements of References 6 and 12, where they relate specifically to remote key establishment and distribution applications: (a) Question 19 - Single Purpose Keys; (b) Question 22 - Key Compromise Procedures; (c) Question 25 - Limit Key Access; (d) Question 28 - Key Administration Procedures; and (e) Question 31 - SCD Procedures; shall be used.	

B.2 Key Generation (KGD) / Key Injection Devices (KID)

(a) These devices are used to generate and inject keys into a PED or KLD. They may generate those keys or inject preloaded keys from an acquirer. To enable the loading into the device “preloaded keys” and/or sending generated keys, they will need the functionality to enable the loading of keys such as transport keys or other acquirer related keys. The handling of the acquirer related keys will be managed in accordance with the General Key Management requirements stated in clause B.5 below.

(b) The key generation device may be a purpose built SCD or it may be a device which contains an SCD for the key generation and storage. Accordingly, it should not be assumed that in the following requirements the term device means only an SCD unless expressly described as such. All attached cables to the device (other than the power cable) must be treated as an integral part of the device.

(c) A KID is either loaded with keys for injection into a PED or it may contain a KGD to generate the keys for injection. The KID will use an SCD to manage the storage and generation of keys. These devices (KIDs) are not used to transport keys to PEDs outside the KIF.

(d) A KID is loaded with keys for injection into a PED, e.g., the keys are generated by a acquirer and loaded into the KID. The KID will use an SCD to manage the storage and injection of keys. These devices (KIDs) are not used to transport keys to PEDs outside the KIF.

(e) There are two types of device that can be used to generate and inject keys. One type of device requires tamper responsiveness and tamper evidence because a compromise of the device could disclose keys previously generated or injected by the device prior to the compromise. The other type of device requires only tamper evidence because the device retains no information that, if disclosed, could disclose any key that had been injected into a cryptographic device prior to the compromise.

KIF Requirements	**Ref**
B.2.1 The generation, and/or storage of plain text keys shall be carried out within an APCA approved SCD, e.g., HSM. The approval process shall include evaluation/approval of any functions specifically required for this function. Where the KGD comprises a personal computer and an SCD: (a) the SCD is to be integral to the device or directly connected (e.g., serially); (b) all openings on the device that are not used for key injection are securely sealed in a tamper-evident and auditable manner. Examples include USB ports, unused serial connections, PCMCIA slots, etc.	5, 11
B.2.2 Where the device (KID) handles clear text secret or private keys, at a minimum, the following controls shall be enforced for the device to be classified as an approved KID classified as an approved KID: (a) All key generation and/or storage is handled in accordance with Requirement B.2.1 by using an SCD which is an Approved Device (KGD); (b) That device (KID) shall meet the requirements of Annex F of Reference 4 (see KIF Audit Guide) and be approved for this use by APCA.	
B.2.3 Where an approved KGDs and KIDs are used then: (a) Where there is a network connection then: (i) Any connection made from or to those devices is mutually authenticated; (ii) that device shall not send or receive cleartext keys or components via the network connection; (iii) the devices must be on a dedicated network segment which is isolated from other network devices; (iv) all communications into and out of those devices is enciphered; (v) the network connection between the two devices is required to be firewalled at both network endpoints and is required to provide an additional security layer over	

KIF Requirements	Ref
any application later cryptographic protection (e.g., IPsec); (vi) only ports required for the KIF functionality are open; and (vii) the network connection shall not be able to be used to compromise or manipulate any process carried out by those devices; (b) The device used for the key injection function, plus any cables, keypads or other attachments, are maintained under dual control at all times; (c) That device maintains an auditable log of all operations which includes as a minimum, the following information: (i) The time and date of any operation, including power on and off; (ii) Details of the operation being performed; (iii) The PPID and serial numbers of any device injected with keys; (iv) User sign-on at system and operator levels; (d) The logs shall be cryptographically authenticated such that an altered or missing log activity can be detected; (e) Hardware use is monitored and logs of key loading activity are maintained; (f) That device is started from a powered off position for each key loading activity; (g) The personnel responsible for the systems administration of the device shall not have authorized access into the room – they shall be escorted by authorized key injection personnel, and they shall not have user IDs or passwords to operate the key injection application; (h) The key injection personnel shall not have system's administration capability on the device; (i) The device shall not be able to boot from external media (such as floppies or CDs). It shall boot from the hard drive only where applicable; (j) Manufacturer's default passwords shall be changed.	

KIF Requirements	Ref
B.2.4 Where an approved Key Injection device (KID) is not used, the following minimum controls shall be enforced: (a) The device shall be standalone; (b) The KID shall comply with clause B.2.1 (c) The device, or any of its components, shall not be removed from the KIF before destroying al memory components; (d) Shall adhere to clause B.2.3(b) to B.2.3(j), above where applicable. Please note, APCA intends to enforce the use of approved KIDs at some future date to be determined by the IAC committee of management.	
B.2.5 No person with existing or prior access to any mechanism used to enforce dual control on the KGD/KID (e.g., password or physical key) has existing, prior, or future access to any other mechanism used to enforce dual control on that device.	
B.2.6 Plaintext keys shall never be written to any form of non-volatile storage outside of the tamper responsive envelope of an approved SCD, e.g., PED.	
B.2.7 Keys shall not be installed in any KGD/KID until it has been inspected by qualified staff, i.e., staff who have been specifically trained for this role, and a reasonable degree of assurance has been reached that the KGD/KID is an authentic device and has not been subject to any unauthorised physical or logical modifications or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using appropriate guidelines from the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment. (e.g., bonded carrier, device authentication code injected by terminal vendor and verified on receipt, tamper evident packaging, etc.). (c) The device is delivered with secret information to allow the KIF to ascertain that the device is genuine and not compromised providing the secret information has not been erased.	37

