Effective:
3 July 2017
Version 005

AUSTRALIAN PAYMENTS CLEARING ASSOCIATION LIMITED

ABN 12 055 136 519

A Company Limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 1
Introduction and Member Obligations

Commenced 1 July 2015

Copyright © 2015-2017 Australian Payments Clearing Association Limited
ABN 12 055 136 519

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

Code Set for ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 1 Introduction and Member Obligations

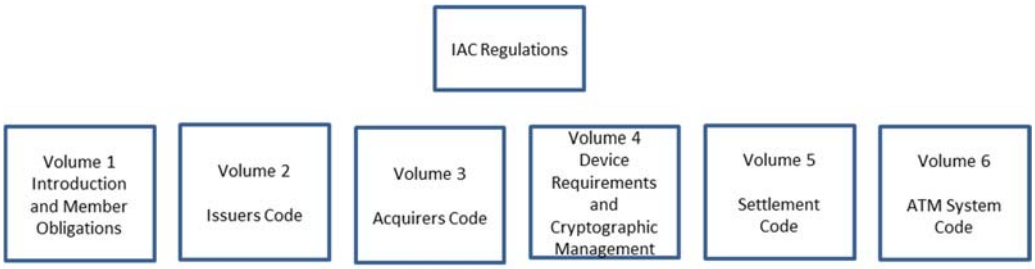
INDEX

Part 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this Code

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

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



Volume 1, this volume, provides an introduction to the IAC standards and services. In addition it identifies those obligations that IAC participation imposes on its members, referred to as Framework Participants. Additionally Volume 1 (See Annexure E) provides a set of guidelines to assist in the implementation of newly emerging Point of Sale technologies.

Amended effective 1.1.16

Volume 2 is intended for Issuers and contains those aspects of PIN 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.

Volume 3 is intended for Acquirers and contains those aspects of PIN based Transaction security that are considered mandatory for all Acquirers participating within the IAC. In addition this volume contains device management requirements applying to all acquiring members participating in the IAC.

Volume 4 identifies the security requirements applicable to Terminals, Security Control Modules and Key Injection and Loading devices that apply to all Secure Cryptographic Devices suitable for use under the IAC. Additionally it describes the approval process for those devices and the necessary requirements and process that enable an evaluation facility to seek approval for it to conduct device evaluations. This volume also specifies the minimum cryptographic algorithms, key lengths and processes that apply to all PINs and Transactions exchanged under the IAC.

Volume 5 provides the operational practices and processes involved in IAC settlement.

Volume 6 provides both the technical and operational aspects of ATM support under the IAC.

Other supplementary documents supporting the IAC include the APCA Specification for a Security Control Module Function Set and the KIF Audit Guidelines.

1.2 IAC requirements

1.2.1 *Application of these requirements*

(a) Inclusions

IAC requirements apply to all Card Transactions between Issuers and Acquirers excluding Transactions switched across international card scheme networks, regardless of the type of Card and/or account being used and/or accessed. This means that the IAC requirements apply to:

(i) all domestically acquired Transactions initiated with a debit or credit Card, including Transactions initiated with the debit functionality of a Card that also has international card scheme credit and/or debit functionality.

(b) Exclusions

(i) Other than as described above, IAC requirements do not apply directly to the electronic processing of credit card Transactions and other international scheme Transactions. These are governed by the rules and regulations published by the various card schemes.

(ii) IAC requirements do not apply to Transactions that are strictly on-us, that is Transactions wholly within the Issuer's environment.

1.2.2 *Relationship with other standards or guidelines*

This IAC Code Set cross-refers to a number of existing standards and guidelines published by bodies other than APCA that apply to Framework Participants, in their various capacities, in consumer electronic transactions and which may apply to Framework Participants either independently of or by virtue of their incorporation by reference in this IAC Code Set. The requirements of these separate schemes, standards or guidelines have not been duplicated in this IAC Code Set and Framework Participants are expected to have familiarised themselves with and adhere to their responsibilities under all such applicable requirements, as a separate matter from the specific standards and requirements which are detailed in this IAC Code Set. These existing schemes, requirements and guidelines include:

Amended effective 1.6.17

Standard or Guideline	Application	Monitor
Card Schemes	All Issuers and Acquirers party to particular schemes	Various
ePayments Code	All Framework Participants	Australian Securities and Investments Commission
Guidelines for EFT Security	All Acquirers	Australian Securities and Investments Commission
AS 2805	All Framework Participants	Standards Australia
ISO 9564	All Framework Participants	International Standards Organization
ISO 13491	All Framework Participants	International Standards Organization
RBA Card Payments Regulation	All Framework Participants	Reserve Bank

1.2.3 *Standards development*

In support of the IAC membership, and to further develop relevant IAC standards, APCA will maintain an active involvement in relevant standards development bodies, including but not limited to:

(a) Standards Australia – relevant working groups and committees;

(b) International Standards Organization – relevant working groups and committees;

(c) PCI Security Standards Council;

(d) EMV Co – relevant working groups.

1.2.4 *Inconsistencies*

(a) If a provision of the Regulations or this IAC Code Set is inconsistent with a provision of the Constitution, the provision of the Constitution prevails.

(b) If a provision of this IAC Code Set is inconsistent with a provision of the Regulations, the provision of the Regulations prevails.

1.2.5 *Governing Law*

This IAC Code Set is to be interpreted in accordance with the same laws which govern the interpretation of the Constitution.

1.3 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.

1.4 Definitions

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

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

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

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

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

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

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

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

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

"**Approved Card Payment System**" has the meaning given in the IAC Regulations.

"**Approved Device**" means a Secure Cryptographic Device that has been evaluated in accordance with clause 3.1 of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) which has been approved for use within IAC. Amended effective 1.1.16

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

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

"**ATM**" or "**ATM Terminal**" means an approved electronic device capable of automatically dispensing Cash in response to a Cash withdrawal Transaction initiated by a Cardholder. Other Transactions (initiated by a Card) such as funds transfers, deposits and balance enquiries may also be supported. The device must accept either magnetic stripe Cards or smart (chip) Cards where Transactions are initiated by the Cardholder keying in a Personal Identification Number (PIN). Limited service devices (known as "Cash dispensers") that only allow for Cash withdrawal are included. Amended effective 1.1.16

"**ATM Access Regime**" means the access regime imposed by the Reserve Bank of Australia under section 12 of the *Payment Systems (Regulation) Act 1998* by regulatory instrument dated 23 February 2009. Inserted effective 1.1.16

"**ATM Affiliate**" means an Affiliate which has subscribed to this Code. Inserted effective 1.1.16

"**ATM Code Committee**" means the committee established by the IAF pursuant to Part 11 of the IAC Regulations. Inserted effective 1.1.16

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

"**ATM Framework Participant**" means a Constitutional Corporation which pursuant to the IAC Regulations, is a Framework Participant in the IAC, and is a subscriber to this Code pursuant to Part 2, clause 2.2 of the IAC Code Set Volume 6 (ATM System Code) and includes, for the avoidance of doubt, each: Inserted effective 1.1.16

(a) IA Participant;

(b) ATM Operator Member; and

(c) ATM Affiliate.

"**ATM Interchange**" means the exchange of payment instructions for value between Acquirers (whether for itself or on behalf of a third party) and Issuers, via an Interchange Link, as a result of the use of an Issuer's Card by a Cardholder to generate an ATM Transaction. Interchange arrangements may, but need not, be reciprocal. Inserted effective 1.1.16

"**ATM Law**" means a law of the Commonwealth or of any State or Territory in relation to the operation of ATM Terminals. Inserted effective 1.1.16

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

"**ATM Operator Member**" means an Operator Member which has subscribed to this Code. Inserted effective 1.1.16

"**ATM System**" means the network of direct and indirect Interchange Lines, Interchange Links, associated hardware, software and operational procedures that facilitate the transmission, authorisation and reconciliation of ATM Transactions between IA Participants in Australia. Amended effective 1.1.16

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

"**ATM Transaction Listing**" means a listing which complies with the requirements of Part 4, clause 11 of the IAC Code Set Volume 6 (ATM System Code). Amended effective 1.1.16

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

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

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

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

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

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

"**Cardholder Data**" means any information that is stored on, or which appears on, a Card, and includes but it not necessarily limited to: Inserted effective 1.1.16

(a) Primary Account Number;

(b) Cardholder Name;

(c) Service Framework; and

(d) Expiration Date.

