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

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 2
Issuers Code

INDEX

Australian Payments Network Limited [ABN 12 055 136 519]

PART 1   INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1   Purpose of this manual

Amended
effective 1.1.19

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:
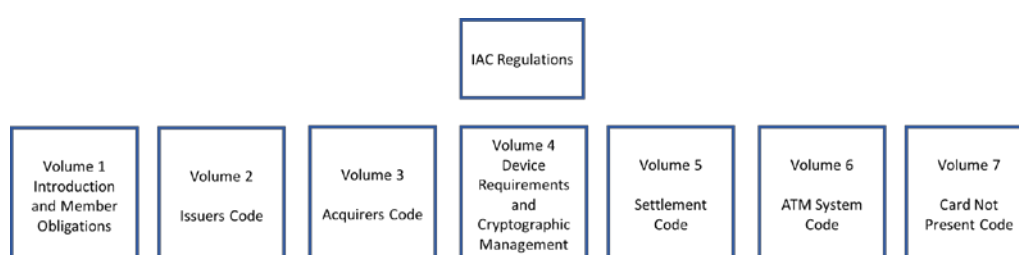
Amended
effective 1.7.19

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 identifies minimum requirements and 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). Part 5 of this volume, when read in conjunction with Volume 7, contains the requirements for Issuers dealing with Card Not Present Transactions, to mitigate the fraud associated with such Transactions.

Last amended
effective 1.7.19

1.2   Interpretation

In this IAC Code Set:

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

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

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

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

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

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

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

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

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

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

1.3   Definitions

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

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

Amended effective 1.1.20

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

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

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

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

Deleted effective 20.8.18 Inserted effective 21.11.17

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

"**Approved Cardholder**" means:

<div style="float:right">Inserted effective 1.1.16</div>

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

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

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

<div style="float:right">Amended effective 1.1.20</div>

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

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

"**Approved 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.

<div style="float:right">Amended effective 1.1.16</div>

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

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

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

<div style="float:right">Inserted effective 1.1.20</div>

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

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

"**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.

<div style="float:right">Amended effective 1.1.16</div>

"**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.

<div align="right">Inserted effective 1.1.16</div>

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

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

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

<div align="right">Inserted effective 1.1.16</div>

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

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

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

(a)   IA Participant;

(b)   ATM Operator Member; and

(c)   ATM Affiliate.

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

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

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

<div align="right">Inserted effective 1.1.16</div>

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

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

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

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

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

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

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

"**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).

<div align="right">Amended effective 1.1.16</div>

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

Amended effective 1.1.20

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

"**Authentication**" [Deleted]

Deleted effective 1.1.20

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

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

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

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

Last amended effective 1.1.20

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

Amended effective 1.1.20

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

Last amended effective 1.1.20

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

Inserted effective 1.1.19

"**Company**" means AusPayNet.

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

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

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

Inserted effective 20.8.18

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

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

Amended effective 1.1.20

"**Device Approval Applicant**" means:

Last amended effective 1.1.20

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

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

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

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

Last amended effective 1.1.20

"**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:

(a)   which the Cardholder denies having initiated; or

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

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

Amended effective 1.1.16
Inserted effective 1.1.16
Inserted effective 1.1.16
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**" [Deleted]

Deleted effective 20.8.18
Inserted effective 1.1.19

"**EFTPOS Terminal**" means a Terminal for processing EFTPOS Transactions.

"**EFTPOS Transaction**" is defined in the IAC Regulations and means a Transaction conducted at a Merchant's point of sale using a Terminal.

Last amended effective 1.1.20

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

"**EMV@ATM Terminal Standards**" means the standards and requirements set out in IAC Code Set Volume 6 (ATM System Code) Annexure G.

Amended effective 1.1.20

"**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 IAC Code Set Volume 6 (ATM System Code) Annexure G EMV@ATM Terminal Standards.