KIF Requirements		Ref
B.2.8	The key generation device will not output any plaintext key except under dual control. Such dual control shall be enforced by the KGD/KID or the PED requiring that at least two passwords be correctly entered within a period of no more than five minutes, before the device will output/accept a key. The device shall ensure that passwords are at least 5 characters long and the characters shall be a mixture of alphanumeric where available.	12
B.2.9	Where an asymmetric key pair is generated for transfer into another device by a KGD/KID that will not use the key pair, then the private key of the key pair and all related secret seed elements shall be 'zeroised' or otherwise permanently deleted immediately after the transfer to the target device has been ensured.	14
B.2.10	The transfer mechanisms by which plaintext keys, key components or passwords are transferred into or out of the KGD/KID are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any keys, key components or passwords. This shall take into account all aspects of monitoring, including the use of surveillance cameras. This will require all cables and attachments to be managed under dual control.	30
B.2.11	All plain text keys that have been injected into a device are to be maintained in one of the acceptable key forms as stated in this document. These keys shall not be retained by the KIF after the keys have been injected and are in the possession of the sponsor of the device.	28
B.2.12	Controls are in place to ensure that no information remains within any KGD/KID that is to be removed from the KIF which could disclose any cryptographic key that ever existed within that device.	29
B.2.13	Controls are in place to detect the unauthorized reinstallation of a KGD/KID previously removed from a facility.	31
B.2.14	Controls are in place to detect the unauthorized removal of the KGD/KID from, and its unauthorized replacement back into, its authorized location.	32

KIF Requirements	Ref
B.2.15 All keys that have been used, or potentially could be used, in a KGD/KID that has been removed from service shall be destroyed. If this cannot be accomplished then the device shall be physically destroyed so that no keys can be disclosed nor the device placed back in service again. This requirement does not include keys that have been already deployed in the field.	86
B.2.16 Controls are in place to detect the unauthorized removal of the KGD/KID from, and its unauthorized replacement back into, its authorized location. This could take the form of: (a) mechanisms such that the removal of that device from its operational location will cause the automatic erasure of the cryptographic keys contained within that device; (b) the KGD/KID is stored, under dual control, in a safe or room that cannot feasibly be penetrated, and each incident of opening or closing the safe or room is recorded under dual control.	16
B.2.17 Unauthorized use of the KGD/KID, when in active use, is prevented or detected by means such as the following: (a) the KGD/KID has functional or physical characteristics (e.g., passwords or physical high-security keys) that prevent use of that device except under dual control, and when in that useable state, that device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any attempted unauthorized access, and able also to prevent such access before it is successful; (b) the KGD/KID is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorized people who ensure that any unauthorized use of that device would be detected.	17 & 19
B.2.18 When the KGD/KID is not in active use, any unauthorized access to that device is prevented by means such as the following: (a) the facility (e.g., room) where the KGD/KID operates has sufficient supervision and controls to prevent any unauthorized access to that device that would allow alteration to that device or disclosure of any key or other sensitive data without detection; (b) the KGD/KID is stored, under dual control, in a safe that cannot feasibly be penetrated without detection, and each incident of opening or closing the safe is recorded under dual control.	18 & 20

KIF Requirements	Ref
B.2.19 Any physical keys used to secure, unlock or operate a KGD/KID are carefully controlled, and available only to authorized persons.	22
B.2.20 The KID is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no "bug" or other disclosing mechanism on the path that the key traverses from the KID to the target device.	50

B.3 Procedures for Handling Target Devices

The target devices referred to in this Part are PEDs. Requirements for Key Loading Devices (KLDs) which do not have key generation or PIN handling functionality are covered in clause B.4. It is important to ensure that no unauthorised access to the device remains undetected from the time of manufacture through to it being put into use.

Prior to an initial key being loaded, the target devices require only tamper evidence because the device retains no information that, if revealed, could disclose any key that had been injected into the device prior to the compromise. PEDs that have a public key (or key pair) installed as part of the manufacturing process shall be in a tamper responsive state once the public key (pair) has been installed. These keys may be for authenticating subsequent application loads and/or key loads.

KIF Requirements	Ref
B.3.1 Keys shall not be installed in any SCD until it has been visually inspected by staff, who are trained to detect a non-authentic or tampered device, and a reasonable degree of assurance has been reached that the SCD is an authentic device and has not been subject to any unauthorised physical or logical modifications, or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using appropriate guidelines provided by the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment (e.g., bonded carrier, device authentication code injected by terminal vendor and verified on receipt, tamper evident packaging, etc.); (c) The device is delivered with secret information to allow the KIF to ascertain that the device is genuine and not compromised providing the secret information has not been erased.	37

KIF Requirements		Ref
B.3.2	Any device, once it has been injected with keys, is controlled so as to prevent or detect unauthorized access to it, with records kept and audited so as to detect and report unauthorised substitution, theft or loss.	39
B.3.3	Controls are in place to ensure the destruction of any existing keys in a device returned to the KIF prior to the injection of new keys into that device.	
B.3.4	The distribution and loading of keys into a PED shall be performed under dual control using one of the following techniques: (a) manual, e.g., key component entry via a key pad when device is in a sensitive state; or (b) electronic direct loading, e.g., direct key injection via a cable from the originating device.	41 & 43
B.3.5	The action of loading a key puts the device in a mode that activates all tamper protection mechanisms within the device unless it is in that mode.	42
B.3.6	KIFs shall ensure that unique symmetric and/or private keys are loaded into each device. The same key(s) shall not be loaded into multiple devices. Public keys (certificates) may be common to a group of devices.	8
B.3.7	Where keys are derived for injection into various types of devices, the same key should not be derived for multiple devices, except by chance.	8
B.3.8	Controls are in place to detect the unauthorized replacement of a PED previously removed from a facility.	31
B.3.9	Upon inspection of a device, where there is any evidence of tampering or doubt about tampering, the acquirer shall be notified immediately.	

