Effective:
21 November 2017
Version 006

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 2
Issuers Code

Commenced 1 July 2015

Australian Payments Network Limited
Level 23, Tower 3, International Towers Sydney, 300 Barangaroo Avenue, SYDNEY NSW 2000
Telephone: (02) 9216 4888 Facsimile: (02) 9221 8057

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 2
Issuers Code

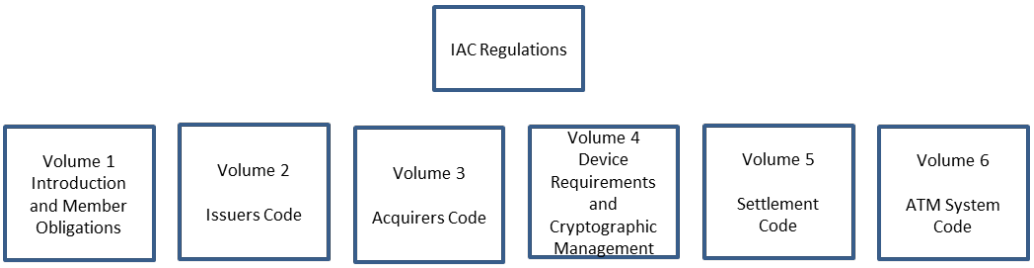
INDEX

PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this manual

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

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



Volume 2 is intended for Issuers and contains, when read in conjunction with Volume 1, those aspects of Personal Identification Number (PIN) and device security that are considered mandatory for all Issuers participating within the IAC. In addition this volume contains guidance and recommendations into non-mandatory aspects of Issuer PIN management.

Part 2 of this volume identifies the mandatory standards specified by the IAC for PIN management as well as recommended practices for the handling of Cardholder PINs. Part 3 covers recommended practices for PIN change over open networks such as the Internet or mobile phones whilst Part 4 covers device management and security including remote access requirements for security control modules. Devices covered are Key Transfer and Loading Devices (KTD, KLD) and Security Control Modules (SCM).

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.

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

Inserted effective 21.11.17

"**Approved Cardholder**" means: Inserted effective 1.1.16

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

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

"**Approved Card Payment System**" 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

"**AusPayNet**" means Australian Payments Network. Inserted effective 21.11.17

"**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 AusPayNet.

"**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:

(iii) clears Items directly; and

(iv) 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 trusted agent.

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

Next page is 2.1

PART 2 ISSUER PIN MANAGEMENT AND SECURITY

2.1 PIN standards

Each Issuer must comply with the current version of ISO 9546.1 which specifies requirements for the management and security of any current PIN, unless a specific exemption is permitted by the IAC Code Set.

Amended effective 21.11.16

2.2 Obligation to use compliant SCMs

SCMs used by Issuers for the handling or management of plaintext PINs and/or related keys must, at a minimum, satisfy current IAC SCD Security Standards (see Part 2 of IAC Code Set Volume 4 (Device Requirements and Cryptographic Management)) and be approved for use by the Company in accordance with Part 3 of IAC Code Volume 4.

2.3 Approval of new or modified SCMs

(a) Any Issuer certified in accordance with Part 3 of Volume 1 of the IAC Code ("certified Issuer"), who proposes to implement a new SCM, must apply for approval of the device as required in accordance with clause 2.2.

(b) Any certified Issuer, which proposes to:

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

(ii) continue to employ an SCM 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 SCM's cryptographic devices, PIN or cryptographic key handling and management processing;

must apply for approval of the device as required by clause 2.2 as if each device is a new device for the purposes of that section.

2.4 Cryptographic standards

Issuers must ensure that all cryptographic operations associated with the processing of Transactions and PIN management satisfy the cryptographic standards set out in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

2.5 PIN generation

Random, including customer-selected, PIN is the preferred option for PIN generation. Where a derived PIN is produced, the PIN derivation technique must be based on a cryptographic algorithm which employs a minimum key size of 128-bits.

2.6 PIN change

PIN change and PIN distribution over any form of open network (e.g., Internet, mobile phone and not using secure cryptographic devices, must conform to the requirements specified in Part 3 of this Volume 2.

2.7 Offline PIN

(a) If offline PIN verification is supported, Australian IC Cards that can be used to initiate a Transaction must be capable of Dynamic Data Authentication (DDA) or Combined Data Authentication (CDA).

(b) Protection of an offline PIN, during transmission to the IC Card must employ an asymmetric cipher mechanism compliant with part 7 of EMV 4.3 Specifications, Book 2 - Security and Key Management. The use of a separate PIN encryption key pair is highly recommended (available from www.emvco.org).

2.8 PIN block formats

Where a message contains PIN data, 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 1 and 2.

Last amended effective 21.11.16

2.9 PIN entry attempts

The number of PIN entry attempts allowed by an Issuer to a Cardholder prior to disabling Card access is at the Issuer's discretion. However, it is recommended that the minimum number of PIN entry attempts (whether consecutive per an individual Transaction or cumulative over a given period of time – generally 24 hours) should be set at 3.

Next page is 3.1

PART 3 PIN USAGE OVER OPEN NETWORKS

Amended effective 29.4.16

This Part 3 contains requirements for PIN usage in Issuer PIN change and delivery mechanisms, and internet banking registration systems, using open networks and not employing secure cryptographic devices for PIN entry, e.g. PEDS.

Where the new PIN is derived or generated by the Issuer (Issuer assigned PIN), delivery to the Cardholder is supported using Internet based mechanisms (e.g., browser based PC or smartphone) or using SMS messaging based mechanisms.

Where the new PIN is to be provided by the Cardholder (customer select PIN), only Internet based mechanisms are supported.

Where an open network is used to enable customer initiated PIN change and/or PIN delivery, or when the Cardholder is asked to provide a PAN and associated PIN in order to register online for internet banking, then the guidelines and requirements of this Part 3 apply. (See also clause 2.6 of this Volume 2).

Note: Issuers are referred to Annexure - A of this Volume 2 for further explanation of principles and requirements underlying the open network PIN change systems described here.

3.1 Principles and preferred model for open network PIN and PAN registration systems

Inserted effective 29.4.16

Open network PIN and PAN registration systems leverage a customer's PAN and associated PIN for one time user identification and authentication credentials. The following principles shall be applied to any PIN and PAN customer registration system over open networks (e.g., Internet, mobile phone etc.):

(a) The PIN and PAN customer registration system for internet banking shall protect the PIN at all times it traverses the Issuer's system through strong encryption[1]. The PIN should be passed as an approved encrypted ISO format PIN block, either format 0 or 3, with format 3 preferred.

(b) Each PIN shall be encrypted on the Cardholder's device to produce unique cipher text, (except by chance) to avoid the possibility of the construction of a rainbow[2] table.

(c) Except for on the Cardholder's device all decryption, translation, and re-encryption of PINs shall occur within an approved SCM/HSM.

[1] E.g. TDEA (112 bits of security), AES (128 bits and higher), RSA (2048 bits and higher), ECC (160 bits and higher), and ElGamal (2048 bits and higher). See NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for guidance on cryptographic key strengths and algorithms.