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

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

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

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

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

"**Certification Undertakings**" means all undertakings and representations given to the Company for the purposes of obtaining Certification. Inserted effective 1.1.16

"**Clearing/Settlement Agent**" means a Direct Clearer/Settler that clears and settles on behalf of Issuers and/or Acquirers which are not Direct Clearer/Settlers. Inserted effective 1.1.16

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

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

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

"**Company**" means APCA.

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

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

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

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

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

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

"**Counterfeit ATM Transaction Chargeback Date**" [Deleted] Deleted effective 3.7.17

"**Counterfeit ATM Transaction Claim**" means a claim by an Issuer under the indemnity in clause 4.5(c) (Liability Shift for Counterfeit ATM Transaction), made in the manner set out in clause 4.6 (Liability Shift Claim Process) of the IAC Code Set Volume 6 (ATM System Code). Amended effective 3.7.17

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

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

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

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

"**Direct Charge**" means a direct charge applied by an IA Participant under the Direct Charging Rules in Annexure F of IAC Code Set Volume 6 (ATM System Code). Inserted effective 1.1.16

"**Direct Clearing/Settlement Arrangements**" means an arrangement between two indirectly connected IA Participants for the purposes of clearing and settlement with each other as Direct Clearer/Settlers. Inserted effective 1.1.16

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

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

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

"**Direct Settler**" or "**Direct Clearer/Settler**" means: Inserted effective 1.1.16

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

(i) clears Items directly; and

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

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

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

(i) clears Items directly; and

(ii) settles directly, using its own ESA,

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

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

"**Disputed Transaction**" means an ATM Transaction: Amended effective 1.1.16

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

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

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

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

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

"**Doubtful ATM Transactions**" means those ATM Transactions which appear to have been successfully completed, although the ATM Transaction may not be recorded against the relevant Cardholder account. Last amended effective 21.11.16

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

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

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

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

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

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

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

"**EMV Phase 1**" means the transition arrangements through which a Transaction is created from the use of an EMV compliant Australian IC Card prior to the migration of the ATM system to full EMV functionality. Amended effective 3.7.17

"**EMV Standards**" means:

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

(b) in relation to ATM Terminals, means the standards set out in the EMV@ATM Terminal Standards.

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

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

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

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

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

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

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

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

"**Fallback Transaction**" means an ATM Transaction initiated using a chip Card, which is processed and authorized by the Issuer using magnetic stripe data.

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

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

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

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

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

"**Framework Participant**" means a Constitutional Corporation:

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

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

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

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

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

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

(a) an Issuer; or

(b) an Acquirer; or

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

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

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

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

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

"**IAC Settlement Rules**" means the set of rules and requirements for the settlement of obligations arising as a result of exchange of Items set out in the IAC Code Volume 5 (Settlement Code). Inserted effective 1.1.16

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

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

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

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

"**Interchange Activity**" means:

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

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

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

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

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

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

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

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

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

"**Interchange Link PIN Encryption**" means encryption of the PIN in accordance with ISO 9564.1 and IAC Code Set Volume 4 Clause 2.7(d)(i). Amended effective 21.11.16

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

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

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

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

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

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

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

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

"**Items**" means Credit Items or Debit Items.

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

"**Key Loading Device/Key Injection Device**" and "**KLD/KID**" means a hardware device and its associated software that is used to inject keys into a Terminal. Amended effective 29.4.16

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

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

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

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

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

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

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

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

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

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

Inserted effective 1.6.17

"**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).

"**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.

Inserted effective 1.1.16

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

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

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

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

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

Amended effective 29.4.16

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

"**PCI Points**" means the attack potential calculated in accordance with Appendix B of the Payments Card Industry (PCI) document "PCI PIN Transaction Security Point of Interaction Modular Derived Test Requirements", version 3.0, 2011.

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

Amended effective 21.11.16

"**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.

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

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

Inserted effective 1.1.16

"**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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"**Settlement Items**" means, Items which are either:

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

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

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

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

"**Standard Interchange Specification**" means the technical specification set out in Annexure A of IAC Code Set Volume 6 (ATM System Code). Inserted effective 1.1.16

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

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

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

"**Terminal**" means an electronic device containing a PED which can be used to complete a Transaction.

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

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

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

(a) interchange;

(b) PIN processing;

(c) transaction processing;

(d) key management; or

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

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

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

"**Transaction**" means any Card Payment or other transaction initiated by a Cardholder which allows for the accessing of available funds held in an account, or a credit facility linked to an account, or account information.

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

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

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

Next page is 2.1

Part 2 FRAMEWORK PARTICIPANT OBLIGATIONS

2.1 Adherence to standards

Subject to the limitations set out in Part 1.2.2, the following requirements apply.

2.1.1 *Issuers*

Subject to clause 4.1 of the Regulations, Issuers must ensure that they and their Third Party Providers ensure:

(a) PIN security complies with the requirements specified in IAC Code Set Volume 2 (Issuers Code);

(b) Any SCMs used in Interchange comply with both the APCA SCM Specification and IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and are approved for use by the Company; and

Modified effective 1.7.15

(c) Settlement procedures comply with the requirements and processes given in IAC Code Set Volume 5 (Settlement Code).

2.1.2 *Acquirers*

Subject to clause 4.1 of the Regulations, Acquirers must ensure that they and their Third Party Providers ensure:

(a) PIN security complies with all relevant requirements given in the IAC Code Set Volume 3 (Acquirers Code);

(b) ATM requirements and procedures comply with all aspects of IAC Code Set Volume 6 (ATM System Code);

(c) any SCMs used in Interchange comply with both the APCA SCM Specification and IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and are approved for use by the Company;

Modified effective 1.7.15

(d) any SCDs used in IAC Interchange comply with the security requirements specified in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and are approved for use by the Company;

(e) settlement procedures comply with the requirements and processes given in IAC Code Set Volume 5 (Settlement Code);

(f) all Key Injection Services and Devices comply with the relevant requirements specified in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management);

(g) all parties to the Interchange, including merchants and any intermediate network entities maintain procedures and practices for preventing the unauthorised disclosure of Cardholder Data and ensure that unencrypted authentication is not stored outside of an SCD (see IAC Code Set Volume 3 (Acquirers Code)); and

(h) that they are aware of the Reserve Bank notification requirements to merchants regarding merchant pricing requirements. Annexure F (Notice of Standard – Merchant Pricing for Credit, Debit and Prepaid Card Transactions) is an optional guide prepared by APCA which may be used by Acquirers and their Third Party Providers to assist them to comply with their notification requirements. Inserted effective 1.6.17

2.2 Third Party Providers

Amended effective 1.1.15

(a) A Framework Participant may contractually engage one or more Third Party Providers to provide outsourced services and functions, which may include services procured to satisfy the Framework Participant's obligation to perform specific functions and requirements necessary to meet the obligations of the IAC Code Set.

(b) It is the responsibility of the Framework Participant to verify the capacity of its Third Party Provider to provide the outsourced services and functions.

(c) It is the responsibility of the Framework Participant to manage, direct and control the provision of outsourced services and functions by its Third Party Providers, and to ensure such Third Party Providers and any sub-contractor engaged by the Third Party Provider are contractually obliged to comply with all applicable IAC standards and requirements.

2.3 Compromised Terminals

Clauses 2.3.1 to 2.3.2 are Confidential

2.4 Change Management

(a) Any proposal to modify or upgrade an existing Interchange that also involves changes by the other party to the Interchange, must be advised by the applicant to the Framework Participant affected no less than 180 days (unless otherwise bilaterally agreed) prior to the date upon which the proposal is to be implemented ("**Implementation Date**").

(b) Each Framework Participant must use reasonable endeavours to make such changes to its own Interchanges by the Implementation Date, or a date otherwise bilaterally agreed, as may be necessary to give effect to a proposal notified to it under this clause.