B.4 Key Loading (KLD) / Key Transport Devices (KTD)

A KLD is an SCD used to load plain text keys into an SCD outside of the KIF, i.e., load keys into a PED in the field. A KTD is an SCD used to transfer keys between an SCD in the KIF and an external SCD. The keys may be moved in either direction.

KIF Requirements	Ref
B.4.1 Keys shall not be installed in any KLD/KTD until it has been inspected by qualified staff and a reasonable degree of assurance has been reached that the SCD is an authentic device and has not been subject to any unauthorised physical or logical modifications or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using approved guidelines from the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment. (e.g., bonded carrier, device authentication code injected by terminal vendor and verified on receipt, tamper evident packaging, etc.).	2
B.4.2 A KLD/KTD shall be an approved SCD designed for the purpose of transporting keys outside the KIF.	47
B.4.3 The KLD/KTD shall not retain a key or, information that may disclose that key, that it has successfully transferred.	47
B.4.4 The KLD will not output any key except when under dual control. Such dual control is enforced by means such as the following: (a) the device requires that at least two passwords be correctly entered within a period of no more than five minutes, before the device will output a key; (b) the device requires that at least two different, non-reproducible physical keys be concurrently inserted into the unit before it will output a key.	49
B.4.5 Controls are in place to ensure the destruction of any old keys from a KLD/KTD returned to the KIF prior to the injection of new keys.	
B.4.6 No person with existing or prior access to any mechanism used to enforce dual control on the KLD/KTD (e.g., password or physical key) has existing, prior, or future access to any other mechanism used to enforce dual control on that device.	23 & 51

KIF Requirements	Ref
B.4.7 If the KLD/KTD only requires tamper evidence then, when the device is not in active use, undetected access to its internal circuitry is prevented by means such as the following: (a) the facility where the KLD/KTD operates has sufficient supervision and controls to detect any such unauthorized access to the KLD/KTD before the device is subsequently put into active use; (b) the KLD/KTD is stored under dual control, in a tamper-evident cabinet for which each incident of opening and closing is controlled and recorded, under dual control; (c) the tamper-evident cabinet, if used, is regularly monitored by at least two trusted people who are qualified to detect and able to observe any unauthorised access.	52
B.4.8 If the KLD/KTD only requires tamper evidence then, when the KLD is in or ready for active use, undetected access to its internal circuitry is prevented by means such as the following: (a) the facility where the KLD/KTD operates has sufficient supervision and controls to detect any such unauthorized access to the KLD/KTD before the KLD/KTD is subsequently used for any cryptographic function; (b) the KLD/KTD is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any such access.	53
B.4.9 The KLD/KTD is loaded with a plaintext key only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism in the path that the key traverses from the key generation device to the KLD/KTD.	58
B.4.10 The KLD is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism on the path that the key traverses from the KLD to the target device.	50
B.4.11 Use of any KLD/KTD shall be monitored and a log of all key-loading activities maintained for audit purposes.	59

B.5 General Key Management

KIF Requirements		Ref
B.5.1	Keys shall exist only in those forms permitted by these requirements.	6
B.5.2	Documented procedures exist and are followed to ensure secret or private keys shall be generated using a process such that it is not possible to predict any secret value or to determine that certain values are more probable than others from the total set of all the possible values.	10
B.5.3	A person with access to one component of a key, or to the media conveying this component, shall not have access to any other component of this key or to any other medium conveying any other component of this key.	9 & 63
B.5.4	Functionality needed to import, export, or transfer cryptographic keys from external sources ensures that the keys are in one or more of the following forms: (a) enciphered under the proper variant of a symmetric key encipherment key; (b) enciphered under the asymmetric public key of the recipient; (c) enciphered with an import key being specifically enabled for a limited time and limited number of function calls; (d) as key components managed under dual control, such that two operators are required to perform any key operation; (e) input under dual or multiple control through the secure operator interface, in components such that full knowledge of all but one component gives no usable information on any bit of the cryptographic key; (f) public keys are entered under dual control or enciphered under the a KLD or a target device as per these requirements; (g) Output as clear text keys under dual or multiple control for injection into a KLD or a target device as per these requirements; (h) Output as clear text keys under dual or multiple control for injection into a KLD or a target device as per these requirements.	15 & 62
B.5.5	The transfer of a key to another SCD: (a) uses a secure communications path; or (b) uses a key transfer device; or (c) uses a secure cryptographic path; or (d) is carried out in a secure environment.	4

KIF Requirements		Ref
B.5.6	Storage of the private key requires that secrecy and integrity are ensured. Storage of the public key requires that authenticity and integrity are ensured.	77
B.5.7	Plaintext private and secret key(s) whose compromise would affect only one party shall exist only within a SCD or a physically secure environment operated by, or on behalf of, that party under dual control and split knowledge.	60
B.5.8	Plaintext private and secret key(s) whose compromise would affect multiple parties shall exist only within a SCD.	61
B.5.9	Transport of public keys shall be conveyed in a manner that protects their integrity and authenticity and provides the ability to validate that the correct key was received. The mechanism used to validate that the correct public key was received shall be independent of the actual conveyance method.	62
B.5.10	Key confirmation is often provided by subsequent use of an established key, and if something is wrong with its use then it is immediately detected. This is called implicit key confirmation. Explicit key confirmation in this case may be unnecessary.	80