Amended effective 1.1.20

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

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

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

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

"**Evaluation Facility**" [Deleted]

Deleted effective 1.1.19 Last amended effective 1.1.20

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

(a)   an Approved Evaluation Facility; or

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

under the Device Approval Process.

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

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

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

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

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

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

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

"**Framework Participant**" is defined in the IAC Regulations and means a Constitutional Corporation:

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

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

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

"**Fraudulent CNP Transaction**" means a CNP Transaction which is also a Fraudulent Transaction.

"**Fraudulent Transaction**" means a Transaction reported to an international card scheme as fraudulent which:

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

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

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

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

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

Amended effective 1.1.20

(a)   an Issuer; or

(b)   an Acquirer; or

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

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

Inserted effective 1.1.20

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

Inserted effective 1.1.20

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

Amended effective 1.1.20

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

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

Amended effective 1.1.20

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

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

Amended effective 1.1.20

(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).

<div style="text-align:right">Amended effective 21.11.16</div>

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

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

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

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

<div style="text-align:right">Amended effective 1.1.20</div>

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

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

"**Issuer Authentication**" [Deleted]

<div style="text-align:right">Deleted effective 1.01.20</div>

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

<div style="text-align:right">Amended effective 1.01.20</div>

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

<div style="text-align:right">Amended effective 1.01.20</div>

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

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

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

<div style="text-align:right">Amended effective 1.1.20</div>

"**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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Inserted effective 1.1.20

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

Inserted effective 1.6.17

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

Inserted effective 1.1.20

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

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

Amended effective 1.1.20

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

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

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

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

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

Amended effective 20.8.18

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

Amended effective 1.1.19

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

Amended effective 1.1.19

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

Last amended effective 1.1.20

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

<div style="float:right">Amended effective 1.1.20</div>

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

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

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

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

<div style="float:right">Amended effective 1.1.20</div>

"**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.

<div style="float:right">Inserted effective 1.1.16</div>

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

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

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

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

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

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

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

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

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

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

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

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

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

Inserted effective 1.07.19

"**Recognised APS**" is defined in the IAC Regulations and has the meaning given in the Constitution.

Amended effective 1.1.20

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

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

Amended effective 1.1.20

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

"**Reporting Date**" means the 15th day of the month which follows the end of each Quarter, being 15 April, 15 July, 15 October or 15 January. If the 15th day of the month occurs on a weekend, the Reporting Date for that month will be the first business day following the 15th day.

Inserted effective 1.07.19

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

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

"**Risk Based Analysis**" has the meaning given to it in IAC Code Set Volume 7 (Card Not Present Code),clause 2.1.1.

Amended effective 1.01.20

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

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

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

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

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

"**SCD Security Standards**" in relation to an SCD, means the standards from time to time published in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), Part 2.

Last amended effective 1.1.20

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

Amended effective 20.8.18

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

Amended effective 1.1.20

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

Inserted effective 1.1.19

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

Amended effective 20.8.18

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

Amended effective 1.1.19

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

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

Amended effective 1.1.20

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

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

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

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

Inserted effective 1.1.19

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

Amended effective 20.8.18

"**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 $\square$ 2n the probability that all of the first L selected elements are different is no smaller than the probability of this happening when the elements are drawn uniformly at random from the set."

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

Amended effective 1.01.20

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

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

Last amended effective 1.1.19

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

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

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

(a) interchange;

(b) PIN processing;

(c) transaction processing;

(d) key management; or

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

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

Amended effective 1.1.20

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

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

Last amended effective 1.1.20

"**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, to the maximum extent possible subject to their security policies and risk management requirements.

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 minimum requirements specified in Part 3 clause 3.1 of this Volume 2, and have regard to the principles and best practice recommendations described in Part 3 of this Volume 2.