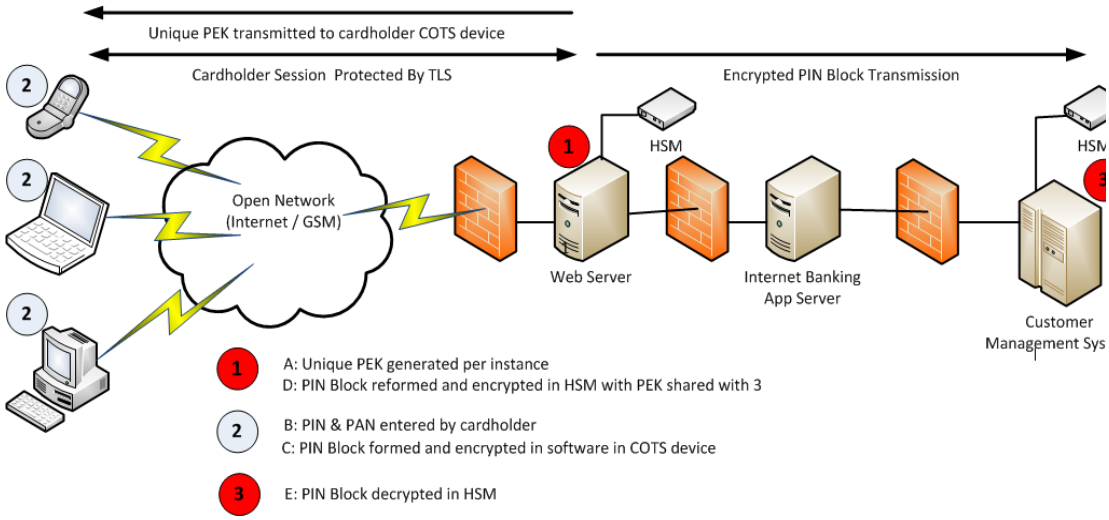
[2] A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes.

(d) The Cardholder's device should protect the PIN by forming an approved encrypted ISO format PIN block, either format 0, 3 or 4 immediately after PIN entry.

(e) The registration system should re-encrypt the customer's PIN block with a different PEK as soon as it is received from the customer.

In summary these principles are illustrated below.

Figure 1 – PIN encryption points during PIN and PAN Internet banking registration. (Example Architecture)



3.2 PIN and PAN Registration Systems over Open Networks – general requirements

Inserted effective 29.4.16

Customer PIN and PAN registration should only be performed using an Issuer approved device (see clause 3.13 of this Volume 2) and functionality, and should comply with the obligations set out below:

(a) PIN usage shall adhere to the principles set out in ISO 9564 (all parts) to the maximum extent possible consistent with the Issuer's security and risk management policies; Amended effective 21.11.16

(b) the plain text PIN shall never be transmitted over communications lines outside of a secure environment as specified in AS 2805.14.2:2009, clause H.5;

(c) PIN and PAN registration shall ensure that the plain text PIN must never be known to, or accessible by, any employee or agent of the Issuer;

(d) a detailed risk assessment paying particular attention to any deviations from the relevant standards – [AS 2805.14, ISO 9564, ISO 13491] - shall be an integral part of any Issuer's decision to provide functionality in support of PIN and PAN registration over open networks; and Amended effective 21.11.16

(e) to assist with fraud monitoring and problem resolution, Issuers should record PIN and PAN registration events including date, time, frequency and the channel over which the event occurred (without recording any PINs).

3.3 Cardholder authentication for PIN and PAN registration systems

Inserted effective 29.4.16

(a) Issuers should:

(i) provide Cardholders with a means to determine that the dialogue with the Issuer is genuine;

(ii) use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and to implement additional Cardholder authentication;

(iii) ensure that PIN and PAN registration systems over open networks provide mutual assurance to the Issuer and Cardholder that they are both genuine e.g., using a separate channel to deliver acknowledgements; and

(b) It is recommended that Issuers also do the following:

(i) acknowledge PIN and PAN registration events back to the Cardholder using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a Cardholder;

(ii) pay particular attention to device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g., browser capable smartphones; and

(iii) provide Cardholders with the means to confirm the outcome of a PIN and PAN registration event.

3.4 Principles and preferred models for open network PIN change and delivery

Amended effective 1.7.2015

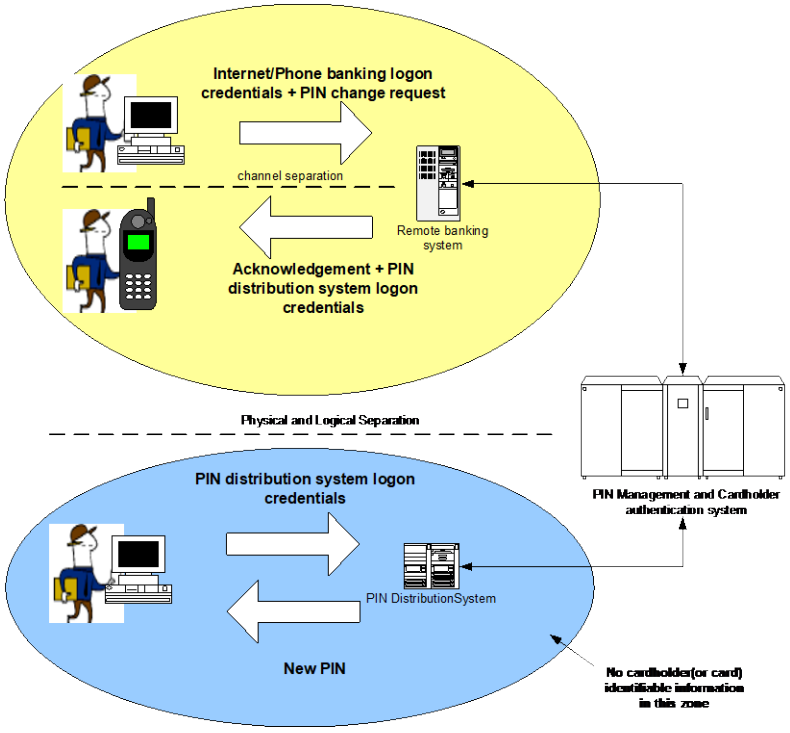
The following principles should be applied to any PIN change and delivery system over open networks (e.g., Internet, mobile phone etc.):

(a) The PIN change and delivery system should be separate to all other PIN processing and card management systems. Its domain should contain no Cardholder identifying/authentication information other than that associated with the PIN change and delivery system itself;

(b) The identification and authentication credentials for the PIN change and delivery system should be communicated to the Cardholder using a totally separate out-of-band channel[3] from that used by the Cardholder to initiate the PIN change or issuance function. These credentials should be time bound and unique per PIN change or delivery event.

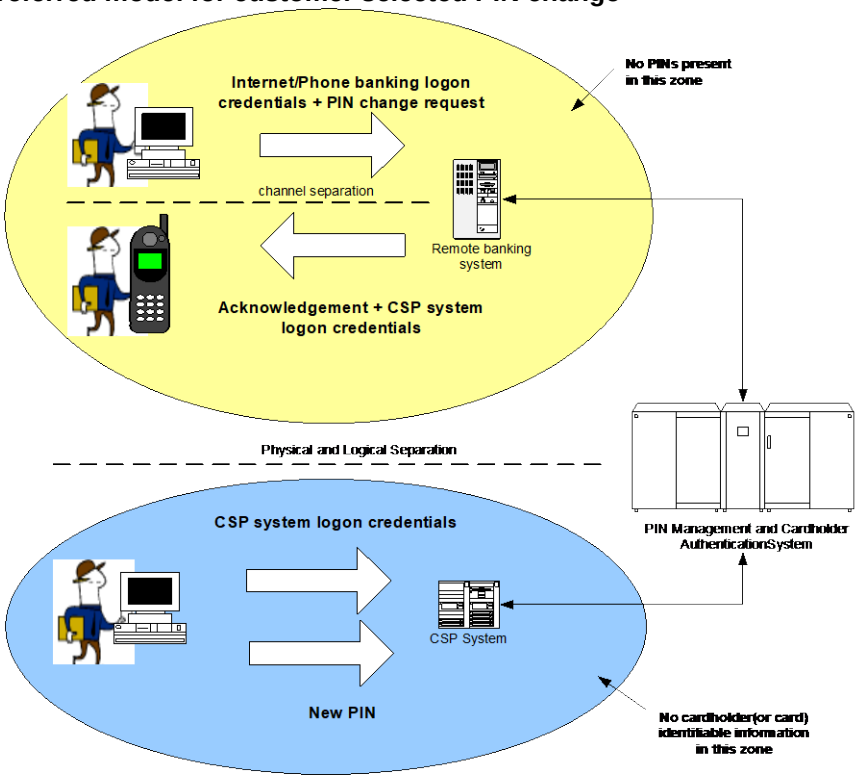
In summary these principles are illustrated below.