KIF Requirements	Ref
B.5.11 One or more of the following techniques shall be used to ensure public key integrity: (a) sign the public key and associated data using a digital signature system, thereby creating a public key certificate. Key certificates, and the management of the keys used to create and verify the certificates, are described in Reference 10, Clauses 5.3 and 6 (see KIF Audit Guide); (b) create a MAC for the public key and associated data, using an algorithm defined by ISO 16609 and a key used only for this purpose; (c) store the public key in an SCD; (d) distribute the public key over an unprotected channel, and distribute a key verification code of the public key and associated data over an integrity assured channel such as an authenticated channel with dual controls (key verification is described in Reference 10, Clause 5.5 - see KIF Audit Guide); (e) using authenticated encryption; (f) when entering the public key into an SCD it shall be managed under dual control.	78
B.5.12 The devices (SCDs) involved in using public key schemes shall check the validity of other such devices involved in the communication prior to any key transport, exchange or establishment. Validation of authentication credentials shall occur immediately prior to any key establishment.	87
B.5.13 Any single clear text key component is, at all times during its transmission, conveyance, or movement between any two organizational entities: (a) under the continuous supervision of a person with authorized access to this component; or (b) locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it; or (c) in a physically secure SCD.	64

KIF Requirements	Ref
B.5.14 When plaintext public keys are stored and are not in the form of a certificate or when their certificate has been checked and they will be used without re-checking the certificate, integrity and authenticity shall be ensured. Protection against substitution of the public key during storage is essential. For example, the substitution of a public key used for encipherment may result in a threat to data secrecy. One means of protecting a public key against substitution is to implement the same techniques as for a private key. Another means is to store the public key in a certificate, allowing verification of the key's integrity and authenticity before use. The unauthorized substitution of stored public keys shall be prevented by one or more of the following means: (a) physically and procedurally preventing unauthorized access to the key storage area; (b) storing a key enciphered as a function of its intended use and ensuring that it is not possible to know both a plain text value and its corresponding cipher text, enciphered under the key encipherment key; (c) storing a certificate containing a public key and verifying the certificate prior to its use; the authenticity and integrity of the public key used to verify the certificate shall be ensured. If unauthorized key substitution is known or suspected, procedures are in place and followed to ensure that the public key is replaced with the correct public key.	79
B.5.15 The components of encryption keys shall be transferred using different communication channels per component, such as different courier services to ensure split knowledge.	65
B.5.16 Mechanisms shall exist to ensure that only authorized custodians have access to plaintext key components and place key components into tamper-evident packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components upon receipt.	66
B.5.17 Unencrypted keys are entered into host HSMs and PEDs using the principles of dual control and split knowledge.	68

KIF Requirements		Ref
B.5.18	The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring (e.g., visual or logical) that could result in the unauthorized disclosure of any component.	69
B.5.19	Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	73
B.5.20	The following requirements are the minimum standards to be applied to Key Encrypting Keys: (a) All Key Encrypting Keys used to transmit or convey or otherwise secure other cryptographic keys are (at least) as strong as any key they are securing; (b) A double-length TDES key shall be enciphered by a double or triple-length TDES key, an RSA key with a key modulus of at least 1024 bits, or an AES key of at least 128 bits. RSA keys encrypting keys greater in strength than double length TDEA keys shall use a modulus of at least 2048 bits. An RSA key with a modulus of at least 1536 bits should be used to encipher double length TDES keys where ever possible; (c) A triple-length TDES key shall be enciphered by a triple-length TDES key, a 128 bit AES key, or an RSA key with a modulus of at least 2048 bits.	67
B.5.21	The use of RSA keys with a modulus of only 1024 bits shall be treated as single use keys; TDES key transport keys shall be treated as single use keys and destroyed after use.	67
B.5.22	Procedures exist to prevent or detect the unauthorized substitution (key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	72
B.5.23	Any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) shall be replaced with a value not feasibly related to the original key.	75

KIF Requirements		Ref
B.5.24	Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage.	76
B.5.25	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	81
B.5.26	Access to secret and private cryptographic keys and key material shall be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	82
B.5.27	Each person acting as a key custodian shall be designated as such and this designation documented on a Key Custodian Form which designates each custodian's responsibilities and duties. Each custodian shall sign the Key Custodian Form as having read and understood these responsibilities and duties in relation to the key material entrusted to them.	82
B.5.28	Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a SCD.	83
B.5.29	Backups of secret and private keys shall exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups shall exist only in one of the allowed storage forms for that key.	84
B.5.30	Documented procedures exist and are demonstrably in use for all key management operations.	85

Next page is C.1

ANNEXUREC. DEBIT CARD FRAUD PREVENTION - GUIDELINES

[Informative]
Annexure C is confidential

Next page is D.1

ANNEXURE D. COMPROMISED DEVICE MANAGEMENT FRAMEWORK

[Informative]
Annexure D is confidential

Next page is E.1

ANNEXURE E. SECURITY CHECKLISTS FOR INSTALLATION OF EFTPOS DEVICES

Annexure E is confidential
[Informative]

Next page is F.1

ANNEXURE F ISSUER AND ACQUIRER BEST PRACTICE GUIDELINES FOR CARD NOT PRESENT TRANSACTIONS

Inserted effective 3.7.17

[Informative]

F.1 INTRODUCTION

The increasing importance of online commerce, which provides convenience and efficiency benefits to both merchants and consumers, means that the volume of digital transactions continues to increase. Online transactions are primarily carried out by either a cardholder entering their payment card number into the merchant website, the merchant keeping the cardholder's details on file from a previous transaction or in-app. Such card-not-present (CNP) transactions provide increased scope for fraud, as there is greater potential for the transaction to be facilitated by someone other than the cardholder. As a result, the significant increase in e-commerce and online transactions has corresponded with a substantial increase in payments fraud.

Different jurisdictions worldwide have attempted to solve this problem in markedly different ways. Mandating a single solution appears to be sub-optimal since a single solution would not necessarily cover all of the facets of fraud mitigation: fraud detection; cardholder authentication and the security of cardholder data.

In contrast, industry best-practice guidelines can address a range of potential solutions and implementation issues. They can also enable non-technical aspects, such as merchant choice, and the education of cardholders and merchants on preventions to be covered. Another advantage of industry guidelines is that they can be reviewed regularly – by APCA – to ensure they remain relevant and fit-for-purpose. This is especially important given predicted changes in the eCommerce space.

