

Effective:
21 November 2017
Version 006

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 6 ATM System Code

Commenced 1 July 2015

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

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

Code Set for
ISSUERS AND AQUIRERS COMMUNITY
FRAMEWORK

Volume 6
ATM System Code

INDEX

| | | |
|---------------|--|------------|
| PART 1 | INTRODUCTION, INTERPRETATION AND DEFINITIONS | 1.1 |
| 1.1 | Purpose of this Code..... | 1.1 |
| 1.2 | ATM System Code | 1.1 |
| 1.3 | Role of the ATM Code Committee..... | 1.2 |
| 1.4 | Obligations of IA Participants..... | 1.2 |
| 1.5 | Subscribers in any other Capacity | 1.4 |
| 1.6 | Scope of Standards and Requirements | 1.4 |
| 1.7 | Interpretation | 1.5 |
| 1.8 | Definitions | 1.6 |
| PART 2 | SUBSCRIBING TO THE ATM SYSTEM CODE | 2.1 |
| 2.1 | Qualifications for Subscription | 2.1 |
| 2.2 | Subscription | 2.1 |
| PART 3 | ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS | 3.1 |
| 3.1 | Network and Interchange Requirements | 3.1 |
| 3.2 | Interchanges | 3.2 |
| 3.3 | Interchange Technical Specifications | 3.2 |
| 3.4 | Temporary Suspension of Interchange..... | 3.4 |
| 3.5 | Unauthorised Access Prevention..... | 3.4 |
| PART 4 | ATM INTERCHANGE OPERATIONS..... | 4.1 |
| 4.1 | Obligation to engage in ATM Interchange..... | 4.1 |
| 4.2 | Terms Applicable to ATM Interchange..... | 4.1 |
| 4.3 | ATM Transactions | 4.2 |
| 4.4 | EMV Phase 1 Processing..... | 4.2 |
| 4.5 | EMV Phase 2 Processing..... | 4.3 |
| 4.6 | Liability Shift Claim Process | 4.5 |
| 4.7 | Counterfeit ATM Transaction Claim - Dispute Resolution | 4.6 |
| 4.8 | Settlement..... | 4.6 |
| 4.9 | Interchange Fees | 4.6 |
| 4.10 | Interchange Reports..... | 4.7 |
| 4.11 | ATM Interchange Reports and Transaction Listings | 4.7 |

| | | |
|---|--|------------|
| 4.12 | Interchange Settlement Reports (Value)..... | 4.8 |
| 4.13 | Interchange Billing Reports | 4.8 |
| 4.14 | Retention Period..... | 4.9 |
| 4.15 | ATM Terminal - Cards Retained | 4.9 |
| 4.16 | Good Design Principles Applicable to ATM Terminal Interface | 4.10 |
| 4.17 | Doubtful ATM Transactions | 4.10 |
| 4.18 | Doubtful ATM Transactions - Issuer Responsibilities [Deleted]..... | 4.10 |
| 4.19 | Doubtful ATM Transactions – ATM Affiliate Responsibilities [Deleted]..... | 4.10 |
| 4.20 | Retention of Records – Doubtful Transactions [Deleted] | 4.10 |
| 4.21 | Disputed Transactions – General | 4.10 |
| 4.22 | Disputed Transactions - Issuer’s Responsibilities | 4.10 |
| 4.23 | Disputed Transactions - Acquirer’s Responsibilities | 4.12 |
| 4.24 | Disputed Transactions - ATM Affiliate and Third Party Responsibilities | 4.14 |
| 4.25 | Re-presentment..... | 4.15 |
| 4.26 | Retention of Records – Disputed Transactions..... | 4.15 |
| 4.27 | Timing | 4.15 |
| 4.28 | Enquiries and Notification of System Outages..... | 4.17 |
| 4.29 | Management of System Outages – Operational Broadcast | 4.18 |
| 4.30 | Notification of a Disruptive Event..... | 4.19 |
| ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION | | A.1 |
| A.1 | Standard Interchange..... | A.1 |
| A.2 | Purpose..... | A.1 |
| A.3 | Scope..... | A.1 |
| A.4 | References..... | A.1 |
| A.5 | Supported Message Types..... | A.2 |
| A.6 | Supported Transaction Set..... | A.3 |
| A.7 | Network Management | A.7 |
| A.8 | Key Management | A.9 |
| A.9 | Time Out Parameters | A.13 |
| A.10 | Link Reconciliation | A.13 |
| A.11 | Link Settlement Times..... | A.15 |
| A.12 | Message Formats..... | A.15 |
| A.13 | Fields | A.40 |
| A.14 | Response Codes..... | A.48 |
| ANNEXURE B. INTERCHANGE BIT MAP..... | | B.1 |
| ANNEXURE C. TECHNOLOGY FALLBACK | | C.1 |
| C.1 | Introduction | C.1 |
| C.2 | Technology Fallback | C.1 |
| C.3 | Field 47 | C.1 |
| C.4 | Terminal Capability Code (047) | C.1 |

| | |
|---|------------|
| ANNEXURE D. COMMUNICATIONS PHILOSOPHY | D.1 |
| ANNEXURE E. STANDARD INTERCHANGE TERMS | E.1 |
| E.1 Application to Third Party Agreements | E.1 |
| E.2 Approved Cards | E.1 |
| E.3 Promotions and Advertising..... | E.1 |
| E.4 Indemnity and Limitation of Liability..... | E.1 |
| E.5 Direct Charging | E.2 |
| E.6 Variation..... | E.2 |
| ANNEXURE F. DIRECT CHARGING RULES | F.1 |
| F.1 General Principles..... | F.1 |
| F.2 Amount and Variation of the ATM Operator fee and decline..... | F.1 |
| F.3 When Cardholders may be charged an ATM Operator Fee..... | F.1 |
| F.4 Disclosure Rules | F.2 |
| F.5 Record of Transaction..... | F.4 |
| F.6 Message Flow | F.5 |
| F.7 Settlement of ATM Operator Fees..... | F.8 |
| F.8 Transition | F.8 |
| F.9 Damages for Non-compliance with Direct Charging Rules | F.8 |
| F.10 Prohibition on hindering or preventing Direct Charging..... | F.9 |
| ANNEXURE G. EMV@ATM TERMINAL STANDARDS | G.1 |
| G.1 Cards | G.1 |
| G.2 Card Acceptance..... | G.1 |
| G.3 Transactions support and processing..... | G.1 |
| G.4 Terminal Processing..... | G.2 |
| G.5 Technical Fallback..... | G.6 |
| G.6 Receipts | G.6 |
| G.7 ATM Configuration | G.6 |
| G.8 Preferred transaction flows..... | G.9 |
| G.9 Contactless Requirements | G.12 |
| ANNEXURE H. ESCALATION PROCEDURE..... | H.1 |
| H.1 Objective | H.1 |
| H.2 Escalation Process..... | H.1 |
| H.3 Severity levels are as follows:..... | H.1 |
| H.4 Escalation of Call..... | H.2 |
| H.5 ATM Interchange Escalation Table..... | H.4 |
| ANNEXURE I. ATM INSTALLATION CHECKLISTS | I.1 |
| I.1 Security Checklists for Installation of ATMs | I.1 |
| I.2 Physical Security Mechanisms | I.1 |
| I.3 Logical Security Mechanisms | I.1 |

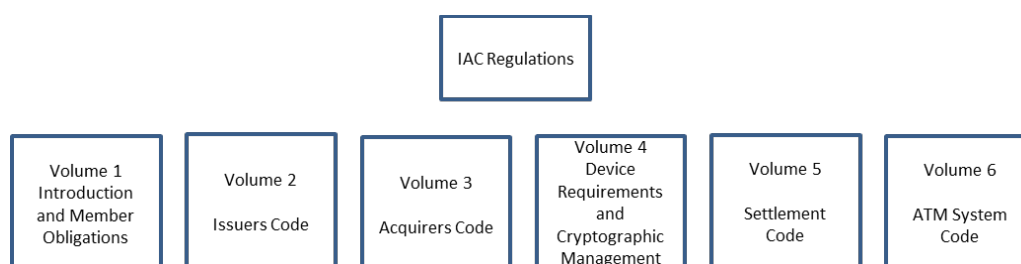
| | |
|--|------------|
| ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS..... | J.1 |
| J.1 Purpose..... | J.1 |
| J.2 Problem statement | J.1 |
| J.3 Requirements..... | J.2 |
| J.4 Possible solutions..... | J.2 |
| J.5 Solutions using standard ATM software | J.3 |
| J.6 Solutions involving modified ATM software..... | J.5 |
| J.7 Recommend framework solution | J.6 |
| J.8 Bibliography | J.7 |
| ANNEXURE K. SUBSCRIPTION FORM | K.1 |
| ANNEXURE L. COUNTERFIET ATM TRANSACTION CLAIM NOTICE | L.1 |
| ANNEXURE M. DISPUTED AND SETTLED FILE TECHNICAL SPECIFICATION | M.1 |
| ANNEXURE N. DISPUTED TRANSACTION PROCESS | N.1 |

PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this Code

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

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



This Part 1 sets out:

- (a) the objects of the Code;
- (b) what the Code covers; and
- (c) the key obligations of ATM Framework Participants.

1.2 ATM System Code

The ATM System Code is a Core Code within the meaning of the IAC Regulations and forms part of, and supplements the other IAC Codes. The objects of the Code are to establish:

- (a) the conditions of an IA Participant's participation in the ATM System;
- (b) the operational and security standards, requirements and procedures which apply specifically to IA Participants in relation to their participation in the ATM System; and
- (c) a Recognised APS Framework within the meaning of the Company's Constitution for the coordinated development implementation and operation of effective standards and procedures to facilitate ATM Interchange between IA Participants in Australia, including without limitation:
 - (i) procedures to promote the efficiency, security and integrity of ATM Transactions; and

- (ii) rules to promote the universal acceptance of Cards at ATM Terminals.

1.3 Role of the ATM Code Committee

The role of the ATM Code Committee is to:

- (a) administer the ATM System Code, in accordance with the terms determined by the IAF, the IAC Regulations and this Code;
- (b) provide a forum for ATM Framework Participants and other interested parties to participate in, and contribute to, the development of ATM industry policy in Australia; and
- (c) provide a forum for ATM Framework Participants and other interested parties to contribute to the development of:
 - (i) procedures to promote the security of ATM Transactions, by making recommendation to the relevant IAC Code Committee;
 - (ii) specifications and standards for ATM Terminals utilised, and Cards issued by, and communications links and message formats between, Framework Participants, by making recommendation to the relevant IAC Code Committee.