Figure 2 - Preferred model for Issuer assigned PIN issuance/change



[3] Out-of-band authentication requires a separate, discrete pathway, such as a telecommunications network, be used in the authentication process. This provides a second secure channel in the event the primary Internet channel is compromised. An attacker would have to exploit both the Internet channel and the secondary one -- the phone network or end-user device -- to launch a successful attack.

Figure 3 - Preferred model for customer selected PIN change



3.5 PIN change and delivery over Open Networks – general requirements

Amended effective 1.7.2015

Cardholder PIN change and delivery shall only be performed using an Issuer approved device (see clause 3.13 of this Volume 2) and functionality, and shall comply with the obligations set out below: Amended effective 29.4.16

(a) PIN change and delivery must adhere to the principles set out in ISO 9564 (all parts) to the maximum extent possible consistent with the Issuer's security and risk management policies; Amended effective 21.11.16

(b) PIN selection shall not be performed using mail (traditional post or otherwise), unless specifically authorised in the IAC Code Set; Amended effective 29.4.16

(c) PIN change and delivery must ensure that the plain text PIN must never be known to, or accessible by, any employee or agent of the Issuer;

(d) PIN change and delivery must only be initiated by the Cardholder;

(e) the host SCM functionality that is used to implement customer select PIN change should be atomic, that is, verification of the Cardholder using the current PIN or account specific control number should be an intrinsic part of that functionality. Specifically an SCM function that accepts a new PIN and a PAN and that outputs an offset and/or PVV for storage in a host database should not exist unless it additionally embodies strong Cardholder authentication as per clause 3.6 of this Volume 2;

(f) the PIN change and delivery process shall ensure the authenticity of the Cardholder; Amended effective 29.4.16

(g) a detailed risk assessment paying particular attention to any deviations from the relevant standards – [AS2805.14, ISO 9564, ISO 13491] - must be an integral part of any Issuer's decision to provide functionality in support of PIN change and delivery over open networks; Last amended effective 21.11.16

(h) to assist with fraud monitoring and problem resolution, Issuers shall record PIN change and delivery events including date, time, frequency and the channel over which the event occurred (without recording any PINs); and Amended effective 29.4.16

(i) the Open Network PIN change/delivery system should not be the sole PIN change or delivery mechanism available to Cardholders.

3.6 Cardholder authentication for PIN change or delivery

(a) Issuers shall: Amended effective 29.4.16

(i) provide Cardholders with a means to determine that the dialogue with the Issuer is genuine;

(ii) ensure that Cardholder authentication credentials are not based on information that is publicly available;

(iii) ensure that the Cardholder's card number cannot be determined solely from the Cardholder's authentication credentials;

(iv) ensure that it is not possible to authenticate a Cardholder using only information contained on the card or other payment instrument;

(v) not transmit the PAN to the Cardholder during a PIN change or delivery operation, nor require that the Cardholder enter such information;

(vi) implement a policy to never send unsolicited PIN change requests and advise Cardholders accordingly;

(vii) use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and to implement additional Cardholder authentication;

(viii) ensure that PIN change or delivery systems requiring the transmission of the PIN over open networks provide mutual assurance to the Issuer and Cardholder that the correct PIN is being delivered to, or from, the genuine Cardholder e.g., using a separate channel to deliver acknowledgements; and

(b) It is recommended that Issuers also do the following:

(i) avoid the use of the card PIN for non-payment transactions including access to electronic banking; Amended effective 29.4.16

(ii) acknowledge PIN change and delivery requests back to the Cardholder using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

(iii) pay particular attention to device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g., browser capable smartphones;

(iv) manage the risks associated with possible redirection of PIN change request or delivery acknowledgements through, for example, phone number porting;

(v) provide Cardholders with the means to audit the outcome of a PIN change or delivery request; and

(vi) ensure that no staff member can legitimately associate a control number with a card number or account.

3.7 PIN advice generally (assigned or derived PIN)

(a) Issuer approved methods of conveying the PIN to the Cardholder shall meet the following requirements: Amended effective 29.4.16

(i) the plain text PIN shall never be transmitted over communications lines outside of a secure environment as specified in AS 2805.14.2:2009, clause H.5, unless there is no feasible way in which the PIN could be associated with the Cardholder, the Cardholder's account or card;

(ii) the Issuer's employees, staff and agents shall not handle the plain text PIN where any of the associated card or account details are also available to them;

(iii) Issuers shall appropriately evaluate and manage the risks associated with change of destination requests from Cardholders;

(iv) Issuers shall examine, on a regular and frequent basis, their procedures and associated risks for delivering cards and PINs to Cardholders.

(b) It is recommended that Issuers also do the following:

(i) ensure that physical distribution of a PIN is made only to pre-registered Cardholder destinations;

(ii) ensure that electronic distribution of a PIN is made only to strongly authenticated Cardholders as per clause 3.6.

3.8 PIN advice by SMS (Issuer assigned PIN)

(a) In addition to the requirements of clause 3.7 of this Volume 2, where an Issuer assigned PIN is conveyed to the Cardholder via an SMS message, the following requirements shall be met: Amended effective 29.4.16

(i) Issuers shall provide the Cardholder with security advice for the management of the mobile phone used for PIN advice. This shall include advice about the dangers of malware and of storing account data and/or PINs on the phone or any additional copies made of the phone data e.g., via synchronizing the data between the mobile phone and a personal computer;

(ii) only pre-registered mobile phone numbers shall be used for PIN advice;

(iii) if control numbers and authentication values are used then the SMS PIN advice message shall be preceded by a communication to the Cardholder containing an identification value or control number and an authentication value. This communication should use a different mechanism other than SMS;

(iv) the identification value or control number and authentication values shall not disclose the account or card numbers;

(v) if the identification value is publicly available, such as the Cardholder's phone number or email address, then a second non-public identification value or mechanism shall be used;

(vi) the PIN distribution system shall have no way of associating an identification value with a specific Cardholder's name, address, account or card number;

(vii) all PINs, control values and authentication data shall be encrypted using strong encryption[4] during transmission to, and storage in, the PIN distribution and PIN management systems;

(viii) the PIN advice message shall be preceded by a Cardholder initiated request;

(ix) the PIN request message shall contain the Cardholder's identification and authentication values;

(x) the PIN distribution system shall transmit the PIN to the Cardholder only upon successful validation of the authentication value;

[4] See 3.1 (a)

(xi) the PIN distribution system shall have limits on the number of attempts made to retrieve a PIN;

(xii) it shall not be possible for authorised staff with access to the PIN distribution system to access any other system where associated Cardholder data can be accessed. Additionally the PIN distribution system database shall be separate to any other database containing Cardholder data;

(xiii) the authentication and identification values together with the PIN shall be deleted from the PIN distribution system immediately after successful delivery is confirmed;

(xiv) the Issuer shall establish an allowable storage window for the PIN distribution system after which time the PIN shall be deleted from the system whether delivered or not;

(b) It is recommended that Issuers also do the following: Inserted effective 29.4.16

(i) the PIN distribution system should run on a dedicated system and be isolated from any other network by a dedicated firewall;

(ii) the PIN distribution system should perform no other function than PIN distribution and any sessions established during the distribution shall be terminated once the PIN has been sent;

(iii) the association of the PIN to a specific account or card number should not be possible with the authorising information available on the PIN distribution system;

(iv) where required, the PIN distribution system should decrypt the PIN immediately prior to transmission to the Cardholder;

(v) it should not be possible to identify the type of Cardholder payment device, account or card number from the SMS message containing the PIN.