2.5 Provision of statistics

2.5.1 *Terminal statistics*

(a) Acquirers must report to the Company the number of ATM and EFTPOS terminals they deploy on a state by state basis for the periods ending on December, March, June and September. The report must separately identify those terminals which the Acquirer directly owns and any other terminals for which it provides acquiring services (e.g., "white label" terminals owned by a third party).

(b) Consolidated figures will be provided to all IA Participants and also made available from the IAC ATM and EFTPOS Statistics Database facility found on APCA's Extranet.

(https://extranet.apca.com.au/extranet/CS3ATMEFTPOSStats.NSF/ADate?OpenView)

2.5.2 *Card fraud data*

(a) Issuers must report card fraud data to the Company on a monthly basis. Information in the report must comply with the requirements set out by the Company and made available from time to time on APCA's extranet.

(https://extranet.apca.com.au/extranet/fraudstats.nsf/AllDebitCardFraudByDate?OpenView&Start=1&Count=100&Expand=1))

(b) Consolidated figures will be provided to all IA Participants and also made available from the IAC Card Fraud Database facility found on APCA's Extranet.

(https://extranet.apca.com.au/extranet/CS3StatDCFS.NSF/ADate?OpenView&Login)

2.6 Notification of a Disruptive Event

(a) A IA Participant that experiences a Disruptive Event must notify the Company and all IA Participants that will or are likely to be affected by the Disruptive Event as soon as possible. Notification of a Disruptive Event must be given to the operational contacts listed on APCA's Extranet and subsequently by a IAC Operational Broadcast (see clause 2.7).

(b) Upon notice of a Disruptive Event, the Chief Executive Officer may, if he considers it appropriate to do so, invoke the Member Incident Plan which is available on the Company's Extranet, either by written notice to, or verbally notifying the committee of management. The Member Incident Plan provides a framework for committee of management communication and consultation during applicable contingency events. If the Chief Executive Officer invokes the Member Incident Plan, the committee of management must comply with its requirements.

2.7 IAC Operational Broadcast

(a) IA Participants may provide operational advice to other IA Participants by issuing an IAC Operational Broadcast (set out in Annexure D).

(b) The IAC Operational Broadcast form may be used to notify other IA Participants about:

(i) unscheduled network outages;

(ii) scheduled network outages;

(iii) to facilitate the exchange of general operational information relevant to network operations;

(iv) Disruptive Events; or

(v) any technical inability to comply with a notification given by the Secretary under clause 2.8 (BIN and AIN Change Management).

2.7.1 *How to Send an IAC Operational Broadcast*

(a) The IAC Operational Broadcast form is an online form which can be accessed, completed and sent by IA Participants using APCA's extranet that is available and processed 24/7.

(b) An IAC Operational Broadcast about a Disruptive Event must include the following information:

(i) the time when the Disruptive Event commenced or is expected to commence;

(ii) the time when normal processing is expected to resume or resumed; and

(iii) the current status of the Disruptive Event.

2.8 BIN and AIN Change Management

This clause 2.8 applies to those BINs and AINs involved in domestic interchange.

2.8.1 *BIN and AIN Change Database*

(a) Other than in the context of a new direct clearing and settlement arrangement, the introduction of a new BIN or AIN, or deletion of or change in the routing of an existing BIN or AIN must occur on an Institutional Identifier Change Date.

(b) An IA Participant wishing to introduce a new BIN or AIN, or change the routing of an existing BIN or AIN, must give the Secretary no less than 10 weeks' notice in advance of the relevant Institutional Identifier Change Date on which such change is to occur and must pay to the Company at the time of giving the notice $6,700 (indexed annually in accordance with Regulation 10.5 and to be rounded to the nearest $100 ($50 being rounded up)). No further fee applies where there is more than one new identifier and/or routing change notified to take effect on the same Institutional Identifier Change Date. Amended effective 1.1.16

(c) An IA Participant wishing to delete an existing BIN or AIN must give the Secretary no less than 10 weeks' notice in advance of the relevant Institutional Identifier Change Date on which such change is to occur.

(d) The Secretary must promptly notify all IA Participants of the new BIN or AIN or the deletion of or change in the routing of an existing BIN or AIN and the Institutional Identifier Change Date on which such change is to occur.

(e) IA Participants must recognise the new BIN or AIN or deletion of or change in the routing of an existing BIN or AIN on and from the relevant Institutional Identifier Change Date notified by the Secretary in accordance with this clause 2.8.1.

Note: "recognise" for the purposes of this clause 2.8.1(e) means making such host system and Terminal changes as are reasonably necessary to ensure that Cards issued on the changed BIN and / or AIN are accepted at Terminals and that Transactions are processed and authorized accordingly.

2.8.2 *Production of test cards*

Issuers that give notice of the introduction of a new BIN or a change to the routing of an existing BIN pursuant to clause 2.8 must, on request by an affected IA Participant, ensure production of any necessary test Cards in sufficient time to allow testing to occur before the applicable Institutional Identifier Change Date.

2.9 Capacity Planning

The IAC committee of management will undertake the facilitation of regular meetings of those IA Participants engaged in Interchange to:

(a) consider the capacity and performance requirements for periods of peak demand;

(b) ensure that IA Participants engaged in Interchange have sufficient capacity and performance to maintain services during peak periods of demand;

(c) share information (such as changes in switch arrangements or major product launches) relevant to capacity and performance to maintain the efficiency of the Australian card payments network at all times;

(d) provide assistance in developing action plans for any IA Participants engaged in Interchange that consider they may not have the required capacity and performance during a period of peak demand;

(e) monitor the action plans for IA Participants engaged in Interchange that may not have the required capacity and performance during a period of peak demand;

(f) report and discuss any issues that it considers may affect the integrity, security or efficiency of interchange, from a capacity requirement and performance perspective, to the committee of management for appropriate action; and

(g) provide recommendations, as appropriate, on issues that have been discussed and agreed by a majority for consideration by the IAC committee of management.

Next page is 3.1

Part 3 CERTIFICATION

3.1 Introduction

This Part 3 sets out the certification requirements to be met by applicants, and the annual compliance requirements for all IA Participants.

By completing the relevant checklists, an applicant or IA Participant confirms, for the benefit of all IA Participants and the Company, that when it operates in the IAC with other IA Participants it meets the applicable requirements in force at that time, including that:

(a) it conforms with IAC Code Set Volume 3 (Acquirers Code);

(b) it conforms with IAC Code Set Volume 2 (Issuers Code);

(c) all PEDs, SCMs and Key Loading and Transfer devices it uses have been approved by the Company and are listed on the Approved Devices List; (see http://apca.com.au/payment-systems/cards-accepting-devices/device-security-evaluations/IAC-approved-devices).

(d) the SCMs it uses are compliant to the APCA SCM Specification;

(e) its settlement procedures conform with IAC Code Set Volume 5 (Settlement Code);

(f) it conforms with IAC Code Set Volume 6 (ATM System Code); and

(g) any services provided on its behalf by Third Party Providers are provided in conformance with the relevant standards and requirements specified in this Code. Amended effective 1.1.15

3.2 Annual Security Audits

The Annual Security Audits (Annexure A of this Volume 1) is designed to ensure that uniform security audit procedures are applied among all Framework Participants. To be effective, all entities involved in either the processing of Interchange PINs from entry at the PED up to and including its delivery to the Issuer's authorisation processor, or involved in the management and security of PINs must adhere to an agreed set of procedures and adopt a common audit process to ensure adherence to those security procedures.

3.2.1 *Submission of Annual Security Audit*

(a) All IA Participants must complete an Annual Security Audit (see Annexure A) once every calendar year. IA Participants must give the Company prior written notice of the date by which they will complete their Annual Security Audit. It must be signed by the IA Participant and countersigned by either an internal or external auditor.

(b) Acquirers who have completed a Visa PIN Security Requirements Self Audit (appendix C of the PCI PIN Security Requirements manual, version 2.0 dated January 2008 or later) within the immediately preceding 6 months may meet the requirements in this clause 3.2.1 by completing Annexure A.1 and submitting a duly signed copy of the Visa checklist should accompany this submission.