1.4 Obligations of IA Participants

An IA Participant, which engages in ATM Interchange in more than one capacity, must satisfy the requirements applicable to each such capacity. In summary, the primary obligations of an IA Participant:

- (a) which subscribes to the Code and participates in an Interchange network as an Acquirer, are to:
 - (i) comply with all of the Certification obligations imposed on Acquirers under Volumes 1 - 4 of the IAC Codes, particularly Volume 1 (Introduction and Member Obligations), Volume 3 (Acquirer Code) and Volume 4 (Device Requirements and Cryptographic Management), which relevantly oblige an Acquirer to:
 - (A) ensure that its ATM Terminals are Certified to be compliant with relevant security standards, including, from the Compliance Date, the EMV@ATM Terminal Standards set out in this Code, prior to connection to the ATM System, and prior to engaging in ATM Interchange: see Part 4;
 - (B) comply with all applicable ATM System network and interchange requirements: see Part 3;

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

- (ii) ensure that its ATM Terminals are capable of processing all Approved Cards: see Part 4;
 - (iii) engage in ATM Interchange with each Issuer on the Standard Interchange Terms: see Part 4 and Annexure E;
 - (iv) comply with the ATM Interchange operational rules set out in Part 4;
 - (v) comply with the ATM Direct Charging Rules set out in Annexure F, in accordance with Part 4; and
 - (vi) settle with Issuers for the obligations arising from ATM Interchange in accordance with the provisions of the IAC –Settlement Code: see Part 4;
 - (vii) comply with the IAC Regulations;
- (b) which subscribes to the Code and participates in an Interchange network as an Issuer, are to:
- (i) comply with all of the Certification obligations imposed on Issuers under IAC Code Volume 1 (Introduction and Member Obligations), Volume 2 (Issuer Code) and Volume 4 (Device Requirements and Cryptographic Management), which oblige an Issuer to:
 - (A) ensure that Cards issued by it comply with the IAC Card Standards including, from the Compliance Date, the EMV Standards for Cards: see Part 4;
 - (B) comply with ATM System network and interchange requirements: see Part 3;
 - (ii) use reasonable endeavours to ensure the integrity of Approved Cardholders: see Part 4 and Annexure E;
 - (iii) engage in ATM Interchange with each Acquirer, on the Standard Interchange Terms: see Part 4 and Annexure E;
 - (iv) comply with the ATM Interchange operational rules set out in Part 4;
 - (v) comply with the ATM Direct Charging Rules in accordance with Part 4 and as set out in Annexure F;
 - (vi) settle with Acquirers for the obligations arising from ATM Interchange in accordance with the provisions of the IAC Settlement Code: see Part 4;

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

- (vii) indemnify each Acquirer in relation to losses arising from the fraudulent use or misuse of Cards issued by it: see Part 4 and Standard Interchange Terms in Annexure E; and
- (viii) comply with the IAC Regulations.

1.5 Subscribers in any other Capacity

- (a) Operator Members and Affiliates are encouraged to subscribe to this Code to ensure that ATM industry policy, standards and procedures established under the auspices of the ATM Code Committee represent the widest possible range of industry interests and perspectives.
- (b) The primary obligations of ATM Operator Members and ATM Affiliates, including but not limited to those whose nominee may have been:
 - (i) appointed as a member of the ATM Code Committee; or
 - (ii) invited to attend ATM Code Committee meetings; or
 - (iii) issued with ATM Code Committee meeting materials;

are to participate in good faith in ATM Code Committee meetings and activities, observe all applicable procedural and confidentiality requirements, and other requirements of Framework Participants, under the IAC Regulations and otherwise under any terms of reference or charter determined by the IAF for the purposes of this Code.

- (c) ATM Affiliates are bound by Part 4 (clauses 4.19 and 4.24) to assist IA Participants with the investigation of Disputed Transactions and Doubtful Transactions.

1.6 Scope of Standards and Requirements

- (a) Subject to paragraph (b), this Code applies to ATM Transactions processed across the ATM System regardless of the type of Card and/or account being used and/or accessed. This includes:
 - (i) all domestically acquired ATM Transactions initiated with a non-scheme debit card, including ATM Transactions initiated with the debit functionality of a Card that also has scheme credit and/or debit functionality, and processed across an Interchange Link and
 - (ii) ATM Transactions initiated with a scheme credit or debit card which result in the direct exchange of an Item across a network, other than a scheme network, or Interchange Link (such as nearly all ATM Transactions initiated with a domestic scheme credit card or debit card).

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

- (b) This Code does not apply to the electronic processing or settlement of credit card transactions and other scheme transactions via scheme networks, or resolution of disputes in relation to such transactions. These are governed by the rules and regulations published by the various card schemes.
- (c) Bilateral Interchange Agreements entered into by IA Participants prior to the Commencement Date continue to be enforceable provided however that if a provision of an Interchange Agreement is inconsistent with a provision of this Code then the latter prevails to the extent of the inconsistency.

1.7 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.

1.8 Definitions

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

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

- (a) under arrangement with and on behalf of an Issuer, discharges the obligations owed by that Issuer to the relevant Cardholder; and
- (b) engages in Interchange Activity with that Issuer as a result.

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

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

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

Inserted effective
21.11.17

“**Approved Cardholder**” means:

Inserted
effective 1.1.16

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

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

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

Amended
effective 1.1.16

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

“**AS**” means Australian Standard as published by Standards Australia.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

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

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

“Cash” means Australian legal tender.

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

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

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

Inserted
effective 1.1.16

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

Inserted
effective 1.1.16

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

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

“Committee of Management” means the committee constituted under Part 7 of the Regulations.

“Company” means AusPayNet.

“Compliance Date” means 31 December 2016.

“Compromised Terminal” means a Terminal that has been tampered with for fraudulent purposes.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“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
- (b) where the ATM Transaction amount is claimed to be incorrect; or
- (c) in respect of which the ATM Operator Fee is claimed to be incorrect.

Inserted
effective 1.1.16

Inserted
effective 1.1.16

Inserted
effective 1.1.16

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

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

“Doubtful ATM Transactions” means those ATM Transactions which appear to have been successfully completed, although the ATM Transaction may not be recorded against the relevant Cardholder account.

Last amended
effective
21.11.16

“EFT” means Electronic Funds Transfer.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“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, in the circumstances described in Annexure G.5.1.

Amended
effective
21.11.17

“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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“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

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

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

“LVSS Contact” means the person nominated by a IA Participant as its primary contact for LVSS inquiries, as listed on the Company’s extranet.

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

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

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

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

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

Inserted
effective 1.6.17

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

“Operator Member” has the meaning given in the IAC Regulations.

Inserted
effective 1.1.16

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

“PCI” means the Payment Card Industry Security Standards Council.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

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

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

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

Amended
effective 29.4.16

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

“PED” means a PIN Entry Device.

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

Amended
effective
21.11.16

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

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

“POI” means Point Of Interaction technologies that can be provided to a merchant to undertake card payments. POI technologies include attended and unattended Point of Sale (POS) devices and ATMs.

Inserted
effective
1.1.16

“Prepaid Card” means a Card that:

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

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

- (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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“**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:

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

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

“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.

PART 1. INTRODUCTION, INTERPRETATION AND DEFINITIONS

“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 SUBSCRIBING TO THE ATM SYSTEM CODE

This Part 2 describes how eligible IA Participants, Operator Members and Affiliates subscribe to this Code.

2.1 Qualifications for Subscription

In order to be a subscriber to this Code and, in the case of an IA Participant, participate in ATM Interchange in accordance with this ATM System Code, a person must:

- (a) be admitted as a member of the IAC in accordance with the IAC Regulations and be able to comply with all terms and conditions of membership;
- (b) be able to comply with any applicable ATM Laws; and
- (c) in the case of an IA Participant, be capable of being Certified in accordance with Volume 1 of the IAC Code Set.

2.2 Subscription

- (a) Subject to satisfying the requirements in clause 2.1, each IA Participant is deemed to be a subscriber to this Code on and from the Commencement Date.
- (b) An Operator Member or Affiliate that wishes to subscribe to this Code may do so by written notice, in the form of Annexure K, to the Secretary. The subscription becomes effective on the date of receipt of the notice by the Secretary.
- (c) Following receipt of a written subscription notice, the Secretary will notify all other ATM Framework Participants of the new subscriber, and the effective date the subscription.
- (d) For avoidance of doubt, the fees payable by an IA Participant, Operator Member or Affiliate under Part 10 of the IAC Regulations are inclusive of all fees referable to its subscription to, and its share of the administration costs of, this Code.

Next page is 3.1

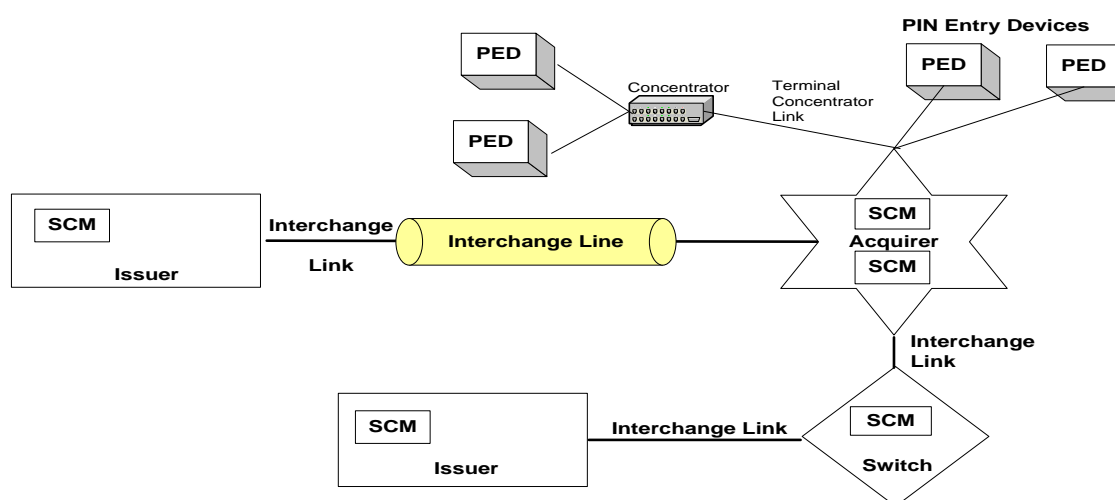
PART 3. ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS

PART 3 ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS

This Part 3 sets out the standards applicable ATM Interchange, including Interchange Links and Interchange Lines.

3.1 Network and Interchange Requirements

- (a) The standards set out in this Part 3 address security requirements from the point of PIN entry through to the point of verification.
- (b) The Acquirer is responsible for the network downstream to the Terminal. This may include Third Party Providers. The Issuer and Acquirer are jointly responsible for the Interchange Link.
- (c) The ATM network can be illustrated as follows:



- (d) An Acquirer switch must not add more than a maximum of three seconds elapsed time through the components of its network to the total processing time of an ATM Transaction (as an ATM Transaction consists of both a request and a reply, message transit times for both Acquirers and any intermediate network nodes should not exceed 1.5 seconds). The three-second target is taken to be the average ATM Transaction time within a peak load hour.
- (e) Where Third Party Providers are engaged in the delivery of Interchange e.g., Switches, the engaging party remains ultimately responsible for ensuring that the third party complies with the standards and procedures specified in this Code.
- (f) Interchange Links shall be supported 24 hours per day, every day including weekends and holidays.

PART 3. ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS

- (g) The availability of each IA Participant's EFT systems shall meet or exceed 98% when averaged over one calendar month excluding telecommunications outages.
- (h) The Issuer host must respond to a request for Authorisation within a period not exceeding 15 seconds. The fifteen-second target is taken to be the average ATM Transaction time within a peak load hour.
- (i) The maximum time-out values in the table below are indicative and are provided for guidance only.

| Component | Time-out | Maximum Delay Introduced |
|-------------------|------------|--|
| ATM Terminal | 60 seconds | |
| Intermediate Node | | 3 seconds total (1.5 seconds per transit) |
| Acquirer | 23 seconds | 3 seconds (1.5 seconds per transit) |
| Issuer | | 15 seconds |

3.2 Interchanges

- (a) For the avoidance of doubt, Interchange Link is the term used to refer to the logical communication path between two communicating Nodes. Interchange Line refers to the physical communication path between those Nodes. A single Interchange Line can support multiple Interchange Links.
- (b) Links wholly internal to an Issuer, an Issuer's exclusive environment, or those not carrying personal identification numbers are not Interchange Links for the purposes of these requirements.
- (c) Terminal concentrator lines are not subject to the requirements of Interchange Lines and Interchange Links.
- (d) Interchange Links shall be so constructed and managed such that each link will form a separate, distinct, cryptographic zone.
- (e) Distinct security requirements apply to both Interchange Links and Interchange Lines.