3.9 PIN advice by internet (Issuer assigned PIN)

(a) In addition to the requirements of clause 3.7 of this Volume 2, the following requirements apply where the PIN is communicated to the Cardholder using the internet: Amended effective 29.4.16

(i) Issuers shall provide the Cardholder with security advice for the management of the end-user device (e.g., PC, Smartphone, etc.) used for PIN advice. This shall include advice about the dangers of malware and of storing account data e.g., Cardholder statements and/or PINs on the end-user device or any additional copies made of the data e.g., backups;

(ii) the PIN shall be cryptographically protected whilst in storage or transmission using strong encryption[5]. PIN transmission should be in accordance with the requirements of clause 3.14 of this Volume 2;

(iii) the encrypted PIN shall be decrypted for display on the end-user device's display by the Issuer-provided application;

(iv) initiation of the PIN advice shall require that the Cardholder enter pre-established credentials such as a control number and authentication value;

(v) as the security of the PIN advice implementation is based on the premise that no individual, other than the Cardholder, can associate the control number with a specific account or card number, it is essential that the pre-established credentials shall not disclose the card or account numbers;

(vi) if control numbers and authentication values are used then the control number and authentication values shall be communicated using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

(vii) any key used to generate a control number shall not be used for any other purpose and shall be managed in accordance with AS 2805.6.1;

(viii) the PIN, and if control numbers and authentication values are used, then the authentication values as well, shall not be logged and shall be deleted immediately after use;

(ix) if control numbers and authentication values are used then issuers shall ensure that the association of Cardholder authentication credentials with a control number does not weaken the principle that the control number cannot be used to determine a specific account or card number;

(x) if control numbers and authentication are used then Cardholder authentication not be performed by the Internet server but rather by the back end Issuer host system and only after the control number has been re-associated with a specific account;

(xi) web servers shall be configured to disable client side caching of web pages that display PIN and associated data during the Internet session.

[5] See 3.1(a)

(b) It is recommended that Issuers also do the following: Inserted effective 29.4.16

(i) if control numbers and authentication values are used then the control number should be generated and delivered to the Cardholder in such a way, e.g., by using a tamper evident mailer, such that no-one, other than Cardholder, can associate that control number with that Cardholder without detection;

(ii) if control numbers and authentication values are used then the control number should be communicated to the Cardholder in such a way that no-one, other than the Cardholder, can access it without detection;

(iii) if control numbers and authentication values are used then the PIN distribution system should have no way of associating a control number with a specific Cardholder's name, address, account, card or phone numbers;

(iv) if control numbers and authentication values are used then the PIN advice function should exchange only strings of numbers (a control number and authentication values) with the Issuer PIN distribution system i.e., there should be no other Cardholder identifying information, other than the control number, exchanged during the PIN delivery function;

(v) if control numbers and authentication values are used then the PIN management system should re-associate the control number with a specific account number, validate the Cardholder using the authentication values and retrieve the Cardholder PIN for that account number;

(vi) if control numbers and authentication values are used then the PIN distribution system should be designed and operated under strictly enforced conditions such that no individual, other than the Cardholder, is able to associate a control number, PIN or authentication values with any specific card or account number;

(vii) if control numbers and authentication values are used then PIN delivery to the end-user equipment (e.g., PC or smart-phone) should not be associated with any Cardholder account data or card number;

(viii) internet PIN advice should be protected using a secure channel established between the client application and the PIN distribution system according to the principles set out in ISO/IEC 11770; and

(ix) the implementation should take into account malware attacks such as man-in-the-browser or man-in-the-middle.

3.10 Customer select PIN change – general

(a) Issuers should advise Cardholders against using the PIN as a credential for electronic banking or any other service and provide an alternative input format for electronic banking credentials e.g., forbidding all numeric passwords.

(b) Issuers shall: Amended effective 29.4.16

(i) provide the Cardholder with appropriate guidance for PIN selection and usage; and

(ii) provide and use cryptographic mechanisms for protecting the PIN from the point of entry and beyond.

3.11 Customer select PIN change by Internet

(a) In addition to the requirements of clause 3.10 of this Volume 2, the following requirements apply where the Cardholder is allowed to change the PIN using the internet: Amended effective 29.4.16

(i) Issuers shall provide the Cardholder with security advice for the management of the end-user device used for PIN selection. This shall include advice about the dangers of malware and of storing account data and/or PINs on the end-user device or any additional copies made of the device's data e.g., backups;

(ii) the PIN shall be cryptographically protected whilst in storage or transmission using strong encryption[6]. PIN transmission shall be in accordance with the requirements of clause 3.14 of this Volume 2;

(iii) initiation of PIN selection shall require that the Cardholder enter pre-established credentials such as a control number and authentication value;

(iv) as the security of the PIN selection is based on the premise that the design and implementation of the system is such that no individual, other than the Cardholder, can associate the control number with a specific account or card number it is essential that the control number and authentication value, where used, not disclose the card or account numbers;

(v) If control numbers are used then the control number and authentication values shall be communicated using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

[6] See 3.1(a)

(vi) any key used to generate a control number shall not be used for any other purpose and shall be managed in accordance with AS 2805.6.1;

(vii) the PIN and authentication values shall not be logged and must be deleted immediately after use;

(viii) internet PIN selection shall be protected using a secure channel established between the client application and the CSP PIN management system according to the principles set out in ISO/IEC 11770;

(ix) the implementation should take into account malware attacks such as man-in-the-browser or man-in-the-middle;

(x) issuers shall ensure that the association of Cardholder authentication credentials with a control number does not weaken the principle that the control number cannot be used to determine a specific account or card number;

(xi) if control numbers are used then Cardholder authentication shall not be performed by the Internet server but rather by the back end Issuer host system and only after the control number has been re-associated with a specific account;

(xii) web servers shall be configured to disable client side caching of web pages that display PIN and associated data during the Internet session.

(b) It is recommended that Issuers also do the following: Inserted effective 29.4.16

(i) If control numbers are used then the control number should be generated and delivered to the Cardholder in such a way (e.g., by using a PIN mailer) that no-one, other than Cardholder, can associate that control number with that Cardholder without detection; Amended effective 29.4.16

(ii) the control number should be communicated to the Cardholder in such a way that no-one, other than the Cardholder, can access it without detection;

(iii) the CSP PIN change system should have no way of associating a control number with a specific Cardholder's name, address, account, card or phone number;

(iv) the PIN advice function should exchange only strings of numbers (a control number and authentication values) with the Issuer CSP PIN change system i.e., there should be no other Cardholder identifying information, other than the control number, exchanged during the PIN change function;

(v) the PIN management system should re-associate the control number with a specific account number, validate the Cardholder using the authentication values and retrieve the Cardholder PIN for that account number;

(vi) the CSP PIN change system should be designed and operated under strictly enforced conditions such that no individual is able to associate a control number, PIN or authentication values with any specific card or account number;

(vii) Cardholder authentication and generation of the reference PIN should be done in real-time during the session with success or failure reported back to the Cardholder.

3.12 Customer select PIN Change by mobile phone

(a) PIN selection via SMS or DTMF tone signalling is not permitted.

(b) The use of Internet-based PIN change on Internet-enabled mobile phones shall comply with the requirements of clause 3.11 of this Volume 2. Amended effective 29.4.16

3.13 Issuer approved PIN Entry Devices (PEDs)

(a) In accordance with clause 3.5, only Issuer approved devices should be used for PIN entry supporting PIN change or selection or PIN and PAN registration. Such devices should be one or more of the following: Amended effective 29.4.16

(i) a functionally secure device i.e., a device that can be compromised only by physical means and whose functionality cannot be subverted through unauthorised inputs to the device; or

(ii) a device providing a level of logical security sufficient to protect the PIN and other account data.