Amended effective 20.8.18

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

This Part 3 contains the principles and best practice recommendations as well as the minimum requirements for PIN usage in Issuer functionality offered over open networks which don't employ secure cryptographic devices for PIN entry. This includes, but is not limited to, PIN change and delivery mechanisms, internet banking registration systems, and other internet product offerings by an Issuer. (See also clause 2.6 of this Volume 2).

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.

3.1   Minimum Requirements for Open Network PIN and PAN Functions

Where an Issuer chooses to implement functionality, which involves open network transmission of the PIN, and where the principles and recommendations set out in clause 3.7 cannot be met, then:

(a)   the requirements set out below must be followed:

(i)   Concurrent existence of clear text PIN and PAN must be kept to the absolute minimum possible consistent with the functionality being implemented.

(ii)   Identification of the Cardholder must use additional identifying data other than that contained on or in the Card itself.

(iii)   Issuers must provide Cardholders with a means to determine that the dialogue with the Issuer is genuine.

(iv)   Issuers must use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and must implement additional Cardholder authentication. *Note: authentication via a mobile app on the phone and the phone itself are considered as different verification methods.*

(v)   All systems transporting PIN data or PAN data, or both, over open networks must provide mutual assurance to the Issuer and Cardholder that they are both genuine e.g. using a separate channel to deliver acknowledgements. *Note: messaging via a mobile app on the phone and the phone itself are considered as different channels.*

(vi)   All events involving the PIN or PAN, or both, back to the Cardholder must be acknowledged using an out-of-band mechanism i.e. through the use of two separate channels working simultaneously to authenticate a Cardholder. *Note: messaging via a mobile app on the phone and the phone itself are considered as different channels.*

(vii)   Issues must provide Cardholders with the means to confirm the outcome of events involving a PIN or a PAN or both.

(viii)   Issuers must consider threats arising through device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g. browser capable smartphones; and

(b)   It is also strongly recommended that:

(i)   The PIN should be encrypted immediately at the earliest point possible using an Issuer approved device.

(ii)   Identification of the Cardholder should occur prior to the entry of the PIN.

3.2   Recommendations for PIN and PAN registration systems over open networks

Amended effective 20.8.18

3.2.1   *Preferred model*

Inserted effective 20.8.18

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 should 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 should 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 should 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 should 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 PIN encrypting key as soon as it is received from the customer.

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

In summary these principles are illustrated below.
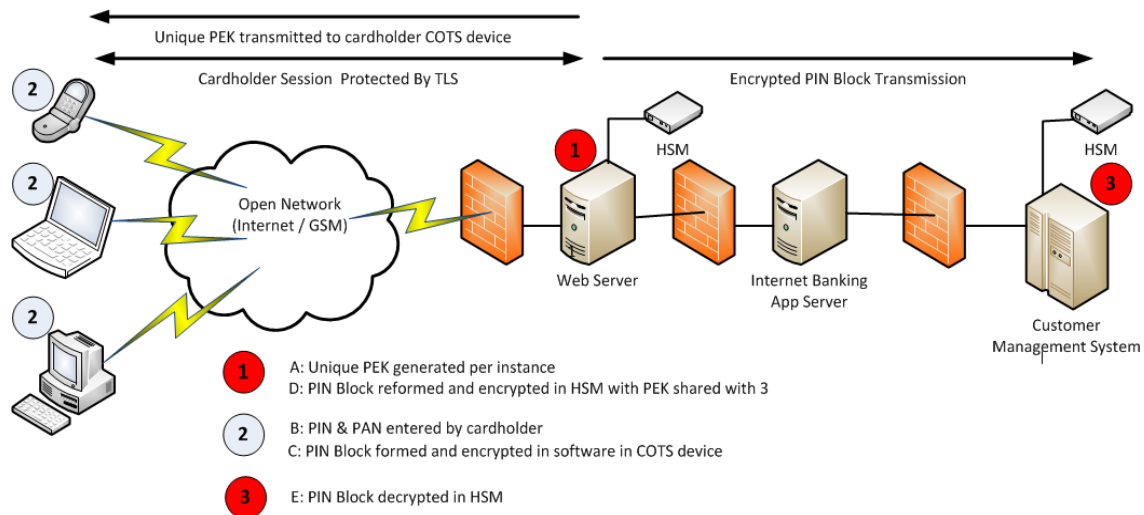
Figure 3.2. 1 – PIN encryption points during PIN and PAN Internet banking registration. (Example Architecture)