3.2.2 *Third Party Providers*

Amended effective 1.1.15

(a) Where services and functions are provided by a Third Party Provider, its compliance with IAC standards and requirements must be demonstrated by the IA Participant by either submission of:

(i) a separate Annual Security Audit checklist for the Third Party Provider; or

(ii) by inclusion of the Third Party Provider within the IA Participant's own Annual Security Audit checklist.

(b) IA Participants' compliance with the obligation to manage service provision by Third Party Providers as set out in this clause 3.2.2 will be assessed as part of the annual security audit.

3.2.3 *Auditor Signoff*

(a) Auditors co-signing Annual Security Audit must be engaged to perform an independent review of the compliance checklists completed by the IA Participant, and to form an opinion on their completeness and accuracy.

(b) The following is a suggested audit process that could be used by an auditor:

(i) Obtain the completed relevant checklist from the IA Participant.

(ii) Select a representative sample of questions from the checklist, including:

(A) all questions which indicate non-compliance with the IAC Code Set; and

(B) a sample of questions which indicate compliance with the IAC Code Set.

(iii) Perform a walk-through of each of the selected questions with the relevant staff, focusing on how they have assured themselves that the responses to the checklist are complete and accurate.

(iv) Where non-compliance is noted on a checklist, ensure that the IA Participant have an adequate and timely action plan in place, including:

(A) remedial actions which will ensure future compliance to the IAC Code Set;

(B) realistic and appropriate resolution time frames; and

(C) accountability is allocated to the relevant staff within the IA Participant.

(v) Raise all concerns with the IA Participant and achieve satisfactory resolution/agreement.

(vi) The auditor should continually be asking the relevant staff as to:

(A) how they ensure compliance with the IAC Code Set; and

(B) to provide evidence which demonstrates that their compliance control/monitoring procedures are operating effectively.

3.3 Exemption Requests

(a) All IA Participants must at all times comply with the requirements specified in the IAC Code Set unless specifically exempted by the Company.

(b) An IA Participant requiring an exemption from certain requirements must make an application to the Company. The application must include the following information:

(i) the name of the IA Participant requiring the exemption;

(ii) date of the request;

(iii) date the out-of-compliance situation occurred;

(iv) a description of the risk and a risk rating;

(v) the section(s) of the IAC Code Set with which the IA Participant is not in compliance;

(vi) description of the requirement with which the IA Participant is not in compliance;

(vii) a statement on the reason for non-compliance;

(viii) a full description of any compensating controls that are offered as justification for the authorisation of the request; and

(ix) exact details of the IA Participant's action plan to comply with the requirements and an indication as to the likely date of achieving compliance.

(c) An exemption request form is provided in Annexure C.

3.3.1 *Exemption Process*

The Company will review the exemption request and accompanying documentation and determine if the proposed remedial action/compensating controls with respect to areas of non-compliance are satisfactory to the Company, having regard to the integrity and efficiency of IAC. The Company will advise the IA Participant of the acceptance or rejection of the exemption request.

3.3.2 *Exemption Duration*

Exemptions will only be granted for a defined period of time. The Company may grant duration different to the one requested by the IA Participant. All exemptions granted for non-compliance, regardless of when they expire, must be reviewed and renewed annually.

3.3.3 *Introduction of New or Modified Devices or New Processes*

In cases where a significant change will cause the IA Participant to be out of compliance with the IAC requirements, the IA Participant may not proceed unless appropriate exemptions have been duly granted. Examples include:

(a) deployment of any new SCD (not currently on the Approved Devices List);

(b) continued deployment of an SCD which has reached its approval sunset date; or

(c) implementing changes to PIN or cryptographic key handling or management processing.

3.4 Certification of Prospective IA Participant

(a) Each applicant must arrange for Certification as part of their membership application.

(b) Certification checklists must be used for Certification. An applicant seeking Certification must complete the relevant New IA Participant Checklist (see Annexure B) and the relevant Annual Security Audit (see Annexure A). Any further evidence of compliance which is reasonably requested by the Secretary or the committee of management must be promptly produced to the Secretary following the request.

(c) All applicants must ensure that Third Party Providers meet the obligations set out in clause 2.2 and clause 3.2.2 of this Volume. Inserted effective 1.1.15

3.4.1 *Guidance for External Auditors*

(a) When Certification is sought by an applicant who does not have, or does not wish to use, an internal auditor, the Certification checklist must be accompanied by a report of an agreed upon procedures engagement (refer Accounting Standard AUS 904) from an external auditor.

(b) The external auditor engaged by an applicant must be acceptable to the Company. The Company maintains a set of Guidance Procedures for applicants wishing to use an external auditor, which contain a proposed set of acceptable audit procedures. Once an acceptable external auditor has been selected by the applicant the external auditor may obtain the Guidance Procedures from the Company.

3.4.2 *Review of Certification documentation*

The Company will review the Certification checklists referred to in clause 3.4 above and accompanying documentation and provide a report of its review to the applicant. Details of the application will be provided to the committee of management for its consideration under Regulation 4.3 as to whether:

(a) all requirements appear to have been met, or

(b) any proposed remedial action/compensating controls with respect to areas of non-compliance are satisfactory to the Company having regard to the desirability to maintain the integrity and efficiency of IAC.

Next page is A.1

ANNEXURE A ANNUAL SECURITY AUDITS

Note: Annexure A.1 Acquirer Annual Security Audit (Part 1) must be completed annually by all Acquirer Framework Participants in combination with either Annexure A.2 Acquirer Annual Security Audit (Part 2) or a duly signed copy of a Visa PIN Security Requirements Self Audit

Note: Annexure A.3 Issuer Annual Security Audit must be completed annually by all Issuer Framework Participants.

A.1 ACQUIRER ANNUAL SECURITY AUDIT (PART 1)

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805.

The following documents are referenced in this checklist;

ISO 9564.1-2011	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems	Amended effective 21.11.16
AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles	
AS 2805.14.2-2009	Electronic funds transfer – Requirements for interfaces Part 14.2: Secure Cryptographic Devices (retail) – Security compliance checklists for devices used in magnetic stripe systems	

A.1.1 General Security Controls

(a) Please provide the details for all ATM and POS devices that you currently have deployed. Please use a separate sheet if necessary. Inserted effective 1.1.16

ATM	POS	Manufacturer	Model No.	Approx Quantity
☐	☐			
☐	☐			
☐	☐			
☐	☐			
☐	☐			
☐	☐			

(b) Please provide the details for all SCM devices that you currently have deployed. Please use a separate sheet if necessary. Inserted effective 1.1.16

Manufacturer	Model No.	Quantity

(c) Third Party Providers

Please provide details of all Third Party Providers used in providing acquiring services. Please use a separate sheet if necessary.

Third Party Providers	Type of service provided

(d) All parties to the Interchange, including merchants, Acquirers, Third Party Providers and any intermediate network entities maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data, which includes but is not necessarily limited to the Primary Account Number, Cardholder Name, Service Code, Expiration Date,

Reference IAC Code Set Volume 3, clause 2.5.

Yes	No	N/A

If N/A response: Reason

(e) Sensitive authentication data, including but not limited to, Full magnetic stripe (or equivalent), CVC2/CVV2/CID, PIN/PIN Block is not stored, outside of an SCD, subsequent to Authorisation.

Reference IAC Code Set Volume 3, clause 2.6.

Yes	No	N/A

If N/A response: Reason

(f) Message Authentication applies to all Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and MAC cryptographic functions are performed within a Tamper responsive SCM.

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(g) Message Authentication applies to all Terminal to Acquirer Links for all financial and key management messages

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(h) Interchange Lines are be subject to whole-of-message encryption in accordance with AS 2805.5.4 (IAC Code Set Volume 3, clause 2.4.4)

Yes	No	N/A

If N/A response: Reason

(i) Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2

Yes	No	N/A

If N/A response: Reason

(j) Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable)

Yes	No	N/A

If N/A response: Reason

(k) Terminal key management practices comply with the requirements of IAC Code Set Volume 4, clause 4.8.2

Yes	No	N/A

If N/A response: Reason

(l) Host systems which support Terminals using the TCP/IP protocol for communications meet the requirements of IAC Code Set Volume 3, clause 3.5

Yes	No	N/A

If N/A response: Reason

(m) Privacy of communication complies with AS 2805.9 for all Terminal to Acquirer links, or any other privacy of communication standard approved by the committee of management (EFTPOS terminals only) IAC Code Set Volume 3, clause 2.4.5

Yes	No	N/A

If N/A response: Reason

(n) Documented procedures exist, and are followed to ensure all PINs are encrypted using DEA 3 when transmitted outside a Secure Cryptographic Device. PINs are not stored in any form. If a transaction is logged, the encrypted PIN block is masked or deleted from the record before it is logged.