(b) Issuers shall ensure that: Amended effective 29.4.16

(i) Cardholders are fully educated as to their responsibilities for the management and protection of permitted personal devices;

(ii) Cardholders are adequately warned about the inherent dangers in storing the PIN;

(iii) Cardholders are provided with a means of ensuring that the communication is genuinely with the Issuer;

(iv) it is possible for the Cardholder to determine that a genuine end-to-end communication with the Issuer is occurring rather than a phishing or other man-in-the-middle malware masquerading as the Issuer application;

(v) the PIN is protected with strong encryption[7] between the approved personal use device and the Issuer; Amended effective 29.4.16

(vi) Cardholders are provided with easy access to applicable malware countermeasures for any approved personal use devices and be made aware of the risks associated with malware;

(vii) PIN change, and PIN and PAN registration applications should provide a mechanism to protect the PIN during PIN entry in case man-in-the-browser or other root-kit attacks are in place, that are undetectable by common anti-virus countermeasures. Amended effective 29.4.16

3.14 PIN transmission

(a) PINs and associated account data transmitted between systems shall be protected against disclosure, and the integrity of the PIN protected against any party eavesdropping on, or manipulating, the communications link. PIN integrity refers to the integrity of the relationship between the PIN and any associated information such as user account data. Amended effective 29.4.16

(b) Issuers shall: Amended effective 29.4.16

(i) protect the PIN during transmission by at least one the following methods;

(A) provision of physical protection;

(B) encryption of the PIN value; or

(C) disassociation of the PIN from the account data, with PIN integrity maintained through the use of an encrypted control value;

(ii) use transmission protocols designed such that the introduction of fraudulent messages, or modification of valid messages, does not yield any useful information concerning the PIN;

(iii) use cryptographic mechanisms such that PIN integrity is ensured;

(iv) where the PAN is available, only encipher PINs using one of the PIN block formats specified in ISO 9564.1 with format 3 preferred; Last amended effective 21.11.16

(v) where the PAN is not available;

(A) use an encrypted control value uniquely linked to the PAN to construct the PIN block. The construction should provide the same security properties as provided by ISO PIN blocks;

[7] See 3.1(a)

(B) the method used to format the PIN block prior to encryption should not enable the PIN to be recovered from the resulting ciphertext (e.g., by using rainbow tables[8]);

(vi) ensure that any PIN translation conforms to the guidance in ISO 9564.1, but only to the extent that such guidance is consistent with the Issuer's security and risk management policies;

(vii) If control numbers are used then ensure that the association of Cardholder authentication credentials with the control number does not weaken the principle that the control number cannot be used to determine a specific account; Amended effective 29.4.16

(viii) use only cryptographic algorithms specified in ISO 9564.2 to provide PIN secrecy and integrity; and Amended effective 29.4.16

(ix) ensure that clear text PIN transmission does not contain any information that can be directly connected with the Cardholder or the account/card number.

Next page is 4.1

[8] See 3.1(b)

PART 4 DEVICE SECURITY STANDARDS

This Part 4 sets out the minimum security standards applicable to Secure Cryptographic Devices (SCDs), including HSMs/SCMs and Key Loading devices (KLDs) that are required to be met by all Issuers.

4.1 Relevant standards

The security standards applicable are contained in:

(a) AS 2805 all parts;

(b) ISO 9564 all parts;

(c) ISO 13491 all parts;

(d) ISO 11568 all parts;

(e) Guidelines for EFT Security (published by the Australian Payments System Council); and

(f) ISO TR14742 Recommendations in relation to cryptographic algorithms and their use;

are considered normative to this security standard. As standards are evolving documents the latest version of these standards should be taken as the normative reference unless specifically identified otherwise.

4.2 Secure Cryptographic Devices

(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 be approved for use using the process described in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

(b) If an Issuer wishes to implement a new SCD for which a Letter of Approval is not held, the Issuer must arrange for that device to be evaluated for conformity with the current applicable SCD security standards, using the device approval process in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

4.3 Device management

4.3.1 *Security Control Modules (Host Security Modules)*

(a) SCMs shall be managed in accordance with the requirements of AS 2805.14.2. The Sponsor must submit to the committee of management an annual compliance statement confirming compliance with Annexures A.3, C.3, E.3 of this Volume 2 and either H.4 or H.5 of AS 2805.14.2 (in respect of any SCMs employed in the implementation of Interchange Transactions. Annexure B.3 of Volume 1 used in connection with the Annual Security Audit (see 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 AusPayNet Specification for a Security Control Module function Set such that all functions not required for the normal operation of the system must be disabled.

4.3.2 *Key Loading and Transfer Devices (KLDs, KTDs)*

Devices used in the initial cryptographic key loading of SCMs or PEDs must be managed in accordance with the requirements of AS 2805.14.2. The Sponsor must submit to the committee of management 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 SCM or PED cryptographic keys (see Annexure B.3 of Volume 1 (Introduction and Member Obligations used in conjunction with the annual Security Audit programme (see IAC Code Set Volume 1 (Introduction and Member Obligations)), provides the required confirmation.

4.4 Security Control Module - limitations on functions

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

4.4.1 *Function set*

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

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

(i) standard functions approved in writing by the Company (e.g., AusPayNet2000 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.

4.4.2 *DEA-1*

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

4.5 Remote management of Security Control Modules

This clause applies to systems which support remote access for the management of SCMs.

4.5.1 *SCM access requirements*

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

(b) there must not be uncontrolled connections between general internal and external networks;

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

(d) for TCP/IP implementations:

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

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

(iii) such firewalls must log and monitor all inbound and outbound traffic to the SCMs.

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

4.5.2 *Management of SCM Remote Management Solutions*

(a) Remote Management Solutions ("RMS") may only be used with AusPayNet approved SCMs;

(b) all SCM RMS must be evaluated to the requirements specified in Volume 4 (Device and Cryptographic Requirements) of the IAC Code and approved for use by the Company;

(c) 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:

(i) the storage of the RMS must be under dual control;

(ii) the operation of the RMS must be under dual control; and

(iii) while the RMS is in operation access must be restricted to authorised personnel.

Next page is A.1

ANNEXURE A GUIDELINES FOR ISSUING PREPAID CARDS

[Informative]

This annexure provides guidelines for IA Participants which participate or propose to participate in the issuance and/or acceptance of Prepaid Cards.

A.1 CARD CHARACTERISTICS

Prepaid Program Providers and sponsoring Issuers should ensure that Prepaid Cards comply with the following guidelines:

(a) Card physical characteristics;

Prepaid Cards should as a minimum, meet the specifications detailed in AS 3521, 3522 and 3524. These standards contain requirements for physical characteristics, dimensions, layout of information and format for encoding Tracks 1 and 2 of the magnetic stripe.

(Note: Cards that do not comply with these guidelines may not be able to generate Transactions at ATMs and/or EFTPOS terminals.)

(b) Minimum descriptive requirements for Prepaid Cards;

(i) Prepaid Cards may, on their front face;

(A) be clearly identified as a Prepaid Card; and

(B) clearly indicate that they should only be used when online authorisation is available (the words "Electronic use only" or similar are recommended);

(ii) The embossing of the PAN and expiry date on Prepaid Cards is optional.

(Note: Prepaid Program Providers and sponsoring Issuers should consider the requirements of other regulatory instruments such as the Australian Securities and Investment Commission's Regulatory Guide 185: Non-Cash Payment Facilities and as an example, its requirements in respect of expiry dates.)

A.2 ENCODING AND TRANSMISSION OF TRACK 2 DATA

(a) Prepaid Program Providers and sponsoring Issuers should ensure encoding of Track 2 on Prepaid Cards in accordance with the requirements of AS 3524 (encoding of Track 1 and Track 3 on Prepaid Cards is optional).

(b) Acquirers should transmit all Track 2 data received by the Acquirer from the Terminal to the Issuer without alteration.

A.3 PERSONALISATION

There are no mandatory requirements for the personalisation of Prepaid Cards.