3.3 Interchange Technical Specifications

- (a) The specifications prescribed by this clause 3.3 will apply to all ATM Interchanges.

PART 3. ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS

- (b) **Dialogue:** A two message dialogue will be used across the Interchange Link.
- (c) **Communications Protocol and Line Configuration:** All IA Participants will support, at a minimum, TCP/IP as the default protocol on the Interchange. Alternative protocols may be used where mutually agreed. Preferably two lines will be installed – primary and secondary with load sharing across them. Testing will be performed using either a separate test line; a swapped secondary or test PVCs defined on the production lines: see Annexure D (Communications Philosophy).
- (d) **Message Formats:** IA Participants must ensure messages are formatted in accordance with the Standard Interchange Specification message formats set out in Annexure A and the Interchange BIT Map set out in Annexure B.

Note: Field 47 indicator modification in case of Technology Fallback is as prescribed by Annexure C.

- (e) **Reconciliation Messages:** The exchange of reconciliation messages will be within 10 minutes from the agreed cut-over time. These reconciliation messages will relate to all ATM Transactions where the request/advice message bears a date consistent with the data being settled.
- (f) **Sign-On:**
 - (i) A Sign-On is unidirectional and therefore each endpoint will be required to Sign On independently;
 - (ii) Both endpoints must receive and successfully verify an 0810 Network Management Request Response (logon) from the other before starting any other message exchange;
 - (iii) When ready to Sign On, a party should attempt to Sign On and continue to attempt to Sign On until a successful response has been received;
 - (iv) Upon receipt of an unsolicited Sign On (i.e. Receiving a Sign On message when in an assumed signed on state) or a message with a response code indicating an irrecoverable error, a party should send an immediate Sign Off message and attempts to Sign On should be made as soon as possible; and
 - (v) All Sign On response messages should be inspected to ensure that the response code indicates a successful sign on. After a successful sign on, both parties must complete a successful key exchange (using 0820/0830 key exchange messages) before either party can send value Transactions.

PART 3. ATM SYSTEM NETWORK AND INTERCHANGE REQUIREMENTS

- (g) **Messages:** The following messages will be used – 0200, 0210, 0220/1, 0230, 0420/1, 0430, 0520/1, 0530, 0800, 0810, 0820, 0830.
- (h) **Redundancy:** It is desirable that both lines are always active, running as primary and secondary. This allows for better redundancy without manual intervention. Both lines require line encryption as stated.
- (i) **Terminal details:** Transaction messages must contain Terminal name, location and Terminal ID to enable completion of statement narratives.
- (j) **Interchange Cryptographic Keys:** IA Participants must comply with the requirements for Interchange cryptographic keys as set out in the IAC Code Volume 3 (Acquirer Requirements).

3.4 Temporary Suspension of Interchange

- (a) Where in the reasonable opinion of an IA Participant or other intermediate network entity, excessive ATM Transaction response times from the other party are causing a downgrading of the service level in the Interchange system the first affected party may temporarily suspend its services for such period or periods as it shall think fit to restore the service level of the Interchange system to normal level.
- (b) The first affected party must notify the other party and the Company prior to suspending the service if practical, or at the earliest opportunity after suspending the service.

3.5 Unauthorised Access Prevention

Each party to the Interchange, including each IA Participant, Third Party Provider and any intermediate network entity must maintain procedures for avoiding any unauthorised access to or use of, the Interchange system through its own hardware, software, Interchange Lines and operational procedures which enable the exchange of authorisation and reconciliation of financial ATM Transactions. It is the responsibility of the engaging IA Participant to make inquiries and to satisfy itself that its Third Party Provider or intermediate network entity complies with this clause 3.5.

Next page is 4.1

PART 4 ATM INTERCHANGE OPERATIONS

This Part 4 sets out:

1. The business rules to be followed by all IA Participants as parties to ATM Interchange; and
2. Regulatory obligations applicable to ATM Interchange.

4.1 Obligation to engage in ATM Interchange

- (a) Subject to clause 4.1(c) each IA Participant must engage, or be ready to engage, in ATM Interchange with each other IA Participant by reason of having established a combination of:
 - (i) Direct Connections;
 - (ii) Direct Clearing/Settlement Arrangements; and/or
 - (iii) having appointed a Clearing/Settlement Agent to engage in ATM Interchange on its behalf.
- (b) This Code does not govern the establishment of the arrangements described in clause 4.1(a).
- (c) Nothing in this Code obliges an IA Participant to engage in ATM Interchange with any other IA Participant which is, in its reasonable opinion, in material default of any ATM Law, any default of any material technical or operational requirement specified in this Part 4 or any device or data security requirement which applies to that IA Participant under any part of the IAC Code Set.

4.2 Terms Applicable to ATM Interchange

Each IA Participant engaging in ATM Interchange with each other IA Participant must do so in accordance with:

- (a) its Certification Undertakings;
- (b) the Standard Interchange Terms in Annexure E;
- (c) the Standard Interchange Specification set out in Annexure A;
- (d) the Direct Charging Rules in Annexure F; and
- (e) the provisions of this Part 4.

4.3 ATM Transactions

- (a) **(Transaction Types)**: Each Acquirer must, as a minimum, be capable of supporting the following ATM Transactions:
- (i) Cash withdrawal transactions;
 - (ii) Balance enquiries; and
 - (iii) Reversal of the above Transactions and enquiries.
- (b) **(Account Selection)**: As a minimum, account selection at ATM Terminals must provide for Cardholder selection of both Cheque and Savings accounts.
- (c) **(Record of Transaction)**: An Acquirer must ensure that:
- (i) each Record of Transaction generated by a Terminal is clear and unambiguous. It must, as a minimum, with the standards detailed in the e-Payments Code.
 - (ii) any Card number included on the Record of Transaction has at least four (4) digits excluded. The preferred method of truncation is to print the first six (6) digits and the last (3) digits of the Card number on the Record of Transaction.
 - (iii) card expiry dates are excluded from Cardholder Records of Transaction.
 - (iv) it (the Acquirer) is clearly identified on the Record of Transaction.
 - (v) Annexure F prescribes additional requirements concerning a Record of Transaction for ATM Transactions which involve an ATM Operator Fee.
- (d) **(Supported Cards)**: Subject to this Code, the Cards to be supported by an Acquirer are defined in each of its bilateral Interchange Agreements.
- (e) **(PIN Data)**: Where a Transaction contains PIN data (bit 52), that PIN data must be formatted in accordance with one of the PIN Block formats specified in AS2805.3.1 with the exception of formats 1, 2 and 8.

4.4 EMV Phase 1 Processing

- (a) Clause 4.4(b) to (h) applies to ATM Transactions arising from the use of Australian IC Cards at an EMV capable ATM during EMV Phase 1.
- (b) Phase 1 processing is only applicable until such times as the Terminal and the relevant Interchange Link(s) are upgraded to be EMV capable.

-
- (c) All ATMs must provide account selection facilities, (minimum cheque/savings) when presented with an Australian IC Card and credit (cash advance) when presented with an EMV combo (Scheme credit/debit) card.
 - (d) The Financial Request Message created for the ATM Transaction is to be presented to the Issuer with the account selected by the cardholder mapped into bit 003.
 - (e) When an Australian IC Card or EMV combo card is presented and a debit (cheque/savings) is selected or credit (cash advance) is selected that is to be routed bilaterally, the Acquirer may choose to use either magnetic stripe sourced card information or optionally card information sourced from the IC to generate the Financial Request Message.
 - (f) Further, the ATM may retrieve the Track Two Equivalent Data from the IC. The Track Two Equivalent Data formatted in accordance with AS 3524 and clause 9.11.3 (Data Element 35) may be used to construct a Financial Request Message, which must be forwarded to the Issuer in accordance with magnetic stripe processing formats and rules (as contained in Annexure A). Where this is done the POS entry mode must accurately reflect the source of the card information.
 - (g) If Track Two Equivalent Data is obtained from an Australian IC Card then POS entry code “051” (contact interface) or POS entry code “071” (contactless interface) must be used in the Financial Request Message.
 - (h) If the Card information of an Australian IC Card or EMV combo card is unable to be read, then the Track Two Data can be electronically captured from the card’s magnetic stripe and the POS entry code “021” (refer 9.11.3) must be used in the Financial Request Message.

4.5 EMV Phase 2 Processing

- (a) **(EMV Compliance):** On and from the Compliance Date:
 - (i) each Issuer must, to the extent that it issues Cards containing a Debit Chip Application, ensure that those Cards comply with the EMV Standards for Cards; and
 - (ii) each Acquirer must:
 - (A) ensure that its ATM Terminals, including those deployed by a third party for which it is the lead Acquirer, comply with the EMV@ATM Terminal Standards; and

Amended
effective
21.11.17

- (B) ensure that each ATM Transaction initiated at its ATM Terminal with a chip Card, containing an AID of any Approved Card Payment System, is processed in accordance with the [EMV Integrated Circuit Card Specifications for Payment Systems]. Amended effective 21.11.17
- (b) **(Issuer Liability for Fraudulent ATM Transaction):** Each Issuer agrees to indemnify each Acquirer against direct loss which is the result of any person's fraudulent use of a Card and PIN issued by that Issuer to effect an ATM Transaction, except to the extent that:
- (i) the Issuer did not authorise the ATM Transaction; or
 - (ii) the loss can be attributed to the Acquirer's failure to comply with clause 4.5(a)(ii).
- (c) **(Liability Shift for Counterfeit ATM Transaction):** Subject to clause 4.5(d), each Acquirer agrees to indemnify each Issuer for the value amount of any Counterfeit ATM Transaction initiated and completed at the Acquirer's ATM Terminal after the Compliance Date where either:
- (i) the ATM Terminal was not EMV Compliant; or
 - (ii) the Counterfeit ATM Transaction was not processed by the Acquirer in accordance with the requirements in clause 4.5(a)(ii)(B).
- (d) **(Liability Shift Exception):** The Acquirer is not liable under clause 4.5(c) in respect of any Counterfeit ATM Transaction processed and authorised by the Issuer as a Fallback Transaction. Amended effective 21.11.17
- Note: Annexure G.5.1 sets out various ICC Card usage scenarios which could result in fallback transaction.*
- (e) **(Presumption):** Unless the Acquirer can produce satisfactory evidence that its ATM Terminal is EMV Compliant, and was so compliant at the relevant time, an Issuer who has suffered loss as a result of a Counterfeit ATM Transaction initiated and completed at the ATM Terminal is entitled to the benefit of the presumption that the Counterfeit ATM Transaction occurred because of the failure of the Acquirer to comply with the requirements of clause 4.5(a)(ii). Amended effective 21.11.17
- (f) **(Satisfactory evidence):** Satisfactory evidence for the purpose of clause 4.5(e) is the ATM Transaction Listing for the ATM Terminal on the relevant day indicating that transactions prior to and subsequent to, the Counterfeit Transaction concerned were successfully processed as EMV transactions using the AID that the Issuer advises was on the card. The Tag 9F06 in the Transaction Listing identifies the AID. Inserted effective 21.11.17

4.6 Liability Shift Claim Process

Note: An Issuer may become aware of a Counterfeit ATM Transaction as a result of a customer complaint about an unauthorised transaction or as a result of its own fraud detection programmes. A customer complaint of unauthorised transaction which is, in the Issuer's reasonable opinion, a Counterfeit ATM Transaction, is to be resolved in terms of this clause 4.6. The timeframes prescribed in this clause 4.6 are therefore intended to be consistent with the timeframes for resolution of customer complaints under the ePayments Code. They are also broadly consistent with those for resolution of Disputed Transactions as set out in Part 4 of the ATM System Code. This process utilises the Disputed Transaction File (Annexure M) but is simplified to reflect the fact that extended investigation by the Acquirer is unnecessary in the case of Counterfeit ATM Transactions claims.