Amended effective 29.4.16

Reference AS 2805.3.1 clauses 5.2 and 12.2.

Yes	No	N/A

If N/A response: Reason

(o) Each type of SCD used in Interchange and those devices providing a Remote Management Solution for Security Control Modules have been evaluated by a Company accredited Evaluation Facility using the method in and against the criteria in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management), and have been approved for use by the Company. Last amended effective 21.11.16

An SCD includes but is not limited to an ATM, PED, SCM or Key Loading and Transfer Device.

Reference ISO 9564.1, clause 5.1; AS 2805.14.2.

Yes	No	N/A

If N/A response: Reason

(p) Clear text PINs and Clear-text keys exist only in an SCD designed for use in its operational environment.

Yes	No	N/A

If N/A response: Reason

A.1.2 Device Management

(a) Documented procedures exist, and are followed, to determine that the SCD is managed in accordance with the privacy shielding requirements in clause 3.2.3 of IAC Code Set Volume 3 (Acquirers Code).

Yes	No	N/A

If N/A response: Reason

(b) For terminals running multiple applications, documented, auditable, key management procedures exist and are followed for the secure management of any key used in the authentication processes associated with PED software authentication. Inserted effective 1.1.15

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of clause 3.3.4 of IAC Code Set Volume 3 (Acquirers Code).

Yes	No	N/A

If N/A response: Reason

(d) From 1 January 2013, all symmetric encryption functionality weaker than DES-3 has been disabled within every deployed SCM.

Yes	No	N/A

If N/A response: Reason

(e) Acquirers shall maintain a register of all authorised non-payment applications per device. Inserted effective 1.1.15

Yes	No	N/A

If N/A response: Reason

(f) Operating procedures and the design of devices utilized require that the Cardholder can reasonably prevent others from observing the entered PIN. Amended effective 21.11.16

Reference AS 2805.14.2, clause B.2.1.B6.

Yes	No	N/A

If N/A response: Reason

A.1.3 General Key Management

Inserted effective 1.1.16

(a) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then:

(i) The key loading device has been evaluated and meets the applicable security requirements (see clause A.2.2);

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g. in a safe) such that no unauthorised person may have access to it; and

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Yes	No	N/A

If N/A response: Reason

(b) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a form such as to preclude it being intentionally used again as active keying material.

Inserted effective 1.1.16

Yes	No	N/A

If N/A response: Reason

A.1.4 Supplementary Questions for Acquirers who are submitting Visa Audits

Note: The following requirements are only to be completed by Acquirers submitting a duly signed copy of a Visa PIN Security Requirements Self Audit to accompany this A.1 Acquirer Annual Security Audit (Part 1) submission (as described in clause 3.2.1).

(a) Compliance with the requirements of the Visa PIN Security Requirements Self Audit has been confirmed.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed for each of the individual requirements in the Visa PIN security Requirement Self Audit.

Yes	No	N/A

If N/A response: Reason

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 1) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.2 ACQUIRER ANNUAL SECURITY AUDIT (PART 2)

Annexure A.2 Acquirer Annual Security Audit (Part 2) must be completed unless submitting a duly signed copy of a Visa PIN Security Requirements Self Audit.

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805 and ISO 9564. Amended effective 21.11.16

A.2.1 General Security Controls

Amended effective 21.11.16

(a) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0 and format 3 PIN blocks specified in ISO 9564.1 meet this requirement.)

Reference ISO 9564.1, clause 9.3 and 9.4.

Yes	No	N/A

If N/A response: Reason

(b) No procedure requires or permits the Cardholder to disclose the PIN (verbally or in writing). Amended effective 21.11.16

Reference ISO 9564.1, clause 6.1.3.

Yes	No	N/A

If N/A response: Reason

A.2.2 Device Management

(a) Any SCD capable of encrypting a key and producing a cryptogram of that key is protected against unauthorised use to encrypt known keys or known key components. This protection takes the form of either or both of the following:

(i) Dual Access controls are required to enable the key encrypting functions; and/or

(ii) Physical protection of the equipment (e.g., locked access to it) under dual control.

Reference AS 2805.14.2, clauses E12 and E13.

Yes	No	N/A

If N/A response: Reason

.....

.....

(b) Documented procedures exist, and are followed, to determine that an SCD has not been subject to unauthorised modification or substitution prior to loading cryptographic keys. This assurance takes the form of one or more of the following procedures:

(i) Physical inspection and/or testing of the equipment immediately prior to key loading; and/or

(ii) Physical protection of the equipment.

Yes	No	N/A

If N/A response: Reason

.....

.....

(c) Documented procedures exist, and are followed, to ensure that the SCD is physically protected (e.g., locked access) to protect against the possibility that the SCD may be stolen, modified in an unauthorised way, and then returned to storage without detection.

Yes	No	N/A

If N/A response: Reason

.....

.....

(d) Documented procedures exist to ensure that keys are not installed in any SCD where suspicious alteration of an SCD has been detected until the SCD has been inspected and a reasonable degree of assurance has been reached that the SCD has not been subject to any unauthorised physical or logical modifications.

Yes	No	N/A

If N/A response: Reason

.....

.....

(e) Documented, auditable, key management procedures exist and are followed for the secure management of any Acquirer controlled key used in the authentication processes associated with PED software authentication. Inserted effective 1.1.16

Yes	No	N/A

If N/A response: Reason

(f) If the SCD can translate a PIN from one PIN block format to another or if the SCD verifies PINS, then procedures exist, and are followed, to prevent or detect, repeated unauthorised calls resulting in the exhaustive determination of PINS. Inserted effective 1.1.16

Yes	No	N/A

If N/A response: Reason

A.2.3 General Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms:

(i) In a SCD;

(ii) Encrypted under a DEA 2 or DEA 3 key; or

(iii) Managed as two or more full length components using the principles of dual control and split knowledge.

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component reasonably protects that component such that no person (not similarly entrusted with that component) can observe or otherwise obtain that component.

Yes	No	N/A

If N/A response: Reason

(c) Documented procedures exist and are followed to ensure keys and key components are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist to ensure each of the following:

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) Key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components are only combined within a SCD.

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions:

(i) XOR; and/or

(ii) Encryption via DEA.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners: Amended effective 21.11.16

(i) Key components are transported in separate tamper-evident packaging; and/or

(ii) Key components are transported in a device meeting the requirements of a Physically Secure Device.

Reference ISO 9564.1 and AS 2805.14.1.

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure a cleartext key component is:

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In a physically secure SCD.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to protect the transfer of a key or key component into SCDs so as to prevent the disclosure of the key or key components. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed, to prohibit, except by chance, the entry or use of the same key in more than one PIN entry device.

Yes	No	N/A

If N/A response: Reason

(m) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared, except by chance, between any other communicating parties.

Yes	No	N/A

If N/A response: Reason

(n) Procedures exist and are followed to ensure a key or key component that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.

Yes	No	N/A

If N/A response: Reason

(o) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to monitor cryptographic synchronisation errors and to investigate multiple synchronisation errors to ensure the SCD is not being misused to determine keys or PINs.

Yes	No	N/A

If N/A response: Reason

(q) Documented procedures exist and are followed to ensure if two or more of a key's components are stored within the same security container (which is under dual control), then the components are secured in tamper evident packaging to preclude one component holder from gaining access to the other component.

Yes	No	N/A

If N/A response: Reason

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.