3.2.2 *Risk and security*

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

Customer PIN and PAN registration should only be performed using an Issuer approved device (see clause 3.6) and functionality, and should follow the recommendations set out below:

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

(a) PIN usage should 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;

<div align="right">Amended effective 21.11.16</div>

(b) the plain text PIN should 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 should ensure that the plain text PIN is never known to, or accessible by, any employee or agent of the Issuer;

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

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

<div align="right">Amended effective 21.11.16</div>

Australian Payments Network Limited [ABN 12 055 136 519]

(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).

3.2.3 *Cardholder authentication*

Issuers should:

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

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

(c) 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;

(d) 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;

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

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

3.3 Recommendations for PIN change and delivery over open networks

3.3.1 *Preferred model*

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.
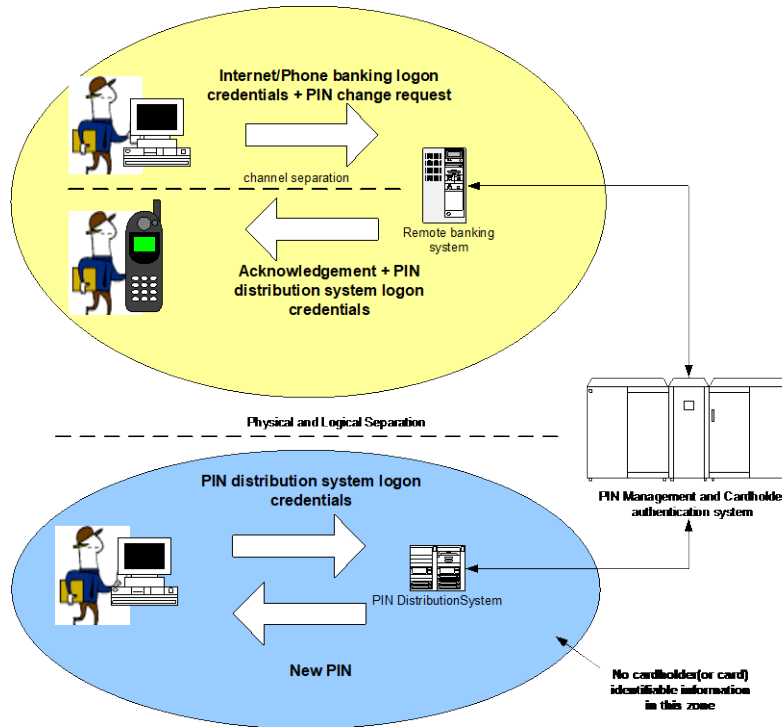
Figure 3.3.1A - Preferred model for Issuer assigned PIN issuance/change