A.4 SIGNATURE PANEL REQUIREMENTS

There is no mandatory requirement for a signature panel on Prepaid Cards.

A.5 PIN STANDARDS

(a) The use of a PIN for Cardholder authentication is not mandatory.

(b) However, when prompted for a PIN, the entry of a four digit number by the Cardholder is mandatory to facilitate the carriage of the Transaction across the Interchange network.

A.6 UNIQUE BINS

Prepaid Program Providers and sponsoring Issuers should ensure that Prepaid Cards are only issued under BINs that are unique from BINs under which non Prepaid Cards are issued.

A.7 TEST CARDS

Prepaid Program Providers and sponsoring Issuers that give notice of the introduction of a new BIN or a change to the routing of an existing BIN for a Prepaid Card pursuant to clause 2.8.2 in the IAC Code Set Volume 1 (Introduction and Member Obligations) must, on request by the affected IAC Members ensure production of any necessary test Cards in sufficient time to allow testing to occur before the applicable Institutional Identifier Change Date.

A.8 INTERCHANGE SETTLEMENT

Prepaid Card Transactions must be settled in accordance with IAC Code Set Volume 5 (Settlement Code).

A.9 DISPUTES

(a) Prepaid Cards are not generally issued with a secure owner authentication mechanism. Therefore, unless bilaterally agreed to the contrary:

(i) Prepaid Cardholder disputes are to be resolved by the applicable Prepaid Program Provider; and

(ii) the other parties involved in the Transaction should co-operate with the Prepaid Program Provider.

(b) It is recommended that IAC Members agree to apply standard IAC dispute resolution processes to Transactions initiated with Prepaid Cards if a PIN (the security of which is managed in accordance with Part 2 of this Volume 2) was issued to the original Prepaid Cardholder.

(c) Settlement disputes between IAC Members are to be resolved in accordance with IAC Code Set Volume 5 (Settlement Code).

Next page is B.1

ANNEXURE B PIN CHANGE OVER OPEN NETWORKS – GUIDELINES

[Informative]

B.1 INTRODUCTION

The purpose of these IAC Guidelines is to provide additional explanatory material for the range of PIN management mechanisms (namely PIN issuance and change) using open networks and issuer approved devices supported in the IAC Code Set.

Where the new PIN is derived or generated by the Issuer (Issuer assigned PIN) delivery to the Cardholder is supported using Internet based mechanisms (PC or smart-phone) or SMS messaging.

Where the new PIN is to be provided by the Cardholder (customer select PIN or CSP) only Internet based mechanisms are supported.

B.2 OBJECTIVES

The intent of the IAC requirements and recommendations is to manage the exposure of PINs and associated data used in enabling PIN management on open networks that could be used to clone Cardholder payment devices and discover PINs for use in any payment channel.

The objectives of the individual components of a PIN management system are identified in subsequent sub-paragraphs.

B.2.1 ISSUER APPROVED DEVICES

Applications that use an Issuer approved device for PIN entry in the Issuer security domain should restrict availability of PINs and related processed account data to other devices, applications and fraudulent access.

B.2.2 PIN TRANSMISSION

PINs and associated account data transmitted between systems should be protected against disclosure and the integrity of the PIN protected against any party eavesdropping on, or manipulating, the communications link. PIN integrity refers to the integrity of the relationship between the PIN and any associated information such as user account data.

B.2.3 CARDHOLDER AUTHENTICATION

Issuers that allow Cardholders to remotely manage their PINs via the internet or Mobile phone may authenticate Cardholders by providing credentials to a CSP PIN change or PIN distribution system (hereafter these systems are referred to as PIN handling systems). Vulnerabilities in these systems could lead to PIN compromise.

B.2.4 PIN ADVICE

Plaintext PINs and associated account details should only be visible to Cardholders.

B.2.5 PIN CHANGE

Plaintext PIN values and associated account details should only be visible to the associated Cardholders.

B.3 THREATS

The following threats are likely to exist against any PIN handling system implemented using open networks without the assistance of secure cryptographic devices. Threats, other than those identified, may additionally be present and any user should fully familiarize themselves with the risks associated with their particular implementation.

B.3.1 ISSUER APPROVED DEVICES

(a) The PIN and associated account data processed in an Issuer approved device are vulnerable to eavesdropping which may arise if the device used for PIN entry has been compromised in any way, either by physical tampering or by execution of malicious software;

(b) Issuer host systems may not check for the presence of a magnetic stripe during a magnetic stripe transaction authorization. For example, authorization may rely solely on online PIN verification and correctness of the submitted PAN. Thus, cross-contamination of magnetic stripe payment transaction technology may be enabled through PIN management technology, i.e., Issuer PIN management may enable a mag-stripe clone to be created without the full mag-stripe present because the issuer does not perform sufficient security checking.

B.3.2 PIN TRANSMISSION

(a) Phone tap/wire tap. (GSM, VoIP, DTMF tones may be in the clear);

(b) Reliance on network encryption (which is not under the application's control and which may not be present or may use a compromised cryptographic technique);

(c) Attacks against the cryptographic algorithms used to encipher PIN codes and provide PIN integrity.

B.3.3 CARDHOLDER AUTHENTICATION

(a) If the credentials for accessing the PIN handling system are the same as those displayed on the Cardholder payment device, an attacker with access to the device could impersonate a Cardholder to access the system;

(b) The channel used to access the PIN management systems may be compromised;

(i) for example malware installed on a PC or installed to a mobile (root kits, sniffers and keystroke loggers, MITB, MITM) may retrieve Cardholder data. Credentials can be recorded and transmitted to fraudsters;

(ii) DNS poisoning may lead to pharming attacks where the Cardholder browser is redirected to a fraudulent website;

(c) Displayed Cardholder data may be surfed or screen scraped;

(d) Vishing (the criminal practice of using social engineering over the telephone system or SMSishing) may be used to socially engineer the Cardholder into entering credentials into a malicious application;

(e) Calling line identification can be spoofed;

(f) Calls to a nominated mobile number can be maliciously forwarded to another number without the Cardholder's knowledge;

(g) A fraudster may impersonate the customer at an issuer branch and present forged documents to inexperienced issuer personnel;

(h) If unsolicited PIN management requests from the issuer to Cardholders are possible, for example via call-centre, email or SMS, a Cardholder may be socially engineered into revealing login credentials.

B.3.4 PIN ADVICE

(a) A Cardholder doesn't destroy the mailer or message containing the PIN;

(b) A Cardholder family member gains access to the Cardholder payment device and PIN after delivery;

(c) An insider at a mail sorting office intercepts the PIN mailer and the Cardholder payment device;

(d) An insider at a mail sorting office intercepts the PIN mailer and the Cardholder payment device, creates cloning data, then forwards both to the Cardholder - possibly avoiding detection;

(e) A telephone engineer eavesdrops call traffic to a call centre or IVR;

(f) IMSI grabbers eavesdrop GSM communication;

(g) Internet Service Provider personnel eavesdrop email and internet traffic;

(h) IVR or web systems may be subject to hacking or eavesdropping. Retrieved PIN and Cardholder data may be sufficient to clone a Cardholder payment device;

(i) Issuer PIN storage systems used for PIN delivery may be hacked;

(j) Cardholder PCs or mobile phones used for PIN advice may contain malware that can forward PIN and Cardholder data to criminals;

(k) A fraudster impersonates customers and socially engineers a bank representative to change Cardholder addresses so that cards and PINs are redirected.

B.3.5 PIN CHANGE

(a) Customer may select a PIN value that is easy to guess;

(b) See also PIN advice threats.

B.4 AN EXAMPLE IMPLEMENTATION OF THE PREFERRED MODELS FOR OPEN NETWORK PIN CHANGE AND DELIVERY

Amended effective 1.7.2015

As described below, separation is the key principle in the IAC Code Set used to achieve reasonably secure open network PIN handling systems.