Yes	No	N/A

If N/A response: Reason

(s) If personal computers are used to load encryption keys into a PIN entry device, procedures exist and are followed to ensure, at a minimum the following controls:

(i) The software loads the encryption key without recording the value in non-volatile storage;

(ii) Hardware used for the key loading function is maintained under dual control;

(iii) Hardware use is monitored and logs of key loading activity are maintained;

(iv) Cable attachments and hardware are examined before each use to ensure that the equipment is free from tampering;

(v) That the computer is started from power off position for each site's key loading activity; and

(vi) An SCD is used in conjunction with the personal computer to complete all cryptographic processing and for the storage of all encryption keys.

Yes	No	N/A

If N/A response: Reason

.....

.....

(t) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is opened to record date, time, person(s) involved and the purpose of the access.

Yes	No	N/A

If N/A response: Reason

.....

.....

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Annual Security Audit (Part 2) the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor	Signature of Auditor
Date	

A.3 ISSUER ANNUAL SECURITY AUDIT

This checklist presents mandatory requirements relating to general procedures and controls associated with the management of PINs and the associated cryptographic practices. The mandatory requirements are based on the requirements of AS 2805.

The following documents are referenced in this checklist;

ISO 9564.1-2011	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems.	Amended effective 21.11.16
AS 2805.6.1-2002/Amdt 3/2007	Electronic funds transfer – Requirements for interfaces Part 6.1: Key management – Principles	
AS 2805.14.1-2011	Electronic funds transfer – Requirements for interfaces – Secure cryptographic devices (retail) – Concepts, requirements and evaluation methods	Inserted effective 21.11.16
AS 2805.14.2-2009	Electronic funds transfer – Requirements for interfaces Part 14.2: Secure Cryptographic Devices (retail) – Security compliance checklists for devices used in financial transactions	Amended effective 21.11.16

A.3.1 General Security Controls

(a) Please provide the details for all SCM devices that you currently have deployed. Please use a separate sheet if necessary.

Manufacturer	Model No.	Quantity.

(b) Third Party Providers

Please provide details of all Third Party Providers associated with the management of PINs and the associated cryptographic practices used in providing issuing services. Please use a separate sheet if necessary.

Third Party Providers	Type of service provided

(c) Any clear-text PIN block format combined with a PIN encryption process has the characteristics that, for different accounts, encryption of the same PIN value under a given encryption key does not predictably produce the same encrypted results. (Note the format 0 and format 3 PIN blocks specified in ISO 9564.1 meet this requirement.) Amended effective 21.11.16

Reference ISO 9564.1, clauses 9.3.1 and 9.3.5.

Yes	No	N/A

If N/A response: Reason

(d) Documented procedures exist, and are followed to ensure all PINs are encrypted using DEA 3 when transmitted outside a Secure Cryptographic Device. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged. Amended effective 21.11.16

Reference ISO 9564.1 clause 4.2.

Yes	No	N/A

If N/A response: Reason

(e) No procedure requires or permits the Cardholder to disclose the PIN verbally or in writing. Amended effective 21.11.16

Reference ISO 9564.1 clause 4.2(h).

Yes	No	N/A

If N/A response: Reason

(f) All parties to the Interchange, including Third Party Providers and any intermediate network entities maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data, which includes but is not necessarily limited to the Primary Account Number, Cardholder Name, Service Code, Expiration Date,

Yes	No	N/A

If N/A response: Reason

(g) Message Authentication applies to all Interchange Links. The MAC must be calculated using, as a minimum, a DEA 3 (128-bit) key, Triple-DES and an algorithm conforming to AS 2805.4.1. All interchange PIN and MAC cryptographic functions are performed within a Tamper responsive SCM.

Reference AS 2805.4.1

Yes	No	N/A

If N/A response: Reason

(h) Interchange Lines are subject to whole-of-message encryption in accordance with AS 2805.5.4 (IAC Code Set Volume 3, clause 2.5.4)

Yes	No	N/A

If N/A response: Reason

(i) Interchange Links comply with the key management practices of IAC Code Set Volume 4, clause 4.5.2

Yes	No	N/A

If N/A response: Reason

(j) Interchange Lines comply with the key management practices of IAC Code Set Volume 4, clause 4.7.2 (if applicable).

Yes	No	N/A

If N/A response: Reason

(k) Open network PIN change solutions available to Cardholders meet relevant requirements.

Reference IAC Code Set Volume 2 (Issuers Code).

Yes	No	N/A

If N/A response: Reason

A.3.2 Device Management

(a) Each type of SCM used in Interchange, and those devices providing a Remote Management Solution for Security Control Modules have been evaluated by a Company accredited Evaluation Facility using the method and against the criteria given in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management) and have been approved for use by the Company. Amended effective 21.11.16

Reference AS 2805.14.1; AS 2805.14.2, IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

Yes	No	N/A

If N/A response: Reason

(b) Documented procedures exist, and are followed, to ensure that any Remote Management Solution for an SCM is managed in accordance with the requirements of IAC Code Set Volume 2, clause4.5.

Yes	No	N/A

If N/A response: Reason

A.3.3 Key Management

(a) Documented procedures exist, and are followed to control keys so that they exist in only one or more of the permissible forms:

(i) In a SCD;

(ii) Encrypted under a DEA 2 or DEA 3 key; and/or

(iii) Managed as two or more full length components using the principles of dual control and split knowledge.

Yes	No	N/A

If N/A response: Reason

.....

.....

(b) Documented procedures exist and are followed to ensure a person entrusted with a key component reasonably protects that component such that no person (not similarly entrusted with that component) can observe or otherwise obtain that component.

Yes	No	N/A

If N/A response: Reason

.....

.....

(c) Documented procedures exist and are followed to ensure keys and key components are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys.

Yes	No	N/A

If N/A response: Reason

.....

.....

(d) Documented procedures exist to ensure each of the following:

(i) A key is changed if its compromise is known or suspected;

(ii) Keys encrypted under or derived from a compromised key are changed;

(iii) A key is not changed to a variant or a transformation of the compromised key; and

(iv) The amount of time in which the compromised key remains active is consistent with the risk to all affected parties.

Yes	No	N/A

If N/A response: Reason

(e) Documented procedures exist and are followed to ensure a key is used for only a single designated purpose.

Yes	No	N/A

If N/A response: Reason

(f) Documented procedures exist and are followed to ensure that when a key is installed under dual control using key components that these key components are only combined within a SCD.

Yes	No	N/A

If N/A response: Reason

(g) Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. Key components are combined using one of the following functions:

(i) XOR; and/or

(ii) Encryption via DEA.

Yes	No	N/A

If N/A response: Reason

(h) Documented procedures exist and are followed to ensure when in secure transit, cleartext key components are protected from compromise in one of the following manners: Amended effective 21.11.16

(i) Key components are transported in separate tamper-evident packaging; or

(ii) Key components are transported in a device meeting the requirements of a Physically Secure Device.

Reference ISO 9564.1

Yes	No	N/A

If N/A response: Reason

(i) Documented procedures exist and are followed to ensure a cleartext key component is:

(i) Under the supervision of a person authorised by management with access to this component; or

(ii) Locked in a security container in such a way that can be obtained only by a person with authorized access; or

(iii) In secure transit; or

(iv) In a physically secure SCD.

Yes	No	N/A

If N/A response: Reason

(j) Documented procedures exist and are followed to ensure if keys are loaded or transported using an electronic key loading device then:

(i) The key loading device has been evaluated and meets the applicable security requirements (see clause A.3.2);

(ii) The key loading device is under the supervision of a person authorised by management, or is stored in a secure manner (e.g., in a safe) such that no unauthorised person may have access to it; and

(iii) The key loading device is designed or controlled so that only authorised personnel under dual control can utilise and enable it to output a key into another SCD. Such personnel ensure that the transfer is not being monitored, e.g., that there is no key recording device inserted between the SCDs.

Yes	No	N/A

If N/A response: Reason

(k) Documented procedures exist and are followed to protect the transfer of a key or key component into SCMs so as to prevent the disclosure of the key or key components. Examples of procedures include physical inspection of the SCD equipment to detect evidence of monitoring and dual custody of the loading process.

Yes	No	N/A

If N/A response: Reason

(l) Documented procedures exist and are followed to ensure that a key exists at only the minimal number of locations consistent with the operation of the system (e.g., including disaster recovery purposes, dual processing sites).