Amended
effective 3.7.17

(a) An Issuer may make a claim under the indemnity given in clause 4.5(c), for the value amount of a Counterfeit ATM Transaction, by making an entry in a Disputed Transaction File in accordance with clause 4.22, adapted as follows:

Amended
effective 3.7.17

- (i) selecting the Dispute Type "Counterfeit Claim";
- (ii) entering the claim reference number in the Originating Bank Reference Number field; and
- (iii) entering the Sequence No. in the STAN (System Trace Audit Number) field.

(b) Within ten (10) Business Days of receipt of a Counterfeit ATM Transaction Claim, the Acquirer must either:

Amended
effective 3.7.17

- (i) accept and settle the claim in accordance with clauses 4.23(d) and 4.23(f); or
- (ii) refuse the claim by making the appropriate entry in a Settled Disputed Transaction File and returning it to the Issuer's claims contact together with satisfactory evidence, in the terms of clause 4.5(f), in support of the refusal.

(c) If the Acquirer:

- (i) refuses a claim under clause 4.6(b)(ii) but fails to provide satisfactory evidence, in the terms of clause 4.5(f), in support of the refusal; or
- (ii) fails to respond to the Counterfeit ATM Transaction Claim within ten (10) Business Days of the date of receipt of the *Counterfeit ATM Transaction Claim*;

Amended
effective
21.11.17

Amended
effective 3.7.17

the Issuer may then initiate a charge back against the Acquirer for the value amount of the Counterfeit ATM Transaction, by making an entry in a Disputed Transaction File with the Charge Back field set to “Yes” and the proposed date of the charge back entered in the “Charge Back Date” field and sending it to the Acquirer’s claims contact in accordance with clause 4.23(j).

Amended
effective 3.7.17

- (d) If the Acquirer refuses a claim under clause 4.6(b)(ii), the Issuer may not initiate a chargeback, but may refer the matter to dispute resolution proceedings in accordance with clause 4.7.

Amended
effective 3.7.17

4.7 Counterfeit ATM Transaction Claim - Dispute Resolution

- (a) Any disputes in respect of the application of clauses 4.5 and 4.6 of this Code shall be determined pursuant to Part 12 of the IAC Regulations.
- (b) The parties to any such dispute shall attempt to resolve it by negotiating in good faith prior to referring it to the Company for determination pursuant to Part 12 of the IAC Regulations.
- (c) For the avoidance of doubt the ATM Code Committee, IAF or Board, as the case may be, may if deemed appropriate, retain the services of one or more third parties to assist with the resolution of any dispute in respect of the application of this part.

4.8 Settlement

- (a) Each IA Participant must be able to settle ATM Transactions with all other Interchange partners by reason of being either a Direct Settler; or having appointed one or more Direct Settlers to settle on its behalf.
- (b) Each Issuer must pay the applicable Acquirer for the total net value of all ATM Transactions initiated with Cards it has issued, and which it has duly authorised in accordance with this Code.
- (c) Settlement of obligations arising between each Acquirer and each Issuer as a result of ATM Interchange must take place at least once each business day in accordance with the procedures set out in the IAC Code Volume 5 – Settlement. IA Participants are bound by the IAC Code Volume 5 – Settlement as if set out in this Code in its entirety.

4.9 Interchange Fees

- (a) Interchange Fees in respect of ATM Transactions are regulated by the ATM Access Regime. Subject to the requirements of the ATM Access Regime, the basis, rate and payment of an Interchange Fee (if any) will be as agreed from time to time bilaterally and specified in the Interchange Agreement.

-
- (b) Following receipt of Interchange billing reports (see clause 4.13), usually within one to five business days of the start of each month IA Participants which are parties to Interchange exchange acquired Transaction data by telephone and facsimile and verify and calculate net difference and agree amount due/to be paid. (This may involve some negotiations and sharing of differences). Monthly Interchange Fee reports may be exchanged to assist identification and resolution of large differences. Net fees will be settled by bank cheque, warrant, drawing voucher, or such other method as may be agreed between the parties from time to time.

4.10 Interchange Reports

- (a) Each IA Participant must ensure that all reports of the Interchange which it is required to produce for the purposes of clauses 4.11 to 4.13 contain information which:
- (i) satisfies the agreed internal audit requirements of both parties to the Interchange;
 - (ii) provides the ability to trace Items in the event of discrepancies/enquiries across the Interchange Link;
 - (iii) assists in verifying settlement figures; and
 - (iv) provides statistical information to provide a basis for calculating applicable Interchange Fees.
- (b) All ATM Transactions, whether approved, declined or cancelled that are processed through the ATM network must be reported using an ATM Transaction Listing to assist with Cardholder enquiries and balancing procedures.
- (c) Interchange Settlement Reports and Interchange Billing Reports are to be exchanged by Acquirers on an exception basis to assist with resolution of discrepancies.
- (d) The format of all reports required is left to the individual IA Participant's discretion, provided that all minimum information requirements have been met. Reports may be kept in microfiche format.

4.11 ATM Interchange Reports and Transaction Listings

Each IA Participant must, in respect of all Interchange in which it engages in that particular capacity, produce a daily ATM Transaction Listing which contains the following:

- (a) Cardholder Number
- (b) Acquirer Sequence/Trace Number (set by Acquirer Host)

Amended
effective
21.11.17

- (c) Issuer Sequence Number (set by Issuer Host)
- (d) Local Posting Date
- (e) Real Calendar Date and Timestamp of Transaction
- (f) Acquirer ATM Sequence Number
- (g) Transaction Type Performed
- (h) Amount of Transaction
- (i) Amount of any ATM Operator Fee
- (j) ATM Location
- (k) Authorisation response code
- (l) Terminal ID number

4.12 Interchange Settlement Reports (Value)

- (a) Each Acquirer must produce, in respect of each Issuer, a daily Interchange Settlement Report for the purposes of and in accordance with the IAC Settlement Code.
- (b) For reconciliation purposes, each Issuer must produce, in respect of each Acquirer, a daily Interchange Settlement Report which complies with the requirements specified in the IAC Settlement Code.

4.13 Interchange Billing Reports

- (a) Each IA Participant must produce a monthly Interchange billing report for each Interchange Agreement that provides for payment of an Interchange Fee, which specifies:
 - (i) number of ATM Transactions acquired;
 - (ii) Interchange Fee applicable to ATM Transactions acquired by that institution;
 - (iii) total sum of Interchange Fees receivable in relation to acquired ATM Transactions (derived by multiplying the number of ATM Transactions acquired, by the Interchange Fee applicable to ATM Transactions acquired by that institution);
 - (iv) number of ATM Transactions issued;
 - (v) Interchange Fee applicable to ATM Transactions issued by that institution;

- (vi) total sum of Interchange Fees payable in relation to issued ATM Transactions (derived by multiplying the number of ATM Transactions issued, by the Interchange Fee applicable to ATM Transactions issued by that institution); and
 - (vii) net settlement figure for monthly Interchange Fee.
- (b) For reconciliation purposes, each Issuer must produce an Interchange Settlement Report which complies with the requirements specified in IAC Settlement Rules.

4.14 Retention Period

Unless applicable legislation, or an IA Participant's policy, specifies a longer retention period, each of the reports produced under clauses 4.11 to 4.13 are to be held by each IA Participant for a minimum period of 12 months, in such a manner that they are capable of being retrieved within 10 business days if required.

4.15 ATM Terminal - Cards Retained

- (a) A Card which has been retained by an ATM during operation for any reason is a "Retained Card" for the purposes of this Part 4.
- (b) Where a Card has been retained by an ATM that is serviced by a branch, the branch may hold the Card for one business day following its removal from the ATM.
- (c) Where the branch staff can determine the reason for the capture of the Card, it may be returned to the Cardholder, within the above timeframe, upon successfully establishing the claimant's identity and provided that the Card was captured due to system or machine malfunction.
- (d) Where the branch staff have any doubt as to the claimant's right to the Card, the claimant should be advised to contact his or her own Issuer branch.
- (e) Where a Card has been retained at the request of the Card Issuer the Card is not to be returned to the Customer under any circumstances. This includes where a Card has been retained due to excessive PIN tries or where the Card Issuer has advised that the Card is a Hot Card or expired Card.
- (f) All Cards that have been captured and not returned to a Cardholder are to be rendered unusable (without damage to any chip on the Card) by the Acquirer and returned to the Issuer (bearing in mind the Card has a signature on it and if it is also a credit Card will have an embossed account number all of which information may be still obtainable from the destroyed Card).

4.16 Good Design Principles Applicable to ATM Terminal Interface

- (a) Acquirers need not adopt a standard Customer interface at ATM Terminals, but the selected interface, instructions and prompts must be unambiguous.
- (b) IA Participants may optionally apply the ATM Installation Guidelines set out in Annexure I to this Code.

4.17 Doubtful ATM Transactions

Amended effective
21.11.16

Inserted effective
21.11.16

In the circumstances where an Acquirer raises a possible Doubtful Transaction (i.e. an ATM Transaction where cash has been dispensed from an ATM but the withdrawal ATM Transaction has not been processed to the relevant Cardholder account), the relevant Cardholder's account will be debited (i.e. force posted) by the Issuer of the relevant Card for the ATM Transaction value within 10 Business Days of the ATM Transaction. If the Issuer does not force post the relevant ATM Transaction within 10 Business Days then the ATM Transaction cannot be force posted. The Cardholder has recourse to raise a Disputed Transaction with the Issuer of the Card if it believes the force posting is invalid. If an ATM has been cashed incorrectly this scenario will not be considered to be a Doubtful Transaction and should be dealt with by the Issuer and Acquirer bilaterally.

4.18 Doubtful ATM Transactions - Issuer Responsibilities [Deleted]

Deleted effective
21.11.16

4.19 Doubtful ATM Transactions – ATM Affiliate Responsibilities [Deleted]

Deleted effective
21.11.16

4.20 Retention of Records – Doubtful Transactions [Deleted]

Deleted effective
21.11.16

4.21 Disputed Transactions – General

- (a) Claims by the Cardholder not to have initiated or authorised an ATM Transaction must be investigated by the Issuer and resolved with the Cardholder in the manner outlined in the ePayments Code.
- (b) The Cardholder is to be required to report these disputes to the Issuer. If a Cardholder approaches the Acquirer, the Acquirer must advise the Cardholder to report the Disputed Transaction to the Issuer.
- (c) All Disputed Transactions are to be managed in the terms of the ePayments Code and this Part 4.