(a) The PIN handling system should be separate to all other PIN processing and Card management systems. Its domain should contain no Cardholder identifying/authentication information other than that associated with the PIN handling system itself;

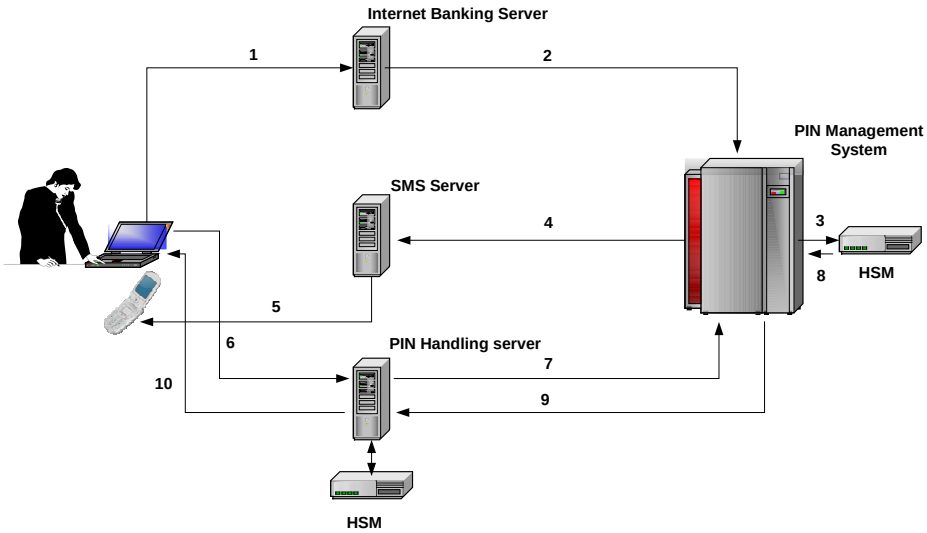
(b) The identification and authentication credentials for the PIN handling systems should be communicated to the Cardholder using a total separate out-of-band channel than that used by the Cardholder to initiate the PIN change or issuance function. These credentials should be time bound and unique per PIN handling event.

B.5 EXAMPLE IMPLEMENTATION

An example implementation, not using control numbers, is illustrated below.

Figure 3 - Example CSP implementation

Amended effective 1.7.2015



The operation of the system is as follows:

(a) the Cardholder logs onto the Internet banking system and requests as PIN change (either Issuer assigned or customer select);

Login credentials to the Internet banking system are user ID and password;

(b) the Internet banking system forwards the request through to the Issuer's PIN management system;

Request includes user ID, password and an identifier to the particular card that is the subject of the PIN change request;

(c) the PIN management system selects the correct PAN and the user's pre-identified phone number. The PIN Management system uses the SCM to generate a derived, unique authentication value;

(i) note that the PIN management system must be able to determine the correct PAN and the phone number that has been previously selected by the customer (alternatively it needs to identify the alternate, out-of-band, channel to be used);

(ii) the PIN management system uses the SCM to derive or calculate a unique authentication value that can be uniquely tied to this PIN change instance. Additional information (e.g., a salt) may be stored in the PIN management system. Nothing other than the PIN management system should be able to determine the PAN from this authentication value (this is ensured through the use of the SCM;

(d) the PIN management system delivers this value to the SMS server;

(e) the Authentication value is delivered to the Cardholder's phone via SMS;

(f) Cardholder logs onto the PIN change system using the newly received authentication value as part of the logon credentials and either requests transmission of the new PIN (if Issuer assigned PIN system) or provides a new PIN if it's a customer select PIN system;

(g) the Cardholder may need to provide additional identification information if publicly known data is used in the logon process. No card identifying information can form part of this access;

(h) the PIN handling system provides this information to the PIN management system;

(i) the PIN management system verifies the authenticity of the Cardholder, reassociates the request with the correct card and either updates the PIN database with the new PIN information (if CSP) or generates a new PIN (is Issuer assigned PIN);

(j) PIN management system provides, via an encrypted channel, the new PIN to the PIN handling system (if Issuer assigned PIN) or indicates the success of the PIN change;

(k) the PIN handling system provides the new encrypted PIN to the Issuer provided application in the Cardholder's browser where it is decrypted for display or otherwise indicates the success of the PIN change to the Cardholder.

A key unstated requirement of this implementation is that the Cardholder's logon credentials not disclose the card number. Alternative implementations may choose to use control numbers, also communicated to the Cardholder out-of-band, as identifiers in the PIN handling system to ensure that the authentication credentials cannot be used to identify the Cardholder or their card numbers.

Next page is C.1

ANNEXURE C DEBIT CARD FRAUD PREVENTION GUIDELINES

[Informative]

Annexure C is confidential

Next page is D.1

ANNEXURE D THIRD PARTY DIGITAL WALLET SECURITY: CARD ISSUER GUIDELINES

Inserted effective 21.11.16

[Informative]

Best practice guidelines for Card Issuers in relation to third party mobile wallet security

D.1 CONTEXT

D.1.1 Introduction

AusPayNet is Australia's peak payments industry association. We work with our members and other payments industry stakeholders to identify and manage security risks in payment systems and payment technologies.

AusPayNet supports payments technology innovation that meets Australian security requirements and that preserves consumers' confidence and trust in the payments system. Mobile banking and payment services, mobile / digital wallets and third party digital wallets are emerging features of the global and Australian payments landscape that potentially offer significant consumer benefits.

Digital or mobile wallets are software applications on consumer devices which act as a repository for payment and other cards, and which by provisioning encrypted payment card data, effectively enable 'card present' mobile payment transactions at POS and in application. Third Party Digital Wallets are those which may be provided by a third party using multiple Card Issuers' payment Card data, customer relationships and existing payment networks, as well as various intermediaries and service providers. Australians are well-served by a robust consumer protection framework for mobile banking and mobile payment services - the *ePayments Code* – which attributes primary liability for unauthorised transactions made by use of such facilities to the Card Issuer subscriber which has promoted or endorsed that facility, even where the liability might be attributable to another party in the shared network.

These Guidelines have been issued by AusPayNet as *industry best-practice* to help Card Issuer members of the IAC to understand and proactively manage potential fraud and security risks in the provision of Third Party Digital Wallet services. They are voluntary.

As an adjunct to the Guidelines, AusPayNet will periodically convene open mobile payments industry fora, develop publications and white papers and invite consultation to promote understanding of, and consider developments in, mobile payments security and fraud management issues.

D.1.2 Scope

The Guidelines focus on the issues which typically require consideration by a Card Issuer in the context of provisioning its Cards to third party mobile wallets, including customer identification and verification, authentication of transactions and management of token generation and Card data security.

These Guidelines are not intended to address the issues of liability apportionment between Cardholders, Card Issuers, Digital Wallet Providers and other parties to a Third Party Digital Wallet transaction: this is a proprietary matter for parties to resolve.

The Guidelines do not apply to software applications that process payments solely using card-on-file data provided directly by a Cardholder to the payment service provider, where 'card-not-present' liability arrangements apply.

The Guidelines have not been drafted to apply to Card Issuers' proprietary mobile banking applications or proprietary wallet services, being those provided by a Card Issuer solely for its own customers. The responsibility for managing fraud and security of proprietary wallet services, and the liability for, and reputational risk associated with, losses resulting from use of proprietary products, rests entirely with the Card Issuer. A Card Issuer may choose to apply aspects of these Guidelines to its proprietary mobile banking applications and wallet services where appropriate.

D.1.3 Objectives

(a) The purpose of the Guidelines is to assist Card Issuers with establishing their respective security and data privacy requirements for Third Party Digital Wallets to promote the integrity and security of these services.

(b) The Guidelines are voluntary and are intended to represent industry best practice for security and tokenisation of mobile payment transactions and for privacy and limited permitted disclosure of Cardholder and mobile payments data.