F.2 ONLINE PAYMENTS IN AUSTRALIA

F.2.1 Australia's Payments Mix

The Australian payments market is characterised by a clear long term trend away from cash to electronic payment methods, such as direct entry and debit, credit and charge cards. The digital economy continues to drive a decline in traditional payment methods such as cheques and cash, with both consumers and businesses continuing to reduce their use of such methods[1]. Current data regarding the use of different payment channels in Australia is available on the APCA website[2].

[1] APCA Milestones Report – The Digital Economy November 2016.
[2] APCA – Payment today – http://www.apca.com.au/about-payments

F.2.2 eCommerce in Australia

These trends have been driven in part by the increasing importance of online commerce, which provides convenience and efficiency benefits to both merchants and consumers. The remote and 'always on' nature of online commerce is attractive to merchants and consumers alike.

For merchants, it enables:

(a) a massive geographic reach without having to invest in multiple physical points of presence (both lowering costs and increasing the size of the available market);

(b) sales to occur 24 x 7; and

(c) small merchants to compete like large merchants.

For consumers, it enables:

(a) the ability to comparison shop across a vast array of offers, both domestic and overseas;

(b) purchases to occur 24 x 7; and

(c) the convenience of shopping from the home/the office/anywhere.

Hence, the ever increasing importance of the internet has meant a burgeoning online economy with online payments growing alongside it. The Reserve Bank of Australia (RBA) estimated that online payments more than doubled between 2007 and 2014[3].

F.3 CARD NOT PRESENT FRAUD

Online transactions inherently involve the card not being physically available for the merchant to inspect at the time of the transaction. Such CNP transactions include online transactions and mail order or telephone transactions, but with the vast majority being online transactions. Online transactions are primarily carried out by either a cardholder entering their payment card number into the merchant website, the merchant keeping the cardholder's details on file from a previous transaction or in-app.

CNP transactions provide increased scope for fraud, as there is greater potential for the transaction to be facilitated by someone other than the cardholder. As a result, the significant increase in e-commerce and online transactions has corresponded with a substantial increase in payments fraud.

[3] The Changing Way We Pay: Trends in Consumer Payments – June 2014.

Payments fraud in the context of a CNP transaction (CNP fraud) can arise in a number of contexts including through cardholder information being:

(a) obtained illegally through card theft, malware on the cardholder's device or merchant database hacking;

(b) intercepted through communications systems; or

(c) obtained by cardholder deception such as through 'phishing' scams, in which fake communications (i.e. emails) that purport to come from a genuine source are used to encourage cardholders to provide information.

Fraud statistics published by APCA[4] indicate that in 2015:

(a) total CNP fraud affecting Australian Merchants and Cardholders reached $398m; and

(b) CNP fraud made up 83 per cent of all payments card fraud in Australia by value.

A factor contributing to the growth in CNP fraud has been successful security initiatives in relation to card present transactions, including the introduction of chip cards (which are currently the most effective technology for preventing counterfeit fraud) and mandatory use of PIN authentication (which reduced lost and stolen card fraud). These increased security measures have made CNP fraud relatively easier for criminals to engage in than at physical point of sale.

Online payments fraud is an issue of concern both across the payments industry as well as for consumers. Consumers are impacted by online payments transaction fraud in four important ways:

(a) consumers meet the cost of fraud through increases in the price of goods purchased online and the cost of payments services;

(b) consumers are inconvenienced by fraud through meeting the cost of fraudulent transactions that they do not identify, the need to request the reversal of fraudulent transactions, obtain new cards, re-establish direct debits on the new card account;

(c) consumers experience undermined confidence in the online payments system and the loss of efficiencies through utilising online payments; and

(d) consumers face significant risks associated with fraud through the disclosure of personal information and potentially identity theft.

[4] The Australian Payments Fraud Report 2016.

Research commissioned by APCA and conducted by IDCARE in 2016 has shown that the impact of such fraud on consumers can be significant:

(a) Cardholders spend on average 1.3 hours consulting with financial institutions and redirecting payment arrangements in response to a compromise; and

(b) 42% of consumers immediately ceased transacting online usually within 72 hours of the event. 79% of these typically re-engaged within a week and the remaining 21% often within a month.

F.4 SOLUTIONS TO CARD NOT PRESENT FRAUD

Different jurisdictions worldwide have attempted to solve this problem in markedly different ways. Research conducted by APCA has shown that:

(a) The scope of various approaches across different geographies is greater than just authentication and now also covers detection and data security;

(b) Co-ordination of authentication analytics (across digital identity, geo-location, device proximity, biometrics and social media analytics) also needs to be considered; and

(c) Collaboration and respect of merchant choice is key.

In addition, the nature of eCommerce and the associated CNP fraud is likely to change markedly over coming years. Separate research commissioned by APCA and conducted by IDCARE in 2016 suggests that the payment landscape is changing:

(a) Card payments will continue to rise and become the majority of total payment mix in 2020;

(b) mCommerce is expected to account for more than 60% of online payments;

(c) Of this percentage, a significant majority (over 75%) is predicted to be funded via stored card information;

(d) Entry of card information into a browser will reduce to represent 20% or less of transactions by 2020; and

(e) As mobile device usage increases, authentication will shift towards more user friendly biometrics.

APCA is therefore of the view that mandating a single solution would be sub-optimal since there are many possible solutions to cover all of the facets of fraud mitigation: fraud detection; cardholder authentication and the security of cardholder data.

In contrast, industry best-practice guidelines can address a range of potential solutions and implementation issues.

In addition, guidelines cover non-technical aspects, such as merchant choice, and the education of cardholders and merchants on prevention.