4.22 Disputed Transactions - Issuer's Responsibilities

Upon receiving advice of a Disputed Transaction, the Issuer must:

-
- (a) establish where the value of the Disputed Transaction is held: e.g., establish that value is not held as a result of internal error;
- (b) prepare an entry in the Disputed Transaction file, which will be in the form of an excel file, or CSV file if bilaterally agreed between members, containing the following fields, which will inform the investigation by the Acquirer “**Disputed Transaction File**” (explanation of each field is contained in the parenthesis but is not required to be included):
- (i) Originating Bank (Issuer);
 - (ii) Originating Bank reference number (Issuer reference number);
 - (iii) Card Number (Cardholder Card Number);
 - (iv) Suspense Account claim to be paid into (Issuer’s Suspense Account details);
 - (v) Terminal Number;
 - (vi) Terminal Name;
 - (vii) Transaction Date;
 - (viii) Transaction Time;
 - (ix) STAN (System Trace Audit Number);
 - (x) Amount request (Amount request in the Transaction);
 - (xi) Amount Received (Amount received by the Cardholder);
 - (xii) Difference (Difference between the amounts requested and amounts received by the Cardholder);
 - (xiii) Dispute Type (drop down field with the selection of: Shortpay; Duplication; Doubtful Transaction, Counterfeit Claim; and Rejected);
 - (xiv) Rejected Reason (Drop down field with selection of: Invalid Card Number; Invalid Terminal; or Other);
 - (xv) Charge Back (Drop down field with the selection of: Yes or No); and
 - (xvi) Charge back date (Date the Charge Back will be processed).

Amended
effective
21.11.16Amended
effective 3.7.17

The Disputed Transaction File must comply with the technical specifications set out in Annexure M to this Code (including the File Naming Convention set out in Annexure M) and is to be sent as an encrypted attachment to an e-mail transmission to the Acquirer, (contact details are found on the AusPayNet Extranet <https://extranet.auspaynet.com.au/>). The Disputed Transaction File is to be used for all Disputed Transactions raised by an Issuer on a particular Acquirer for the relevant day and therefore may contain multiple entries;

- (c) if it receives a rejected entry from an Acquirer in accordance with clause 4.23(b), resend the corrected entry in the next available Disputed Transaction File following correction of the error in the rejected entry; Inserted effective 21.11.16
- (d) if requested by the Acquirer as part of its investigations, provide to the Acquirer, the Issuer's Transaction Listing and/or Interchange Settlement Report; and Amended effective 21.11.16
- (e) grant written approval of any extension of time requested by the Acquirer in accordance with clause 4.23(h) for the purposes of its investigation. Amended effective 21.11.16

4.23 Disputed Transactions - Acquirer's Responsibilities

The Acquirer must:

- (a) confirm receipt from the Issuer of the Disputed Transaction File via return e-mail transmission. The email confirmation can be by way of automated response. If no confirmation is received from the Acquirer, the Issuer is entitled to proceed as if a response had been received from the Acquirer on that day; Amended effective 21.11.16
- (b) immediately following receipt of the Disputed Transaction File, commence validation of the Disputed Transaction File. Entries in the Disputed Transaction File that cannot be matched, validated or are otherwise considered invalid are to be dealt with as follows: Inserted effective 21.11.16
 - (i) a specific entry may be rejected by returning the entry to the Issuer. Rejected entries must be returned in an encrypted excel file (or CSV if bilaterally agreed between members) as an attachment to an e-mail transmission to the Issuer, in the same format as the Disputed Transaction File including a reason code for each rejection; and Inserted effective 21.11.16
 - (ii) rejection can be by way of automated response and must be sent immediately following validation of the Disputed Transaction File, which is to be completed as soon as possible following receipt of the Disputed Transaction File. Inserted effective 21.11.16
- (c) promptly initiate investigations through use of internal reporting mediums and, where necessary, consultation with the Issuer;

PART 4. ATM INTERCHANGE OPERATIONS

-
- (d) if the value of the Disputed Transaction is held by the Acquirer, promptly provide value to the Issuer in accordance with the Suspense Account Details instructions in the Disputed Transaction File. (Where the value has already been forwarded to the Issuer, the Acquirer should advise date and method of value processed); Amended effective 21.11.16
- (e) complete its investigation within 10 business days of receipt of the Disputed Transaction File or, in the case of a rejected entry in a Disputed Transaction File under clause 4.23(b), receipt of the invalid (not rejected) entry in a Disputed Transaction File, and promptly notify the Issuer in writing of the outcome or whether more time is required to complete its investigation; Amended effective 21.11.16
- (f) provide confirmation to the Issuer that the value of the Disputed Transaction has been settled or denied by sending to the Issuer an ATM Settled Disputed Transaction File by way of an encrypted attachment to an e-mail transmission not later than 10 business days after receipt of a Disputed Transaction File. The Settled Disputed Transaction File must include all of the same fields as in the Disputed Transaction File (specified in clause 4.22(b)) as well as the following additional fields: Amended effective 21.11.16
- (i) Amount Paid; Inserted effective 21.11.16
 - (ii) Date Payment Sent (to Issuer); and Inserted effective 21.11.16
 - (iii) Responding Bank Reference (optional), Inserted effective 21.11.16
- and must comply with the technical specifications set out in Annexure M (including the File Naming Convention set out in Annexure M). Inserted effective 21.11.16
- (g) Where the claim is denied, appropriate reports are to be provided to verify that there was no equipment or system malfunction at the time of the ATM Transaction. The reports to be provided must include at least two of the following: Inserted effective 21.11.16
- (i) a copy of the device's journal roll or its electronic equivalent including evidence of notes dispensed where appropriate;
 - (ii) a reconciliation report covering the period;
 - (iii) a statement confirming that the device in question was not in surplus at the time of the next balancing operation, subsequent to the date of the Disputed Transaction;
 - (iv) a bill counter report; Inserted effective 21.11.16
 - (v) ATM terminal balance as at the first balancing following the Transaction; and Inserted effective 21.11.16
 - (vi) other evidence that the ATM Transaction was reversed. Amended effective 21.11.16
-

- (h) The Acquirer will be granted an extension of time to complete its investigations in the following circumstances: Inserted effective 21.11.16
- (i) if the Disputed Transaction relates to an offsite or remote ATM, unserviced ATM or an ATM owned by a third party other than the Acquirer, a 10 business day extension must be granted by the Issuer provided that the Acquirer informs the Issuer of the expected date of balancing the relevant ATM. In these circumstances, the Acquirer must complete its investigation and provide confirmation to the Issuer no later than 20 business days of the initial receipt of a Disputed Transaction File; and Amended effective 21.11.16
 - (ii) if a Disruptive Event has occurred and been reported by the Acquirer by way of an IAC Operational Broadcast, a 10 business day extension must be granted by the Issuer. In these circumstances the Acquirer must complete its investigation and provide confirmation to the Issuer no later than 20 business days of the initial receipt of a Disputed Transaction File. Inserted effective 21.11.16
- (i) If the Acquirer fails to respond to the Issuer within 10 business days, or if an extension has been granted in accordance with clause 4.23(h)(i) or 4.23(h)(ii), 20 business days, the Issuer is permitted to charge back the value amount to the Acquirer. The value amount is the amount defined in the 'Difference' field of the Disputed Transaction File. This period commences on and from the date the Disputed Transaction File is taken to be received, in accordance with Step 3 in the table set out in clause 4.27. Amended effective 21.11.16
- (j) The Issuer must send an e-mail attaching the encrypted Disputed Transaction File to the Acquirer (see contact details, <https://extranet.apca.com.au/>), with the 'Charge Back' field set to 'Yes' and the proposed date of the charge back entered in the 'Charge Back Date' field. The Issuer must give 3 business days' warning of the proposed charge-back. In the case where an Acquirer has sought a 10 business day extension, in accordance with clause 4.23(h)(i) or 4.23(h)(ii), this email regarding the charge back is to be sent on or after the expiration of the 20 business day period (as applicable). In all other cases, the email regarding the charge back is to be sent on the expiration of the 10 business day period. Amended effective 21.11.16

4.24 Disputed Transactions - ATM Affiliate and Third Party Responsibilities

To the extent that any Acquirer or Issuer reasonably requires information, assistance or co-operation of an ATM Affiliate or a Third Party Provider or other person to properly investigate a Disputed Transaction, the ATM Affiliate is obliged to use reasonable endeavours to provide that information, assistance or co-operation, and the Acquirer or Issuer must otherwise ensure that it has proprietary arrangements in place to ensure that Third Party Provider or other person is obliged to provide such information, assistance or co-operation.

4.25 Re-presentation

- (a) Re-presentation by the Acquirer is allowed only if:
- (i) the charge-back by the Issuer is improper or invalid;
 - (ii) Cardholder received the requested Cash; or
 - (iii) the Acquirer has processed an adjustment for the disputed ATM Cash disbursement.
- (b) Re-presentation must be received by Issuer within 10 business days of the charge-back, otherwise it will not be valid.

Amended
effective
21.11.16**4.26 Retention of Records – Disputed Transactions**

All Interchange parties are to maintain details of Disputed Transactions for at least 12 months.

4.27 Timing

- (a) Timing for processing of Disputed Transactions is governed by the requirements of the ePayments Code and by the requirements of this Framework. A summary of resolution steps and associated time frames for resolution of Disputed Transactions is set out below. A detailed illustration of the process for resolution of Disputed Transactions is set out in Annexure N.

Amended
effective
21.11.16

(Note: Currently the ePayments Code requires the Issuer to advise the Cardholder within 21 days of a receipt of a complaint either of the outcome of the investigation or the need for more time to complete the investigation. Unless there are exceptional circumstances which the Issuer advises to the Cardholder in writing, the ePayments Code requires the Issuer to complete its investigation within 45 days of receipt of the complaint. Times stipulated below are intended to enable Issuers to be in a position to meet their obligations under the Code, however Framework Participants are required to comply with the shorter timeframes stipulated in this Part 4 rather than the timeframes for complaints stipulated in the ePayments Code, in relation to Disputed Transactions).

Amended
effective
21.11.16

| Issuer | Acquirer | Time Frame |
|---|----------|-------------------------|
| 1. Issuer receives Cardholder complaint (ePayments Code – Day 1). | | |
| 2. Sends Disputed Transaction File to Acquirer. | | As soon as practicable. |

Amended
effective
21.11.16

PART 4. ATM INTERCHANGE OPERATIONS

| | | |
|--|--|---|
| | <p>3. Confirm receipt and “received on” date: if received before 10am on a business day then this will be IAC Code Set – Business Day 1. If received after 10am on a business day, or received at any time on a day that is not a business day, then IAC Code Set – Business Day 1 will be the next business day following date of receipt.</p> <p>In the case of a rejected entry in a Disputed Transaction File, the “received on date” calculated by reference to when the valid (not rejected) entry in a corrected Disputed Transaction File is received.</p> | On receipt of the Disputed Transaction File. |
| | 4. Investigate and resolve if possible. | Prior to IAC Code Set – Business Day 10, i.e., IAC Code Set Day 1 plus 9 business days. |
| | 5. Send Issuer Settled Disputed Transaction File and process payment and/or request a 10 business day extension if conditions for extension met. | On or prior to IAC Code Set – Business Day 10. |
| 6. Advise Cardholder of final outcome (if Acquirer has sent Settled Disputed Transaction File) or current status if an extension has been granted. | | On IAC Code Set – Business Day 10 (which will be before ePayments Code Day 21, i.e., ePayments Code – Day 1 plus 20 calendar days). |

| | | |
|--|---|---|
| 7. Initiate charge back by sending Disputed Transaction File to Acquirer with charge back details – if appropriate. | | On IAC Code Set – Business Day 11. |
| 8. Post charge back and advise Cardholder of final outcome. | | On IAC Code Set – Business Day 14. |
| | 9. If 10 business day extension has been granted – Send Issuer Settled Disputed Transaction File and process payment. | On IAC Code Set – Business Day 20. |
| 10. 10 business day extension – Advise Cardholder of final outcome (if Acquirer has sent Settled Disputed Transaction File). | | On IAC Code Set – Business Day 20. |
| 11. 10 day business extension – Initiate charge back by sending Disputed Transaction File to Acquirer with charge back details – if appropriate. | | On IAC Code Set – Business Day 21. |
| 12. 10 business day extension – Post charge back and advise Cardholder of final outcome. | | On IAC Code Set – Business Day 24 (which will be before ePayments Code – day 45). |

4.28 Enquiries and Notification of System Outages

- (a) Enquiries relating to Cardholders' ATM Transactions are to be directed to the Issuer.
- (b) Enquiries relating to Cardholder disputes/queries should be directed to the appropriate contact in <https://extranet.auspaynet.com.au/>.
- (c) Enquiries regarding settlement matters and any related discrepancies are to be directed to the appropriate contact in <https://extranet.auspaynet.com.au/>.