Yes	No	N/A

If N/A response: Reason

(m) If for archival purposes, reconstruction of a given key is required at a later date, procedures exist and are followed to ensure the key is retained in a form such as to preclude it being intentionally used again as active keying material.

Yes	No	N/A

If N/A response: Reason

(n) Documented procedures exist and are followed to ensure a key shared between communicating parties is not shared, except by chance, between any other communicating parties.

Yes	No	N/A

If N/A response: Reason

(o) Procedures exist and are followed to ensure a key or key component that has been used for a cryptographic purpose is erased or destroyed when it is no longer required using approved destruction procedures.

Yes	No	N/A

If N/A response: Reason

(p) Documented procedures exist and are followed to ensure that when a key transport key (KTK) is changed because its compromise is known or suspected, an organisation which has previously shared the key is informed of the compromise even if the KTK is no longer in use.

Yes	No	N/A

If N/A response: Reason

(q) Documented procedures exist and are followed to ensure if two or more of a key's components are stored within the same security container (which is under dual control), then the components are secured in tamper evident packaging to preclude one component holder from gaining access to the other component.

Yes	No	N/A

If N/A response: Reason

(r) Documented procedures exist and are followed to ensure a key loading device does not retain a clear-text copy of any key it has successfully transferred.

Yes	No	N/A

If N/A response: Reason

(s) Documented procedures exist and are followed to maintain a record of every instance when a container securing cryptographic materials is opened to record date, time, person(s) involved and the purpose of the access.

Yes	No	N/A

If N/A response: Reason

SIGNED for and behalf of **THE FRAMEWORK PARTICIPANT**

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit for and on behalf of the Framework Participant.

Name of Authorised Person

Signature of Authorised Person

Office Held

Date

AUDITOR SIGNOFF

By signing this Issuer Annual Security Audit the signatory states that the signatory is duly authorised to sign this Audit as auditor for and on behalf of the Framework Participant and that the signatory is satisfied with the accuracy of the responses contained within the Audit.

Name of Auditor

Signature of Auditor

Date

Next page is B.1

ANNEXURE B NEW FRAMEWORK PARTICIPANT CERTIFICATION

Note: Annexure B.1 Acquirer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.1 ACQUIRER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Clearing Association Limited
Level 6
14 Martin Place
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): .....

Place of Incorporation: .....

ACN / ABN / ARBN: .....

Registered Office Address .....

.....

Name of Contact Person:: .....

Telephone Number: (.....) .....

Email Address: .....

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Acquirer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Acquirers which are set out in IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) and IAC Code Set Volume 6 (ATM System Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Acquirer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Acquirer Certification Checklist is required to obtain that Certification;

(b) warrants that it satisfies the requirements applicable generally to Acquirers as set out in clause 2.1 of IAC Code Set Volume 3 (Acquirers Code), IAC Code Set Volume 5 (Settlement Code) and IAC Code Set Volume 6 (ATM System Code) as at the date of this Acquirer Certification Checklist, and that the information contained in this completed Acquirer Certification Checklist is correct and accurately reflects the results of system testing against current IAC requirements and including, if applicable, use of an appropriate test script supplied by the Company;

(c) if the Applicant is granted Certification, agrees to:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this Acquirer Certification Checklist is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with full particulars of any such wrong or misleading information.

Terms used in this Acquirer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Acquirer Certification Checklist the signatory states that the signatory is duly authorised to sign this Acquirer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the certification checklist.

Name of Auditor	Signature of Auditor
Date	

Note: This Annexure B.2 Issuer Certification Checklist is ONLY to be completed by a new Framework Participant.

B.2 ISSUER CERTIFICATION CHECKLIST

To: The Secretary
Australian Payments Clearing Association Limited
Level 6
14 Martin Place
Sydney NSW 2000

Re: Issuers and Acquirers Community

From: Name of Applicant ("**Applicant**"): .....

Place of Incorporation: .....

ACN / ABN / ARBN: .....

Registered Office Address .....

.....

Name of Contact Person:: .....

Telephone Number: ( ) .....

Email Address: .....

CERTIFICATION OBJECTIVES

The objective of Certification is to ensure that each IAC Applicant that becomes an Issuer confirms for the benefit of each other Framework Participant and the Company that it meets the technical, operational and security requirements applicable to Issuers which are set out in IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) as applicable.

REPRESENTATIONS AND UNDERTAKINGS

By signing this Issuer Certification Checklist, the Applicant:

(a) acknowledges that membership of IAC is conditional on the Applicant having obtained Certification in accordance with the IAC Regulations and Manual and that this Issuer Certification Checklist is required to obtain that Certification;

(b) warrants that it satisfies the requirements applicable generally to Issuers as set out in Part 5 of IAC Code Set Volume 2 (Issuers Code) and IAC Code Set Volume 5 (Settlement Code) as applicable, as at the date of this Issuer Certification Checklist, and that the information contained in this completed Issuer Certification Checklist is correct and accurately reflects the results of system testing against current IAC requirements and including, if applicable, use of an appropriate test script supplied by the Company;

(c) if the Applicant is granted Certification, agrees to:

(i) immediately notify the Company if it becomes, or has become, aware that any information contained in this Issuer Certification Checklist is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and

(ii) provide to the Company with full particulars of any such wrong or misleading information.

Terms used in this Issuer Certification Checklist have the same meanings as in the IAC Code Set unless otherwise defined.

SIGNED for and behalf of **THE APPLICANT**

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist for and on behalf of the Applicant.

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

AUDITOR SIGNOFF

By signing this Issuer Certification Checklist the signatory states that the signatory is duly authorised to sign this Issuer Certification Checklist as auditor for and on behalf of the Applicant and that the signatory is satisfied with the accuracy of the responses contained within the Issuer Certification Checklist.

Name of Auditor	Signature of Auditor
Date	

Next page is C.1

ANNEXURE C EXEMPTION REQUEST FORM

Framework Participant: _____ Approval to disclose to eftpos Payments Australia Limited **given** / **not given** (*delete as applicable*):

Authorised by:_____

Date:_____

Date of Request: _____ Date of Original Request: _____ Reference Number:_____

Section & clause number of requirement	Requirement for which Framework Participant is not in compliance	Situation (reason for non-compliance)	Risk	Rank	Compensating Controls	Residual Risk	Action to be taken and timeframe
If exemption is sought in respect of a particular device, insert Manufacturer, model, revision and software version	Type in the actual wording of the Requirement with which the Framework Participant is not complying	Describe the situation, including when and why out-of-compliance occurred.	Describe the risks the out-of-compliance situation poses	High, Medium or Low	List the compensating controls that reduce the risk	High, Medium or Low	List what you are doing to correct the non-compliance **For Extension Request** Indicate the reason why an extension is sought **Promised date of correction** Indicate the date when the situation will be corrected.

Risk Weighting

HIGH	MEDIUM	LOW
• potential loss of integrity of PINs • potential material losses to Framework Participants, Card Acceptors or Cardholders • potential mass fraud • potential loss of public confidence	• potential reduced integrity of PINS • potential changes to financial content of transaction • potential monetary losses to Framework Participants, Card Acceptors or Cardholders could be significant.	• minimal effect on the integrity of PINs • potential monetary losses to Framework Participants would not be significant.

Next page is D.1

ANNEXURE D IAC OPERATIONAL BROADCAST FORM

Disclaimer:

This document has been compiled from information provided by third parties. No representation or warranty is made by APCA as to the truth or accuracy of the information and APCA, its officers, employees and agents expressly disclaim all and any liability in respect of the information.