Another advantage of guidelines is the ability for them to be reviewed regularly by APCA to ensure they remain relevant especially given predicted changes in the eCommerce space. Indeed, the guidelines need to enable the growing use of solutions such as tokenisation, online and in-app wallet services, and authentication techniques such as digital identity, geo-location, device proximity, biometrics and social media analytics.

F.5 PROPOSED SOLUTION - GUIDELINES

F.5.1 Guidelines Introduction and scope

(a) These Guidelines set out a range of best practices for Australian Card Issuers and Acquirers in relation to acceptance and processing of CNP transactions. They focus on the following main areas:

(i) Secure collection, storage and transmission of Card data;

(ii) Cardholder authentication;

(iii) Fraud detection;

(iv) Tokenisation;

(v) Cardholder and Merchant education on prevention.

(b) These Guidelines are intended to complement or improve existing systems and practices to further secure the CNP environment.

F.5.2 Objectives and Principles

(a) The Guidelines are intended to represent best practice for Card Issuers and Acquirers, enabling CNP Transactions to take place with minimal disruption to the Cardholder whilst managing the security of Card data.

(b) The Guidelines are not intended to, and do not, of themselves:

(i) affect the rights of any Card Scheme administrator to establish scheme rules in relation to CNP fraud management;

(ii) affect the right of any Card Issuer or Acquirer to exercise commercial freedom in the selection of third party service providers or partners;

(iii) affect the obligations of any Card Issuer or Acquirer as a subscriber to the ePayments Code or to its Cardholders more generally; or

(iv) affect the right of any Card Issuer or Acquirer to determine to apply different requirements or standards to those set out in the Guidelines.

(c) The Guidelines are technology neutral and are not to be construed as promoting, endorsing or impeding any particular fraud solution or service provider(s).

(d) APCA does not enforce any Acquirer or Card Issuer's adoption or use of, or compliance with, these Guidelines.

(e) APCA will monitor and review periodically these Guidelines to ensure they remain effective and relevant; particularly as global standards develop.

F.5.3 Glossary

In this document:

Acquirer means a body corporate which provides transaction acquiring services on behalf of a Merchant.

AFCX means the Australian Financial Crimes Exchange.

APCA means Australian Payments Clearing Association Limited (ABN 12 055 136 519).

AS2805 means the authorisation protocol used in Australia for payment Card transaction messages.

Authentication means the act of confirming either a transaction or a person's identity is genuine and not originating from a fraudulent source.

BIN means the bank identification number allocated in accordance with ISO/IEC 7812

Card means any payment Card, device, application or identifier provided by a Card Issuer, which is linked to an account or credit facility operated by them.

Cardholder means a customer of a Card Issuer who is issued with a Card and PIN or other authentication method or process.

Card Issuer means a body corporate which, pursuant to the rules of a Card Scheme, issues a Card to a Cardholder and, in connection with any Card transaction effected using that Card assumes obligations to the relevant Cardholder.

Card Scheme means the set of functions, procedures, arrangements and rules that enable a Cardholder to make payment transactions with a third party other than the Card Issuer. For the avoidance of doubt, a Card Scheme may be a three-party scheme or a four-party scheme.

CNP means card not present.

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 app.

CVM means Cardholder Verification Method, used to evaluate whether the person presenting a payment instrument, such as a payment Card, is the legitimate Cardholder.

ePayments Code means the electronic payments code published by the Australian Securities and Investments Commission (ASIC), as amended from time to time.

EMV is the payment specification standard published by EMVCo that is used on electronic payment Cards incorporating an integrated circuit microchip.

EMVCo means EMVCo, LLC, the global technical body formed in 1999 that defines the standards for EMV payment Card processing.

FIDO Alliance means the Fast Identity Online Alliance, a not for profit organisation that develops standards for authenticating users of online services. Further information on the work carried out by the alliance can be found on their website: www.fidoalliance.org

Frictionless Authentication means Authentication without any interruption to the consumer during their online shopping experience.

IAC means the Issuers and Acquirers Community, APCA's industry forum for the development and administration of industry standards and policy for card payments in Australia.

ISO means the International Standards Organisation, responsible for ISO 7812 for the issuance of payment Card ranges to individual organisations and ISO 8583 for systems that exchange electronic transactions made by Cardholders using payment cards and other payment standards.

Jailbroken Device means a smartphone or other electronic device where restrictions imposed by the manufacturer or operator were removed, allowing the installation of unauthorised software or application.

MCC means Merchant Category Code, used to classify the Merchant by the type of goods or services it provides.

Merchant means a trading entity that has an agreement with an Acquirer to process and settle their Card payment transactions.

PA DSS means Payment Application Data Security Standard for Card payment applications, as amended from time to time.

PAN means Primary Account Number. The number assigned by a Card Issuer to a debit or credit Card.

Payment Account Reference (PAR) provides a means by which systems that made use of the original PAN such as fraud pattern detection systems or a Merchant loyalty scheme can continue to be effective without the PAN data being available. PAR Data was introduced to the EMV Payment Tokenisation Technical Framework[5] to provide stakeholders in the payment value chain with a means by which they could link multiple payment tokens that reference back to one or multiple Cards.

PCI DSS means the Payment Card Industry Data Security Standard for Card transactions, as amended from time to time.

PCI SSC means the Payment Card Industry Security Standards Council, the overarching body responsible for producing payment Card security standards such as PCI DSS.

Phishing means the fraudulent practice purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit Card numbers, online.

POS means the Point Of Sale in a Card present environment, utilising a POS device where the customer pays.

Privacy Act means the *Privacy Act 1988 (Cth).*

Static Authentication means Authentication using a method, such as a code, that is unchanging and remains the same over multiple requests. Such codes are more vulnerable to compromise as they can be re-used by fraudsters.

Token Requestor means an entity in the payment chain requesting the Token Service Provider to issue a token in place of a PAN. Merchants, Card Issuers, Digital Wallet providers or other parties can all perform the role of Token Requestor.