- (d) Both parties to an Interchange are to advise each other of any scheduled or unscheduled downtime. All problems resulting in unscheduled downtime and general enquiries regarding the Interchange Link problems are to be directed to the appropriate contact in <https://extranet.auspaynet.com.au/>.
- (e) In the event that either institution has scheduled downtime resulting in the Interchange Link being unavailable, a written advice is to be sent prior to this advising the date and approximate commencement and completion times. This advice is to be directed to the appropriate contact in <https://extranet.auspaynet.com.au/>.
- (f) In the event of unscheduled outages, Framework Participants will apply the escalation procedures set out in Annexure H (Escalation Procedures).

4.29 Management of System Outages – Operational Broadcast

- (a) Framework Participants may provide operational advice to other Framework Participants by issuing an operational broadcast using the Company's extranet ("Operational Broadcast").
- (b) The Operational Broadcast form is an online form which can be accessed, completed and sent by Framework Participants using AusPayNet's extranet.
- (c) The Operational Broadcast form may be used to notify other Framework Participants or Non-Framework Participants about:
 - (i) unscheduled network outages;
 - (ii) scheduled network outages;
 - (iii) to facilitate the exchange of general operational information relevant to network operations; or
 - (iv) Disruptive Events.
- (d) Operational Broadcast forms may be completed by Framework Participants and submitted to AusPayNet during business hours (Monday to Friday 8.30 am to 5.30 pm) for action.
- (e) AusPayNet will process the Operational Broadcast form during business hours, and broadcast as requested in the "Communication Process" section of the form.

- (f) An Operational Broadcast about a Disruptive Event must include the following information: (1) the time when the Disruptive Event commenced or is expected to commence; (2) the time when normal processing is expected to resume or resumed; and (3) the current status of the Disruptive Event.

4.30 Notification of a Disruptive Event

An IA Participant that experiences a Disruptive Event must notify the Company as soon as possible. Notification of a Disruptive Event shall be given to the operational contacts listed at <https://extranet.auspaynet.com.au> and subsequently by an Operational Broadcast.

Next page is A.1

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

A.1 Standard Interchange

- (a) This Annexure A sets out the interchange specifications required to be met by all IA Participants, to the extent applicable to the capacities in which they participate (or are deemed to participate) in Interchange.
- (b) Although it is not necessary that all Interchanges engaged in by IA Participants and Non-Members conform to this specification, it is a requirement that all IA Participants are capable of supporting this interface and it is to be used where bilateral agreement cannot be reached.
- (c) As this specification is taken from the previous version of the CECS Manual (in force until 30 June 2015) it contains elements that are unnecessary for an ATM only interchange. These elements have been retained as a transition measure only.

A.2 Purpose

The purpose of this Annexure A is to define the standard message set capable of supporting the range of Interchange Transactions arising from Card-originated, debit Transactions and associated interactive message traffic between IA Participants.

A.3 Scope

- (a) The scope of this Annexure A is to specify IAC requirements for debit authorisation Interchange in sufficient detail to allow construction and implementation of the required interface (see also Part 2).
- (b) The message specifications given in this Annexure A are based on the Australian Standard, AS2805 Electronic funds transfer - Requirements for interfaces. The requirements of this specification take precedence over those of the AS2805 standard if any contention arises during the implementation of an interface using this specification.

A.4 References

The following documents are referred to in this Annexure A:

- (a) AS2805.2-2007/Amdt 2-2008 Electronic funds transfer - Requirements for interfaces Part 2: Message structure, format and content
- (b) AS2805.4.1-2001/Amdt 1/2006 Electronic funds transfer - Requirements for interfaces Part 4.1: Message authentication - Mechanism using a block cipher

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (c) AS2805.6.3-2000/Amdt 1/2003 Electronic funds transfer - Requirements for interfaces Part 6.3: Key management - Session Keys - Node to node
- (d) AS2805.6.1-2002/Amdt 3/2007 Electronic funds transfer - Requirements for interfaces Part 6.1: Key management - Principles Amended effective 27.04.11
- (e) AS2805.16 Electronic funds transfer - Requirements for interfaces Merchant Category Codes
- (f) AS2805.6.6- 2006 Electronic funds transfer - Requirements for interfaces Part 6.6: Key management – Session Keys – Node to node with KEK replacement.

A.4.1 Normative references

Unless specifically identified otherwise, the terms, definitions and specifications contained in the referenced publications given in clause A.4 are normative to this specification.

Amended
effective
21.11.17

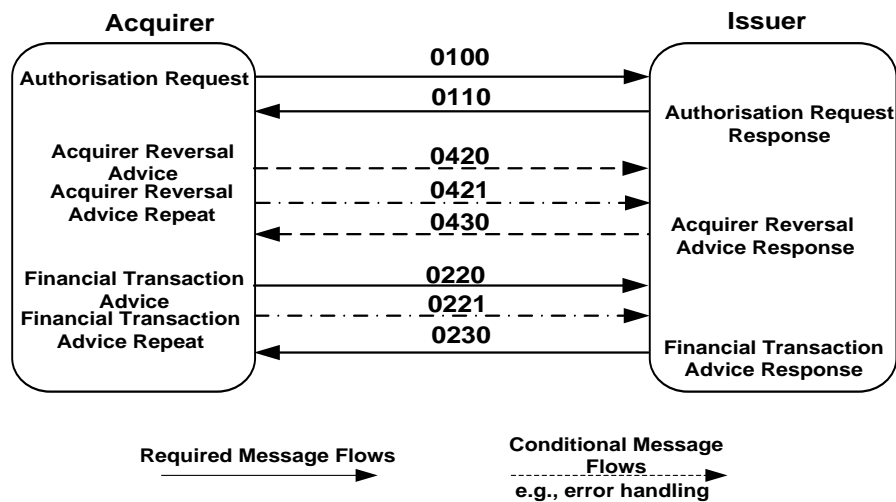
A.5 Supported Message Types

| Request | Response | Description |
|---------|----------|---------------------------------------|
| 0100 | 0110 | Authorisation Request |
| 0200 | 0210 | Financial Transaction Request |
| 0220 | 0230 | Financial Transaction Advice |
| 0221 | 0230 | Financial Transaction Advice Repeat |
| 0420 | 0430 | Acquirer Reversal Advice |
| 0421 | 0430 | Acquirer Reversal Advice Repeat |
| 0520 | 0530 | Acquirer Reconciliation Advice |
| 0521 | 0530 | Acquirer Reconciliation Advice Repeat |
| 0800 | 0810 | Network Management Request |
| 0820 | 0830 | Network Management Advice |

A.6 Supported Transaction Set

A.6.1 Pre-authorised Transaction

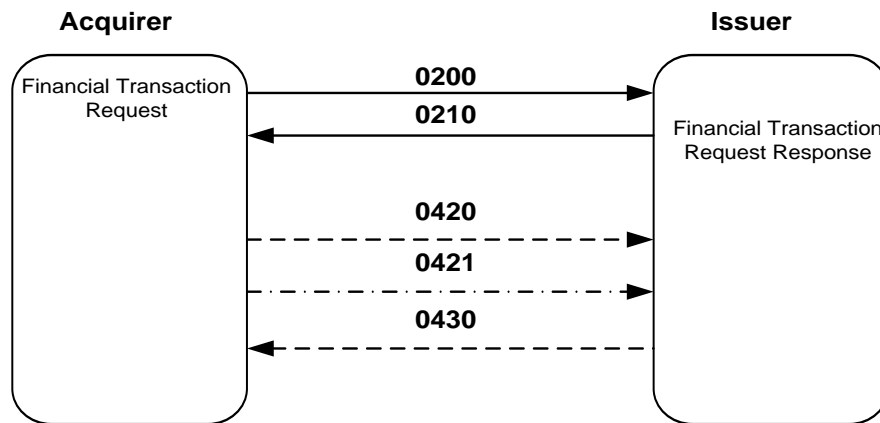
- (a) A pre-authorised Transaction is a two-phase Transaction. An authorisation request (message type 0100) is used by the Card acceptor for the approval or guarantee of funds from the Card Issuer or their agent. If an authorisation request is approved it is not to be debited against the Cardholder's account, which will be performed by the Financial Transaction Advice (message type 0220) that may follow.
- (b) The Issuer may put a temporary hold on the Cardholder's account for the amount authorized. In the absence of the 0220 Advice Message (or a reversal of the pre-authorization) that completes the Transaction, the lifetime of the pre-authorization request shall not exceed 24 hours.
- (c) Pre-authorization Transactions are generated from devices such as fuel dispensers and Card-activated phones. The Transaction is used where the Merchant or Terminal does not know the final cost of the goods or services to be provided. The authorisation message will contain the maximum amount that the Terminal is able to dispense. The Pre-authorization response message will contain the Issuer authorised amount for this Transaction. This value may be less than the requested value.
- (d) The Financial Transaction Advice that completes the Transaction must be for a value equal to or lower than the amount for which the authorisation was approved.



- (e) If the amount of the advice is greater than the amount authorised, the Transaction may be rejected by the Issuer.
- (f) For Acquirer Reversal Advice messages the amount field must contain the same value as in the original Authorisation Request message.

A.6.2 Balance Enquiry Transaction

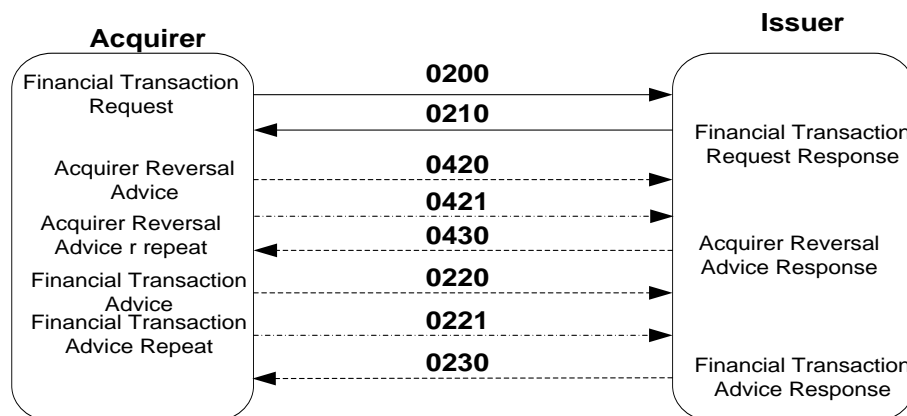
- (a) A Balance Enquiry Transaction requests the Issuer to provide information about the current balance and available (cleared) funds of an account linked to the Card. The Transaction has no financial impact on the account, other than fees that may arise from the execution of the Transaction.
- (b) A balance enquiry Transaction uses a “Financial Transaction Request” message (0200)



- (c) Acquirer Reversal Advice (0420) messages are used to handle error conditions arising from the inability to complete the Transaction for example, failure to print a receipt if requested, timeouts etc.