---

[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.
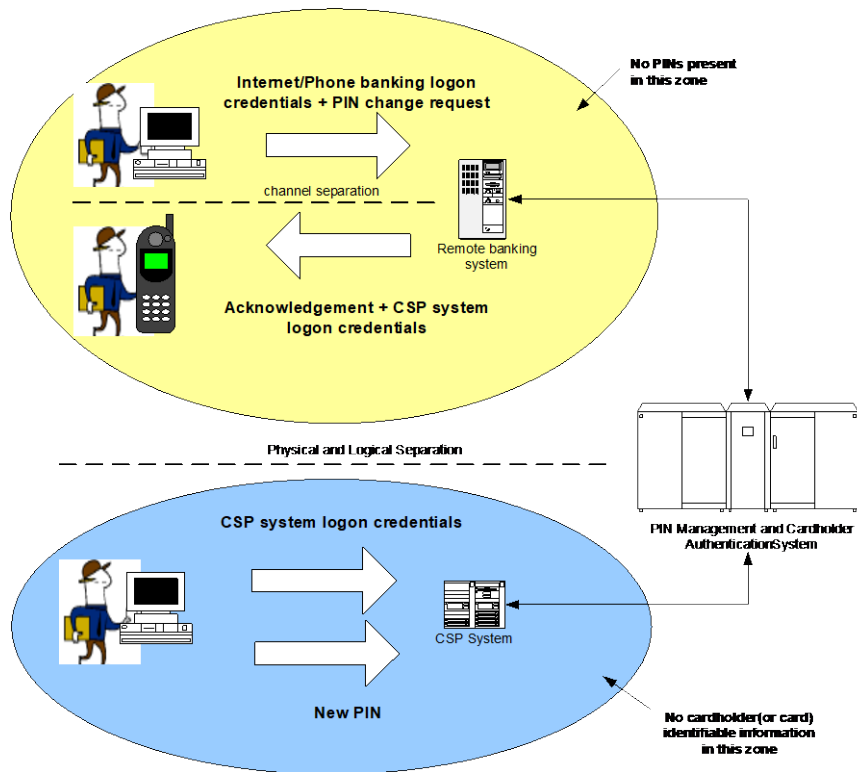
Figure 3.3.2B - Preferred model for customer selected PIN change

3.3.2 *Risk and security*

Cardholder PIN change and delivery should only be performed using an Issuer approved device (see clause 3.6) and functionality, and should follow the recommendations set out below:

(a) PIN change and delivery should 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;

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

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

(d) PIN change and delivery should 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 clause3.3.3;

Last amended effective 20.8.18

Last amended effective 20.8.18

Amended effective 21.11.16

Amended effective 29.4.16

Amended effective 20.8.18

Australian Payments Network Limited [ABN 12 055 136 519]

(f) the PIN change and delivery process should 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] - should 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 should 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.

3.3.3 *Cardholder authentication*

Amended effective 20.8.18

Issuers should:

Amended effective 29.4.16

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

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

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

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

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

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

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

(h) 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;

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

Amended effective 29.4.16

(j)   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;

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

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

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

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

3.4   Recommendations for PIN advice (assigned or derived PIN) over open networks

Amended
effective 20.8.18

3.4.1   *Methods of conveying the PIN*

Inserted
effective 20.8.18

Issuer approved methods of conveying the PIN to the Cardholder should follow the recommendations set out below:

Last amended
effective 20.8.18

(a)   the plain text PIN should 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;

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

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

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

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

Amended
effective 20.8.18

(f)   Issuers should ensure that electronic distribution of a PIN is made only to strongly authenticated Cardholders as per clause 3.3.33.3.3.

Amended
effective 20.8.18

3.4.2   *PIN advice by SMS (Issuer assigned PIN)*

In addition to the recommendations set out in clause 3.4.1, where an Issuer assigned PIN is conveyed to the Cardholder via an SMS message, the recommendations set out below should be followed: <small>Last amended effective 20.8.18</small>

(a)   Issuers should provide the Cardholder with security advice for the management of the mobile phone used for PIN advice. This should include advice about the dangers of malware and of storing account data or PINs, or both, 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; <small>Amended effective 20.8.18</small>

(b)   only pre-registered mobile phone numbers should be used for PIN advice;

(c)   if control numbers and authentication values are used then the SMS PIN advice message should 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;

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

(e)   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 should be used;

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

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

(h)   the PIN advice message should be preceded by a Cardholder initiated request;

(i)   the PIN request message should contain the Cardholder's identification and authentication values;

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

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

---

[4] See 3.1 (a)

(l)   it should 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 should be separate to any other database containing Cardholder data;

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

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

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

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

(q)   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;