TSP means Token Service Provider, an entity that provides a token service, comprising a token vault and related processing, and which has the ability to use licensed ISO BINs as token BINs to issue payment tokens for PANs that are submitted in accordance with EMVCo's Payment Tokenisation Specification.

---

[5] *EMV specification bulletin No.167, January 2016*

W3C means the World Wide Web Consortium, responsible for the development of global web standards. Further information on the work carried out by the consortium can be found on their website: www.w3.org

CARD ISSUER AND ACQUIRER BEST PRACTICE GUIDELINES

F.6 CARDHOLDER DATA AND ITS SECURITY

F.6.1 Protect Cardholder data

(a) Acquirers and Card Issuers should ensure the protection of the Cardholder's Card data during transactions. This includes during any correspondence, written or electronic, to prevent any unauthorised party gaining access to it. Where reference to the Primary Account Number (PAN) is required, a truncated version of it should be used where possible. Each Acquirer and Card Issuer should ensure that any third party service provider engaged in transaction processing also meets the requirements in this section.

(b) Each Acquirer should have a plan in place to ensure PCI DSS requirements are met by their online Merchants in accordance with PCI Data Security Standards v3.2 (published April 2016 and effective 1st February 2018).

(c) Each Acquirer and Card Issuer should aim to provide Merchants with solutions which will assist them in reducing their PCI SSC obligations such as tokenisation or hosted payment page solutions and to decrease the risk of Card data being lost or stolen.

(d) Each Acquirer and Card Issuer should consider the use of EMV payment tokens to protect the PAN in the environments in which payment tokens may be used. For further information on tokenisation, refer to section 9.

F.6.2 Maximise the use of available data

(a) It is noted that construction of the authorisation message (AS2805 / ISO8583) is based on data elements which effectively limit the data available to support authorisation. However, each Acquirer and Card Issuer should consider inclusion of additional information that could be used to assess the risk of a transaction. For example, Acquirers and Card Issuers should consider capturing information on the use and behaviour of the device initialising the payment to provide further input to decision making.

(b) Each Card Issuer should consider leveraging the data obtained between Cardholder application, authorisation and authentication systems so that each environment has as much visibility and data for assessing risk as possible.

(c) Each Card Issuer should consider leveraging the data available from cross-channel banking systems (such as mobile transaction banking application activity) to provide a broader view of any suspicious account activity when assessing each transaction request for risk.

(d) Each Acquirer and Card Issuer should consider the value of leveraging data sharing entities to detect and prevent further fraud through the sharing of data on compromised accounts or methods of operation. For example, AFCX has recently been established to facilitate information sharing.

(e) Each Card Issuer and Acquirer should consider the use of external data sources to validate the Cardholder such as the geolocation capabilities of Digital Wallets and/or the biometric and device proximity capabilities of smartphones.

F.6.3 Privacy – Treatment of data generated during transactions

(a) Compliance with the Privacy Act:

All entities which collect, use and disclose Cardholder personal information in Australia are bound by their respective obligations under the Privacy Act.

(b) Disclosure of transaction data to Card Issuer:

Acquirers should have effective arrangements in place with Merchants to ensure that they can lawfully disclose authentication and geolocation transaction data generated during a CNP Transaction to Card Issuers for effective investigation and resolution of CNP fraud events.

(c) Terms and Conditions on merchant website

Acquirers should ensure that merchant terms and conditions reflect these practices within their Merchant Services Agreements.

F.7 CARDHOLDER AUTHENTICATION

(a) The Card Issuer is responsible for determining the appropriate CVM and therefore should:

(i) ensure the CVM method selected for a Card is in accordance with any applicable Card Scheme rules;

(ii) avoid Static Authentication for Cardholders. Static Authentication is not recommended for CNP Transactions as unsuspecting Cardholders may disclose this information without knowledge, allowing the data to be re-used by unauthorised persons for subsequent transactions;

(iii) consider delivery of one time passcodes (OTPs) via a method other than SMS to reduce the threat of interception (e.g. digitally certified push notifications); and

(iv) if SMS is used, then additional controls should be in place to identify and/or mitigate the risk of intercepted SMSs.

(v) consider the use of additional fraud tools where OTP is delivered by SMS.

(b) Each Card Issuer should consider Frictionless Authentication to verify a transaction where possible, through the capture of data such as (but not limited to) device ID, geo-location, device proximity, Wi-Fi connectivity and time of day.

(c) In circumstances where messages are exchanged between Acquirers and Card Issuers to authenticate Cardholders:

(i) the Card Issuer should consider the implementation of access control servers that support enhanced data collection to perform risk based authentication using techniques such as device and user profiling;

(ii) the Card Issuer should ensure that where risk based authentication is in place, there is sufficient monitoring in place to ensure the risk scoring accuracy is upheld; and

(iii) the Acquirer and Card Issuer should also consider implementing industry standard message protocols for improved risk analysis to facilitate Frictionless Authentication and support multiple device form factors.

(d) Each Acquirer should encourage Merchants to implement a Risk Based Approach (RBA) to authenticating the Cardholder so as not to impact low risk transactions but to provide an additional level of verification for higher risk transactions.

(e) Each Card Issuer should consider the use of dynamic data that is stored outside of the integrated circuit or magnetic stripe on the Card and that could be included as part of the CNP authorisation message, for example data that can be provisioned via a Card Issuer smartphone application.

(f) Each Card Issuer should ensure that any third party vendors of authentication solutions support local Australian requirements (such as network selection for multi-network Cards).

(g) Each Card Issuer and Acquirer should consider making available cardholder authentication options for each individual payment channel including but not limited to POS terminals, internet and in app payment.

(h) Each Card Issuer and Acquirer should consider emerging online global standards currently under development. This includes (but is not limited to) the work being undertaken by the likes of W3C and the FIDO Alliance.