A.6.3 Cash Withdrawal Transaction

- (a) A Cash Withdrawal Transaction is used by an Acquirer to request authorisation from the Card Issuer to complete a Cardholder initiated withdrawal request at a Terminal.

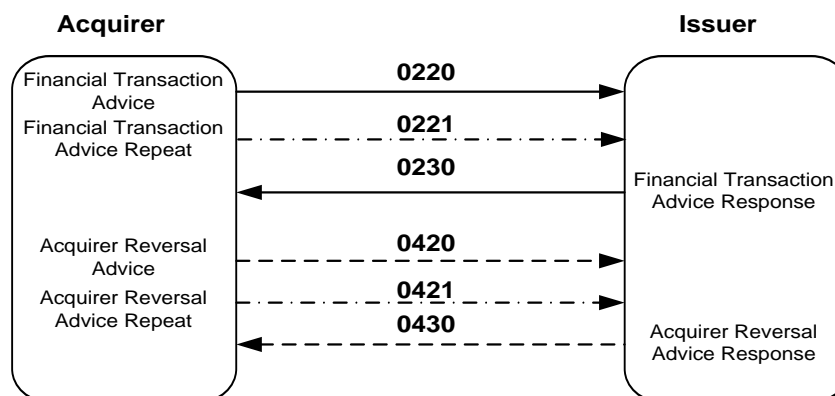


ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (b) The approval issued by the Issuer must be for the total amount of the request; approval of partial amounts is not supported.
- (c) The “Acquirer Reversal Advice” must be for the full amount contained in the request.
- (d) In the case where a partial dispense occurs, only for ATM Transactions, the Acquirer must send a “Reversal Advice” message for the full amount of the original “Financial Transaction Request” message, followed by a “Financial Transaction Advice” message for the amount of the actual dispense.

A.6.4 Fall-Back Transaction

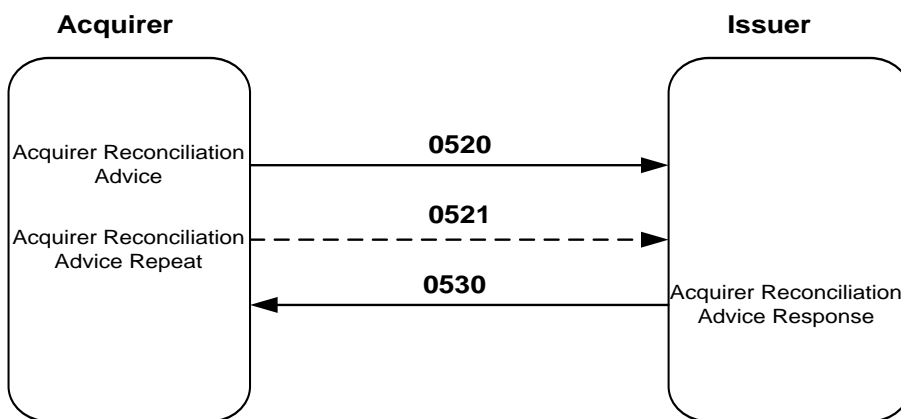
- (a) Fall back Transactions are used when there is a failure to process an EFTPOS Transaction on line. The failure could be at the Merchant’s device, the Merchant to Acquirer link or the Interchange.
- (b) There are four specific fall-back modes for ICC originated Transactions namely:
 - (i) Chip Fall-back: occurs where the Transactions rules require online authorisation and the Terminal is unable to go online. Transaction processing proceeds in accordance with the Issuer and Terminal default processing rules (EMV default processing);
 - (ii) Technology Fall-back: occurs when due to a fault of either the ICC or the IFD, the Terminal is unable to retrieve data from the chip. Fall-back is to magnetic-stripe;
 - (iii) Manual Entry: occurs when the Terminal is unable to retrieve Card data from both the ICC and the magnetic-stripe;
 - (iv) Fall-back Override refers to the situation where, when in Chip Fall-back, the ICC returns a decline, and where the Merchant, under certain specified conditions, chooses to override the result.
- (c) For additional details see Annexure B (Technology Fallback).



- (d) A reversal message may be sent when the Terminal fails to receive a 0230 “Financial Transaction Advice” response or when the Terminal fails to authenticate the 0230 response message.

A.6.5 Reconciliation Transaction

- (a) Reconciliation Transactions are used between two end points of a link to confirm the number and value of financial Transactions that have been approved since the last reconciliation process occurred.
- (b) For Acquiring nodes, the reconciliation totals must not be updated until the financial Transaction response message is received from the Issuing node with an approval action code.
- (c) Separate reconciliation totals and processing is required for each interface between nodes.
- (d) A sending node must maintain a set of reconciliation totals for each reconciliation date that the node is currently using in messages being sent. Similarly, the receiving node must maintain reconciliation totals for each date that it is receiving.
- (e) Each node must support reconciliation dates of the current date, plus the following day. Transactions with reconciliation dates that do not match one of these two dates may be rejected by the receiving system.
- (f) In the case of bi-lateral links (both acquiring and issuing) separate reconciliation totals must be maintained for messages sent and for those received i.e., they must not be netted.



A.6.6 Declined ICC Transactions

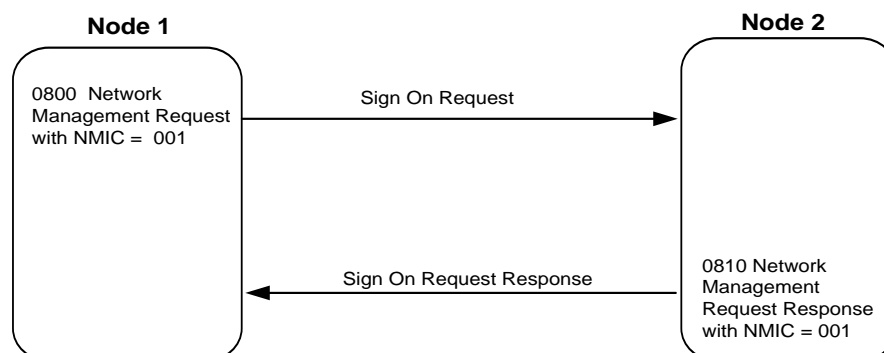
- (a) For ICC originated Transactions a declined Transaction is any Transaction where the Issuer sends, or where an ICC responds with, a response within the permitted response time, declining the Transaction for reasons which may include but are not limited to, PIN errors, account errors and insufficient funds.
- (b) Where the Transaction is declined by the ICC (AAC returned), the declined Transaction is not to be forwarded to the Issuer, except where the merchant chooses to override the Card decision in which case the fallback indicator “FBKO\” must be included in the 0220 Advice message sent to this Issuer indicating that the override has occurred.

A.7 Network Management

- (a) Network management involves the initial and ensuing dialog between the applications running at both end of the Interchange Link, which are required to start and maintain the reliable and secure flow of financial messages. It includes messages to establish and restore communications at the application layer (session establishment), the exchange of security keys, verification of link status and session termination by either node.
- (b) Network Management Transactions include link “Sign On/Off, Key Change Requests as well as link status (echo) requests.
- (c) A Sign On request must precede any other message type on a link and must be immediately followed with a Key Change Advice.

A.7.1 Sign On Request

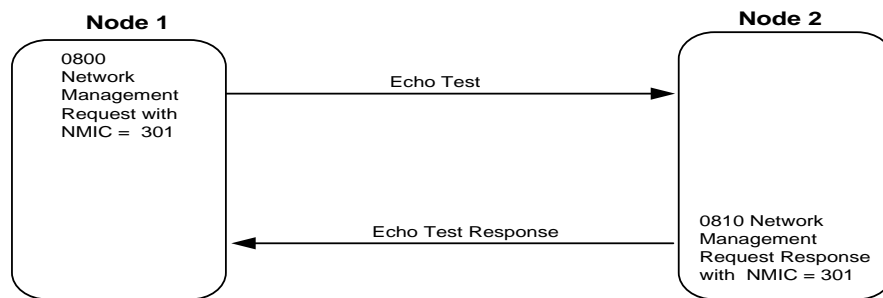
- (a) A “Sign On” request is used by a node to request permission from the receiving node to transmit financial messages. A “Sign On” is unidirectional and each endpoint is required to “Sign On” independently.
- (b) A “Sign On” request performs proof-of-endpoint processing as described in clause A.8.4.



- (c) A “Sign On” request must precede any other message type on a link and, if successful, be immediately followed by a Key Change Request.

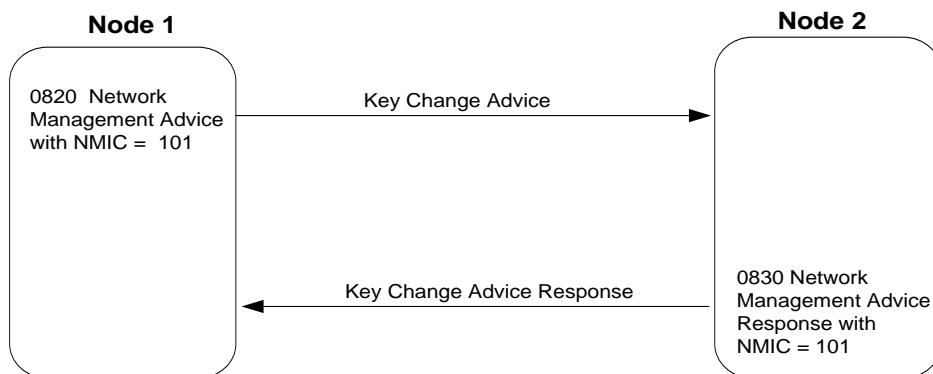
A.7.2 Echo Test

- (a) Echo Test Transactions are used by both nodes of a link to ensure that the other node is receiving messages and responding at an application's level. They do not indicate that the link is available for use. These Transactions can be sent at any time once session keys have been established, that is subsequent to a successful Key Change Transaction.
- (b) They must be sent where no activity has occurred on the link during the preceding sixty seconds and the link is in the signed on state.



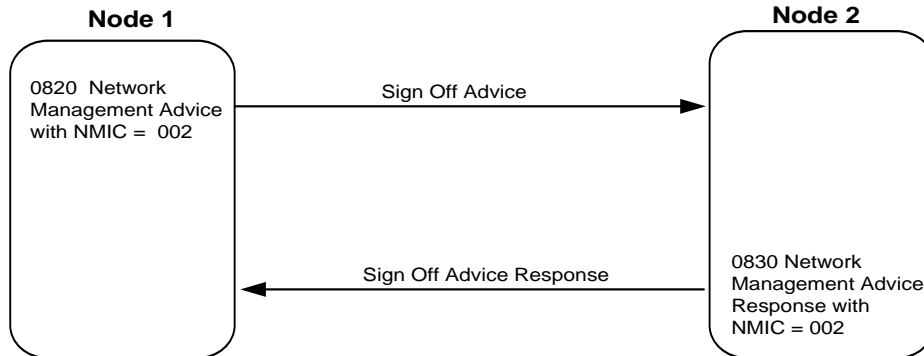
A.7.3 Key Change Advice

A Key Change Advice is required after each successful Sign On, and subsequently at intervals not exceeding one hour or the transmission of 256 financial Transactions, to establish the session keys to be used for MAC generation/verification and PIN encipherment/decipherment as described in clause A.8.3.