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

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

3.4.3   *PIN advice by internet (Issuer assigned PIN)*

In addition to the recommendations set out in clause 3.4.1, the recommendations set out below should be followed where the PIN is communicated to the Cardholder using the internet: <small>Last amended effective 20.8.18</small>

(a)   Issuers should provide the Cardholder with security advice for the management of the end-user device (e.g., PC, Smartphone, etc.) used for PIN advice. This should 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;

(b)   the PIN should be cryptographically protected whilst in storage or transmission using strong encryption[5]. PIN transmission should be in accordance with the recommendations in clause 3.7 ;   <small>Amended effective 20.8.18</small>

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

---

[5] See 3.1(a)

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

(e)   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 should not disclose the card or account numbers;

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

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

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

(i)   if control numbers and authentication values are used then issuers should 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;

(j)   if control numbers and authentication are used then Cardholder authentication should 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;

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

(l)   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;

(m)   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;

(n)   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;

(o)   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;

(p)   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;

(q)   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;

(r)   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;

(s)   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

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

3.5   Recommendations for Customer select PIN change over open networks

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

3.5.1   *Issuer's actions*

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

Issuers should:

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

(a)   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;

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

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

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

3.5.2 *Customer select PIN change by Internet*

In addition to the recommendations in clause 3.5.1, Issuers should follow the recommendations set out below where the Cardholder is allowed to change the PIN using the internet:

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

(a) Issuers should provide the Cardholder with security advice for the management of the end-user device used for PIN selection. This should 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;

(b) the PIN should be cryptographically protected whilst in storage or transmission using strong encryption[6]. PIN transmission should be in accordance with the recommendations in clause 3.7;

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

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

(d) 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;

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

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

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

(h) internet PIN selection should 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;

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

(j) Issuers should 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;

---

[6] See 3.1(a)

(k)   if control numbers are used then Cardholder authentication should 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;

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

(m)   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

(n)   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;

(o)   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;

(p)   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;

(q)   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;

(r)   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;

(s)   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.

3.5.3   *Customer select PIN Change by mobile phone*

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

Amended effective 20.8.18

(b)   The use of Internet-based PIN change on Internet-enabled mobile phones should follow the recommendations of clause 3.5.2.

Last amended effective 20.8.18

3.6 Recommendations for Issuer approved Devices used to enter PINs

3.6.1 Device Guidelines

In accordance with clause3.3.2, 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:

(a) 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 (refer to ISO 9564.4); or

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

3.6.2 Issuer's actions

Issuers should ensure that:

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

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

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

(d) 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;

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

(f) 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;

(g) 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.

---

[7] See 3.1(a)

3.7 Recommendations for PIN transmission

3.7.1 *PIN protection*

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.

3.7.2 *Issuer's actions*

Issuers should:

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

    (i) provision of physical protection;

    (ii) encryption of the PIN value; or

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

(b) 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;

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

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

(e) where the PAN is not available;

    (i) 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;

    (ii) 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]);

(f) 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;

---

[8] See 3.1(b)

(g)   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;

<div style="text-align:right">Amended effective 29.4.16</div>

(h)   use only cryptographic algorithms specified in ISO 9564.2 to provide PIN secrecy and integrity; and

<div style="text-align:right">Amended effective 29.4.16</div>

(i)   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

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:

Australian Payments Network Limited [ABN 12 055 136 519]

(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 5.1

PART 5   CARD NOT PRESENT TRANSACTIONS

5.1   Compliance Provision

Each Issuer must comply with the obligations in Part 3 clause 3.1 of the IAC Code Set Volume 7 (Card Not Present Code).

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.

Australian Payments Network Limited [ABN 12 055 136 519]

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 at least 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 [DELETED]

Deleted effective
20.8.18

[Deleted]

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.

Australian Payments Network Limited [ABN 12 055 136 519]

(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

Australian Payments Network Limited [ABN 12 055 136 519]

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

Deleted effective 1.1.20

[Deleted]

END