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

(i) presume, affect or prescribe the terms of any arrangement established by any Card Issuer with any Digital Wallet Provider/s;

(ii) affect the rights of any Card Scheme administrator to establish scheme rules for provisioning its co-branded Cards to Digital Wallets or the obligations of any Card Issuer under those rules;

(iii) affect the right of any Card Issuer to exercise commercial freedom in the selection of mobile payments services processors and partners;

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

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

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

(e) Card Issuers are encouraged to promote awareness of the Guidelines amongst Digital Wallet Providers, Card Scheme administrators, and other participants in the provision of Digital Wallet services.

(f) Card Issuers are encouraged to ensure that the provisioning of Cards to a Third Party Digital Wallet does not affect or derogate from the intrinsic capabilities and functions of Cards, or any priority network arrangement that applies to them.

(g) AusPayNet does not monitor or enforce any Card Issuer's adoption or use of, or compliance with, these Guidelines.

(h) AusPayNet will periodically review these Guidelines to ensure they remain effective and relevant, particularly as international standards for mobile payments develop, and may amend them from time to time.

D.1.4 Glossary

In this document:

AusPayNet means Australian Payments Network Limited (ABN 12 055 136 519).

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

Card means any card, device, application or identifier provided by an Issuer, which is linked to an account or credit facility with the Card Issuer.

Cardholder means a customer of an 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, which obligations are in the first instance discharged on its behalf by an acquiring institution.

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.

CVM means Cardholder verification method.

Digital Wallet means a software application on a digital device that:

(a) functions as a digital container for payment Cards, tickets, loyalty cards, receipts, vouchers and other forms of payment; and

(b) provisions and uses the encrypted Card data associated with an enrolled payment Card.

For the avoidance of doubt, a software application that processes payments solely using 'card on file' data is not a Digital Wallet for the purposes of these Guidelines.

Digital Wallet Provider means a body corporate which is a third party provider of Digital Wallet services to its, and a Card Issuer's, mutual customers/Cardholders.

ePayments Code means the electronic payments code published by ASIC, as amended from time to time.

EMV Card means a Card issued by a Card Issuer that contains an integrated circuit that conforms to EMV specifications, in respect of which the EMV Issuer Country Code data element (tag 5F28) is equal to "036".

IAC means the Issuers and Acquirers Community constituted by the Regulations.

ID&V means identification and verification.

PAN means primary account number.

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

Regulations mean the regulations for the IAC, as prescribed by AusPayNet, as amended from time to time.

Third Party Digital Wallet means a Digital Wallet that is provided by a Digital Wallet Provider.

TSP means 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 EMV Co's *Payment Tokenisation Specification*, version 1.0 (March 2014).

D.2 GUIDELINES

D.2.1 Security

D.2.1.1 Customer identification and authentication on enrolment

(a) The Card Issuer is responsible for making the decision as to whether a particular Card can be enrolled in a Third Party Digital Wallet.

(b) The Card Issuer is responsible for determining appropriate ID&V methods and the data elements required to support enrolment of its Cards into Third Party Digital Wallets. In determining appropriate ID&V levels, the Card Issuer should have regard to the following criteria:

(i) Enrolment ID&V for Third Party Digital Wallets should achieve levels of security that are, as a minimum, equivalent to ID&V used in the Card Issuer's proprietary digital wallets and/or Card Issuer mobile banking applications;

(ii) any 3D Secure processing standards which may apply (if a Card-based ID&V process is to be used); and

(iii) any relevant global industry best practices for ID&V.

(c) The Card Issuer may outsource key parts of its ID&V process to a third party (including the Digital Wallet Provider), but should ensure the third party meets the requirements in this section 1.1.

(d) The Card Issuer may authorise the enrolment of a particular Card in more than one Third Party Digital Wallet.

D.2.1.2 Customer authentication at the time of transaction

(a) The Card Issuer is responsible for determining the appropriate CVM for authenticating transactions made using the Card Issuer's issued Cards in accordance with any relevant Card Scheme rules in place for those Cards. To the extent the Card Issuer has the right to exercise discretion when determining appropriate CVMs, the Card Issuer should do so having regard to the following criteria:

(i) CVM for transactions in Third Party Digital Wallets must achieve levels of security which are as a minimum equivalent to CVM for transactions made using EMV Cards;

(ii) industry best practice; and

(iii) any list of CVMs that may have been approved by AusPayNet for Card payments in Australia.

(b) The Card Issuer should not use a CVM which is:

(i) inconsistent with the CVMs prescribed by the relevant Card Scheme rules applicable to the Card; or

(ii) not in AusPayNet's approved list of CVMs for Card payments in Australia.

(c) The Card Issuer may outsource key parts of the CVM process for Third Party Digital Wallet transactions to a third party, but should ensure the third party meets the requirements in this section 1.2.

D.2.2 Tokenisation

D.2.2.1 Use of Tokenisation Services

(a) Tokenisation is not compulsory for transactions made using a Third Party Digital Wallet if the Third Party Digital Wallet includes an embedded secure element solution. In this case, it is up to the Card Issuer to decide if tokenisation services are appropriate for Third Party Digital Wallet transactions made using the Card Issuer's issued Cards.

(b) Tokenisation should be used for transactions made using a Third Party Digital Wallet if:

(i) mandated by applicable Card Scheme rules; or

(ii) the Third Party Digital Wallet does not include an embedded secure element solution.

D.2.2.2 Selecting Tokenisation Services

(a) The Card Issuer is responsible for selecting token service provider/s, and may choose the tokenisation services of any TSP or supply its own tokenisation service, provided the chosen service conforms to the minimum standards prescribed by section 2.3.

(b) The Card Issuer may choose to use the tokenisation services of more than one TSP.

D.2.2.3 Minimum standards

The Card Issuer should ensure that any TSP it engages to provide tokenisation services meets the minimum standards set out in EMVCo's *Payment Tokenisation Specification – Technical Framework*, version 1.0 (published March 2014).

D.2.3 Privacy – Treatment of Data Generated During Transactions

D.2.3.1 Compliance with Privacy Act

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

D.2.3.2 Disclosure of Transaction Data to Card Issuers

It is advisable that the Card Issuer has effective arrangements in place to ensure that Digital Wallet Providers and, if applicable, other parties in a shared mobile payments network:

(a) have obtained Cardholders' informed consent to the disclosure of any authentication data and any geolocation data which may be collected by that Digital Wallet Provider or party in relation to a transaction effected using a Third Party Digital Wallet; and

(b) will disclose such information to the Card Issuer if it reasonably requests such information, from time to time, for the purposes of investigation and resolution of fraud, disputed and unauthorised transactions and Cardholder complaints.

Next page is E.1

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

Inserted effective 3.7.17

[Informative]

E.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 AusPayNet – to ensure they remain relevant and fit-for-purpose. This is especially important given predicted changes in the eCommerce space.

E.2 ONLINE PAYMENTS IN AUSTRALIA

E.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 AusPayNet website.

[1] AusPayNet Milestones Report – The Digital Economy November 2016.

E.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[2].

E.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.

[2] 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 AusPayNet[3] 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.

[3] The Australian Payments Fraud Report 2016.

Research commissioned by AusPayNet 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.

E.4 SOLUTIONS TO CARD NOT PRESENT FRAUD

Different jurisdictions worldwide have attempted to solve this problem in markedly different ways. Research conducted by AusPayNet 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 AusPayNet 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.

AusPayNet 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 AusPayNet 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.

E.5 PROPOSED SOLUTION - GUIDELINES

E.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.

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

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

E.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.

AusPayNet means Australian Payments Network 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, AusPayNet'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[4] 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.

[4] *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

E.6 CARDHOLDER DATA AND ITS SECURITY

E.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.

E.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.

E.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.

E.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.

E.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.

E.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.

E.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 AusPayNet's website e.g. "Get smart about Card fraud online".

(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