DOCUMENT TITLE *<Framework Participant>* *<Brief Broadcast Title>*	
DOCUMENT NUMBER:	IAC CS3\COB\nnn.yyyy
DETAILS	
Date of Advice:	<DD/MMM/YYYY>
Notifying Framework Participant:	
Framework Participant Experiencing Difficulty:	
CONTACT POINT	
Name:	<Contact Name>
Phone Number:	<Contact Phone>
Fax Number:	<Contact Fax>
Email Address:	<Contact Email>
PAYMENT SYSTEM AFFECTED	IAC – Issuers and Acquirers Framework
PROCESSES AFFECTED List of processes affected which may directly or indirectly impact other Framework Participants: • Unscheduled network outage; • Scheduled network outage; • Exchange of Operational Information; and • Disruptive Event.	
EXPECTED DURATION OF AFFECTED PROCESS	
Date Occurred / Scheduled:	<DD/MMM/YYY>
Start Time of Outage:	<HH:MM> (Approximate)
End Time of Outage:	<HH:MM> (Approximate)

COMMUNICATION PROCESS	
Advise Framework Participants:	<YES / NO>
Advise Non- Members:	<YES / NO>
APCA to provide prepared Statement:	<YES / NO>
(Please attach text of statement in Attachments below)	
Refer media to affected Framework Participant:	<YES / NO>

COMMENTS

ATTACHMENTS
Attach any IAC Operational Broadcast (COB) related documents here.

APCA Comments

Next page is E.1

ANNEXURE E PRINCIPLES FOR TECHNOLOGIES AT POINT OF INTERACTION

Inserted effective 1.1.16

[Informative]

E.1 Introduction

E.1.1 Background

New methods of conducting point of sale transactions, such as the widespread use of card-not-present acceptance in stores, or the technological innovations resulting in the use of other "form factors" for payments for e.g. creation of a virtual magnetic strip on a mobile phone that may not be adequately catered for in existing standards or processes are increasingly being introduced.

Establishing a set of principles to which the industry as a whole is in agreement, will allow greater clarity over what activities are to be encouraged or discouraged, and the extent to which existing rules can and should be modified in response to new technologies. It is not intended that these principles be considered binding – but that they be seen more as a guide to industry participants when considering new payments techniques.

In such cases the following principles define the basis of what is acceptable in the Australian point of sale/point of interaction card payments environment.

E.1.2 Scope

These principles apply to all face-to-face card transactions where both cardholder and merchant are present, and where another individual, organisation or the industry as a whole could be impacted by the transaction or any resulting fraudulent activity.

E.2 Principles

E.2.1 Usability

Clarity and ease of use for cardholders and simplicity of deployment for merchants are paramount to the success of the system; therefore:

(a) Where feasible, card acceptance terminals should be multi-purpose and able to accept different types of card payments so that merchants are not required to deploy different terminals dependant on payment type.

(b) In order to support multiple accounts linked from combo cards, terminals should be capable of implementing appropriate procedures for card account selection.

E.2.2 Reliance on standards

The use of standards for card payments improves security, interoperability and reliability; therefore:

(a) Wherever possible, industry rules should rely upon International, open standards (including ISO, Australian or other national standards as well as the global standards from PCI and EMV).

(b) If an acquirer wishes to deviate from a standard, then it should be agreed through a joint industry process.

(c) If a relevant standard does not exist, individual issuer, acquirers or card schemes may choose to support a particular solution, with the development of a suitable industry standard to be encouraged.

E.2.3 Security of cardholder data

Trust in the card payments system is integral to its success; therefore:

(a) Card payment products should be designed with security and reliability for cardholders and other users of the system.

(b) The PIN must continue to be strongly protected, especially whilst the magnetic stripe and card number are still widely used on Australian cards.

(c) When using static cardholder data across different products, account must be taken of potential risks to other products (e.g. FIs using the PIN to authenticate customers to internet banking or merchants using the PAN to identify customers on their backend systems).

E.2.4 Preferred payment facility

While different forms of card acceptance are allowed in the merchant environment, the goal is to achieve security as close as possible to chip and PIN. Therefore, acquirers should be encouraging merchants to implement a card payment solution in the following order of preference, and with appropriate security in place:

	Face to face – payment facilities
1.	Approved POS device providing a card present facility
2.	Using the cardholder's smartphone or other device using an app1 with the card present in other "form factor" but capable of interacting with the POS device
3.	Using the cardholder's smartphone or other device using an app providing a card not present facility e.g. using stored card details
4.	Card not present facility e.g. – card details entered manually on merchant's device / website or app for each transaction

Next page is F.1

[1] Apps are pieces of computer software (applications) that allow customisation of a smartphone, tablet or other device.

ANNEXURE F NOTICE OF STANDARD MERCHANT PRICING FOR CREDIT, DEBIT AND PREPAID CARD TRANSACTIONS

Inserted effective 1.6.17

[Acquirer Logo] ***[Informative]***

F.1 INTRODUCTION AND PURPOSE

Reforms driven by the Reserve Bank of Australia, and enacted by the Australian Competition and Consumer Commission banning excessive surcharging have into effect.

Specifically, from 1 September 2016, Large Merchants are required to ensure that their customer surcharges for accepting credit, debit and prepaid card payments do not exceed the cost of acceptance for each of those payment types. The requirement applies to all other merchants from 1 September 2017.

This document summarises the key elements of these reforms. More information is available through the Q&As created by the RBA and the ACCC.

F.2 BENEFITS TO MERCHANTS

The framework emphasises the right of merchants to surcharge to cover their acceptance costs and signal differences in costs to consumers. It also improves the transparency of payment costs to merchants.

F.3 PERMITTED SURCHARGES AND COST OF ACCEPTANCE

Merchants are entitled to levy surcharges for card transactions as long as they do not exceed the cost of acceptance for the Merchant for that scheme at that time.

The cost of acceptance is the average cost for a card scheme for a particular reference period, calculated by expressing the total value of all merchant service fee/s and other applicable fees and premiums paid by you to us or third party payment facilitators as a percentage of the total value of all card transactions for that scheme during that reference period.

F.4 MERCHANT FEE STATEMENTS

Each month and annually from 1 June 2017, we will provide you with a fee statement, indicating the average fees applicable to the card transactions we acquire for you, to help you calculate your costs of acceptance for the following:

(a) **debit card schemes** (which include prepaid card schemes in all cases): eftpos, Debit Mastercard, and Visa Debit; and,

(b) **credit card schemes**: MasterCard Credit, and Visa Credit.

This transparency will help merchants to know how much it costs them to accept card payments and will also enable merchants to make more informed decisions about whether to surcharge different payment methods.

The fee statement will clearly detail:

(a) the reference period to which the fee statement relates;

(b) the fees paid by you to us in relation to the card transactions we acquired for you during the reference period; these will be the aggregate of merchant service fees, terminal rental fees, gateway or fraud prevention fees, and any other fees for processing transactions (such as international service assessments, switching fees and fraud-related chargeback fees, but not the cost of any actual chargebacks);

(c) the total value of card transactions we acquired for you during the reference period; and

(d) the average cost of acceptance for card transactions by scheme.

The fee statement will typically follow the format set out below:

MERCHANT FEE STATEMENT **FOR THE PERIOD [ ] TO [ ]** **(Statement Period)**						
	eftpos / eftpos Prepaid	**Debit Mastercard/ Mastercard Prepaid**	**Mastercard Credit**	**Visa Debit / Visa Prepaid**	**Visa Credit**	**Other***
TOTAL VALUE OF CARD TRANSACTIONS $AUD ("X")						
TOTAL VALUE OF FEES $AUD ("Y")						
AVERAGE COST OF ACCEPTANCE ("Y/X%")						

* Acquirers are encouraged, but not obliged, to disclose acceptance costs for card payment types not expressly covered by the reforms (e.g. Union Pay, JCB, Diners Club).

Note: Merchants will be able to surcharge any of the cards covered by the RBA's standard up to the average percentage cost of acceptance in their annual statement for that card type. However, some merchants may have other costs of accepting a particular type of card that they would like to include in their surcharge. These may include:

- *gateway fees paid to a payment service provider*
- *the cost of fraud prevention services paid to an external provider*
- *any terminal costs paid to a provider other than the merchant's acquirer or payments facilitator*
- *the cost of insuring against forward delivery risk. This applies to agents (such as travel agents) who pay an external party to insure against the risk that the agent will be liable to a customer for the failure of a principal supplier (such as an airline or hotel) on payments accepted via cards.*

If those costs meet the requirements for inclusion and can be documented, merchants will be able to add them to the costs charged by their acquirer or payment facilitator over the previous year and, based on their total costs, calculate their average percentage cost for that card system. Merchants may not surcharge above this average cost.

END