F.8 FRAUD DETECTION

(a) Each Acquirer and Card Issuer should ensure the integrity of the data provided in the authentication message is present and the data is verified as valid. As much of this data as possible should be captured by the fraud detection system to provide better visibility of the transaction scenarios.

(b) Each Acquirer and Card Issuer should make use of real-time fraud detection systems.

(c) Each Acquirer and Card Issuer should ensure sufficient monitoring of fraud detection systems is in place to maintain their effectiveness.

(d) Where feasible, each Acquirer and Card Issuer should make use of data available outside of the traditional authorisation message – such as unexpected variations to device ID history or non-financial events (e.g. recent change of account holder's phone number or address) – to profile each transaction request with increased accuracy and to highlight any potential risks.

(e) Each Acquirer and Card Issuer should consider the use of additional Card Scheme services that support network level analysis on transactional and other available data.

(f) The use of external data from telecommunication networks may also be leveraged by each Acquirer and Card Issuer as part of its risk assessment to validate whether the phone number of a Cardholder has been recently ported.

(g) Data sharing opportunities can allow for Card Issuers to be alerted by Merchants of any high risk transactions that may have been stopped by the Merchant's own fraud tools prior to it being sent to the Card Issuer. This data could be used to alert the Card Issuer should the same Card be attempted to be used to pay for goods at another Merchant that may be less prepared to identify the risk.

(h) In the same way defined in section 6.2, the Card Issuer should consider the use of shared data to alert Merchants of suspicious activity on, or the compromise of, specific Cards.

(i) Each Card Issuer and Acquirer should consider sharing any identified fraud data with the AFCX and/or other data sharing organisations to prevent fraudulent activity across different entities in the payment value chain.

(j) Each Card Issuer should consider the use of transaction history from other domains such as POS or telephone orders as well as cross channel banking activity in any risk scoring.

(k) Each Card Issuer and Acquirer should make use of validation services on specific data types to ensure details provided are not fictitious and are related to the Cardholder.

(l) Each Acquirer should consider promoting the benefits of real-time fraud detection approaches to their Merchants.

F.9 TOKENISATION

(a) Each Card Issuer and Acquirer should consider the use of payment tokens and benefit from a reduced risk of fraud exposure in the event of a Merchant data breach. It may also prevent the expense and inconvenience of needing to re-issue Cards and address Cardholder enquiries.

(b) Each Card Issuer should consider the following:

(i) To ensure the integrity of tokens is maintained, each Card Issuer should provision payment tokens limited for usage via individual devices, channels or Merchants. This includes (but is not limited to):

(A) Location, such as domestic country of issue, a list of allowed countries or select Merchants;

(B) Network – use of one token per payment network to facilitate the multi-network operations;

(C) Goods & services – the token may be restricted to be used for payments in only selected MCCs (i.e. travel, retail or financial services);

(D) Payment channel such as contact EMV (Card chip), NFC for contactless payments via mobile phone, or eCommerce (also referred to as “domains”);

(E) Device – use of one token per payment device e.g. smartphone, wearable, tablet or plastic Card; and

(F) Limiting the number of times a specific token can be used for payment.

(ii) EMV tokenisation services may be provided by one or more certified Token Service Provider (TSP) such as scheme, or the Card Issuer may choose to implement a token provisioning platform of their choice. Card Issuers should take into consideration:

(A) Certification efforts with the various stakeholders in the payments value chain (Card Schemes, Acquirers, TSPs and others); and,

(B) Tokenisation at the farthest point possible in the payment chain (the Card Issuer) eliminates the exposure of the PAN to all other entities thus reducing the impact of any Merchant data breach.

(iii) Card Issuers and Acquirers should ensure that the PAR Data is passed in all relevant token and transaction messages to ensure the integrity and efficacy of fraud detection systems as Cardholder data is replaced by one or more payment tokens.

(c) Where the Acquirer or Card Issuer fulfils the role of the Token Requestor the level of appropriate Cardholder authentication during enrolment should be carefully considered.

F.10 CARDHOLDER EDUCATION AND MERCHANT FRAUD PREVENTION

(a) Card Issuers should use reasonable endeavours to educate their Cardholders around the risks of CNP Transactions, both in app and online. Cardholders should be given clear and accessible information in relation to:

(i) protection of the device(s) used to make remote purchases e.g. PC, smartphone, tablet etc. This should include topics such as exercising caution around the installation of unknown applications to reduce the risk of malware, anti-virus protection, and the use of Jailbroken Devices. Information should also cover the impact these can have to the Cardholder's security and data privacy;

(ii) enrolment in any authentication solution provided by the Card Issuer;

(iii) potential techniques used by fraudsters to obtain personal and financial details and how best to avoid them (e.g. only providing their Card details on secure websites, avoiding following links sent via SMS or email, Phishing techniques and identity theft);

(iv) the potential risks of placing purchases at non-reputable or unfamiliar websites; and

(v) the importance of regularly checking industry led initiatives, such as education forums about online safety to keep abreast of current developments.

(b) Acquirers should pro-actively educate their Merchant customers about online fraud and techniques available to combat it. In particular, Acquirers should focus on those MCCs that are exposed to a high risk of fraud and make use of available resources such as those available on APCA's "Get smart about Card fraud online" online tool[6].

(c) Acquirers should endeavour to provide alerts to their Merchants if vulnerabilities become known to applications, systems, processes or other components used in the Merchant operating environment to prevent further loss of Cardholder data.

(d) In the absence of a Merchant-owned fraud detection and prevention strategy, Acquirers should encourage their Merchant customers to adopt suitable fraud detection and authentication solutions offered by their chosen payment service provider.

(e) Acquirers should consider the benefits of educating Merchants around their selection of third party providers of online products such as shopping cart software. Acquirers and Merchants should focus on ensuring that product vendors meet PCI SSC standards, such as PCI DSS and PA DSS.

END

[6] www.apca.com.au/getsmart