A.7.4 Sign Off Advice

A Sign Off Advice is used by either node to terminate the transmission of financial messages in both directions.



A.8 Key Management

This clause A.8 describes the Interchange key management and exchange process using DEA 3 (128-bit) KEKs (Key Enciphering Keys) with proof of end-point capability. Reference can be made to AS 2805.6.3 or AS2805.6.6.

A.8.1 AS 2805 Conformance

Key Management will conform to AS 2805.6.1.

A.8.2 Interchange Key Encrypting Keys

- (a) Each interchange node will contain an Interchange Send Key Encrypting Key (KEKs) and an Interchange Receive Key Encrypting Key (KEKr). The Interchange Send KEK will be the same key as the Interchange Receive KEK in the partnering node, similarly the Interchange Receive KEK will be the same as the Interchange Send KEK in the partnering node. The manner by which these keys are generated and installed must be agreed between the partners and employ one of the methods identified in IAC Code Set Manual Volume 4 (Device Requirements and Cryptographic Management).
- (b) The Interchange Key Encrypting Keys are used to encipher and decipher the session keys when they are transmitted between the nodes and in the proof of end points process.
- (c) Interchange Key Encrypting Keys must be Statistically Unique and must be changed, at a minimum, once every two years.

Amended
effective 1.1.16

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| NODE A | | NODE B |
|---|---|--|
| Interchange Key Encrypting Key, send (KEKs) | = | Interchange Key Encrypting Key, receive (KEKr) |
| Interchange Key Encrypting Key receive (KEKr) | = | Interchange Key Encrypting Key send (KEKs) |

A.8.3 Session Keys

- (a) Each node keeps four sets of session keys, two send sets and two receive sets.
- (b) Each set of session keys consists of three keys, MAC Key, PIN Protect Key and optionally a Data Enciphering Key. Each session key is 128-bits long and stored in a secure manner.
- (c) The send session key sets are generated by the sending node and numbered "1" or "2". The send session key sets are then forwarded to the receiving node to be used as the receive session key sets.
- (d) The receive session key sets are received in a 0820 Network Management Advice message with bit 070 equal to 101 from the sending node. The set number of either "1" or "2" contained in bit 53 indicates the receive session key set used by the receiving node to verify the MAC, decipher the data and translate or verify the PIN.
- (e) One set of send session keys is used at a time and all Transactions sent from the sending node will generate the MAC and encipher the PIN, if present, using the MAC Generator Key and PIN Protect Key, respectively, from the same send session key set. The send session key set used is indicated by bit 53 (contains "1" or "2") in each message.
- (f) Session Keys must be statistically unique and replaced, at a minimum, once every hour or on every 256 Transactions, whichever occurs first.
- (g) The Data Encipherment Key is unused. The Data Encipherment Key may optionally be included in the Key Change Message (see Network Management Key Change Advice message format (clause A.12.17) and clause A.13.6).
- (h) When enciphered for transmission, each session key type will use a unique variant of the Key Encrypting Key in accordance with AS 2805.6.1.

Amended
effective
21.11.17

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| NODE A | | NODE B |
|---------------------------------|---|---------------------------------|
| Send Session Keys Set 1 | | Receive Session Keys Set 1 |
| • MAC Key (KMACs1) | = | • MAC Verification Key (KMACr1) |
| • PIN Protect key (KPEs1) | = | • PIN Protect key (KPEr1) |
| • Data Encipherment Key (KDs1) | = | • Data Decipherment Key (KDr1) |
| Send Session Keys Set 2 | | Receive Session Keys Set 2 |
| • MAC Key (KMACs2) | = | • MAC Verification Key (KMACr2) |
| • PIN Protect key (KPEs2) | = | • PIN Protect key (KPEr2) |
| • Data Encipherment Key (KDs2) | = | • Data Decipherment Key (KDr2) |
| Receive Session Keys Set 1 | | Send Session Keys Set 1 |
| • MAC Verification Key (KMACr1) | = | • MAC Key (KMACs1) |
| • PIN Protect key (KPEr1) | = | • PIN Protect key (KPEs1) |
| • Data Decipherment Key (KDr1) | = | • Data Encipherment Key (KDs1) |
| Receive Session Keys Set 2 | | Send Session Keys Set 2 |
| • MAC Verification Key (KMACr2) | = | • MAC Key (KMACs2) |
| • PIN Protect key (KPEr2) | = | • PIN Protect key (KPEs2) |
| • Data Decipherment Key (KDr2) | = | • Data Encipherment Key (KDs2) |

A.8.4 Establishing a Link

- (a) A link must be established using the 0800/0810 Network Management Messages with a NMIC of “Sign On” (001). Each side must be successfully Signed on before a session can be established.
- (b) A proof of endpoints check is part of the sign on process.
- (c) A Random number (RNs) is generated along with its inverted form (RNr) both are enciphered under KEKs. The enciphered RNs is forwarded to the interchange partner in Data Element 48 of the logon request. The enciphered RNr is stored awaiting the logon response.
- (d) The interchange partner will, on receipt of the sign on request, generate the inverted form of the enciphered RNs received (RNr) and return it, enciphered by KEKr, in the sign on response. The enciphered RNr must be forwarded in Data Element 48.
- (e) On receiving the sign on response, the enciphered RNr in the message is compared with the stored version of enciphered RNr. If the two values match, proof of endpoints is established.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (f) Following these messages the key change messages establish the current session keys. Then, and only then, can other Transactions be processed.
- (g) Following is an example of the message flow to establish a link showing the key set used. The terms "send" and "receive" are from Node A's viewpoint.

| NODE A | | NODE B |
|-------------------------------|---|----------------------------------|
| 0800 (Sign On) | ⇒ | |
| | ⇐ | 0810 (Sign On Reply) |
| | ⇐ | 0800 (Sign On) |
| 0810 (Sign On Reply) | ⇒ | |
| 0820 (Key Change, Send Set 1) | ⇒ | |
| | ⇐ | 0830 (Key Change Reply) |
| | ⇐ | 0820 (Key Change, Receive Set 1) |
| 0830 (Key Change Reply) | ⇒ | |
| | ⇐ | 0200 (Receive set 1 keys) |
| 0210 (Send set 1 keys) | ⇒ | |
| | | |
| etc. | | etc. |

A.8.5 Changing Session Keys

The method of session key changes is detailed below:

- (a) While one set of send session keys is being used, the other send session key set is randomly generated by the sending node and their KVCs generated, the keys are then enciphered under the Interchange Send KEK and transmitted to the receiving node in a 0820 "Network Management Advice" message.
- (b) When a 0820 message is received by the receiving node, the session keys are deciphered using the Interchange Receive KEK. These deciphered keys are set up as the set of receive keys specified by the set number contained in bit 53 of the 0820 message. The Key Verification Codes (KVCs) are calculated by the receiving node and transmitted to the sending node in bit 48 of the 0830 message.

- (c) When the 0830 “Network Management Advice” response message is received at the node initiating the key change, the KVCs contained in the 0830 message are validated. If the KVCs are correct, the new send session key set can be used immediately. If the KVCs are invalid, new send session key set must be generated and the whole process is repeated.

A.8.6 Sign Off

Either node may terminate the transmission of financial messages by sending a “Sign Off” advice. A “Sign Off” is accomplished by the transmission of a “Network Management Advice Message” with a Network Management Information Code equal to 002.

A.8.7 Key Change During Normal Processing

A session key change can occur at any time; each node independently initiates the change of their send keys. The sender will advise their sending session keys to the receiver using a 0820 “Network Management Advice” message with a NMIC for key change (101). Once a valid response (0830 message) is received and the KVCs confirmed, the new keys can be used.

A.9 Time Out Parameters

Link timeouts must conform to clause 3.1.

A.10 Link Reconciliation

- (a) Link Reconciliation will be effected by the receipt of a Reconciliation Advice Message initiated by a link end-point, typically the Acquirer, once in every 24-hour period. This message contains the sender's totals (counts and the value if appropriate) of financial and other Transactions that have occurred on the link since the previous Link Reconciliation.
- (b) The receiving party, typically the Issuer, acknowledges the Advice by sending a “0530” Reconciliation Advice Response message that contains its own totals of the Transactions that it has received in the settlement period.

A.10.1 Link Reconciliation Requirements

Link Reconciliation must comply to the following:

- (a) Only 0520/0521 reconciliation advice messages and 0530 reconciliation response messages must be used in the reconciliation process;
- (b) Only one reconciliation advice message per logical interchange must be sent by the Acquirer or intermediate network node, every calendar day;

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (c) The reconciliation advice message must contain all the totals for that link;
- (d) The transmission of the reconciliation advice message must indicate the end of the reconciliation period for that Acquirer or intermediate network facility;
- (e) The reconciliation messages must not be used as the sole basis of financial settlement;
- (f) Field 15, Date Settlement usage must be as follows:
 - (i) the Acquirer, or intermediate network facility, is responsible for setting this field for all Transactions being forwarded and may change the value of the field in order to forward a Transaction. All Transactions (requests and advices) must contain a Date Settlement field value greater than that contained in previous reconciliation advice messages across that link. The Acquirer or intermediate network facility, may start sending financial messages with the following day's Date Settlement before closing the current reconciliation period;
 - (ii) the institution receiving a message may reject a Transaction if the Date Settlement field contains a date prior to, or more than one day in advance of, the current reconciliation date;
 - (iii) all repeat Transactions must contain the same settlement date as their original (unrepeated) Transactions;
- (g) The reconciliation advice messages may be placed in a store and forward file with the aim of sending all previous advice messages with the appropriate date prior to sending the reconciliation message;
- (h) To ensure that all Transactions are completed prior to sending the reconciliation advice message, the reconciliation advice message should not be formatted nor sent for at least the time of the timeout period and preferably for at least two minutes, after the link settlement date has changed for a link (cutover);
- (i) Where two related Transactions (e.g., an original request and its reversal or a pre-authorization and its completion advice) are transmitted either side of cutover time, the two Transactions must contain different dates in their Date, settlement fields;
- (j) Advice messages must be added to the settlement totals only once, when they are first sent;
- (k) Reversal messages must be added to the settlement totals only when the original Transaction has also been added.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

A.11 Link Settlement Times

Link Reconciliation, for the day of reconciliation must be effected on or by 22:00 hours, or other such time as may be mutually agreed.

A.12 Message Formats

- (a) Full specifications for the messages and fields described herein are to be found in AS 2805.2. The specifications and requirements of AS 2805.2 are taken to apply unless specified otherwise in this clause A.12.
- (b) The presence of a mandatory field is indicated by the letter 'M' in the right most columns in the following tables. Conditional fields are indicated by the letter 'C' and optional fields by the letter "O".

A.12.1 0100 Authorisation Request Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--------------------------|--------|----|--|----------------|
| --- | Message Type | n | 4 | '0100' | |
| --- | Bit Map Primary | b | 64 | | |
| 003 | Processing Code | n | 6 | Digits 1&2 = '00' for Pre-authorisation, Digits 3&4 = '10' if from Savings A/C, '20' if from Cheque A/C, Digits 5&6 = '00'. | M |
| 004 | Amount Transaction | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc'. | M |
| 007 | Transmission Date & Time | n | 10 | Sender's message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit No. | n | 6 | A number assigned by the Card acceptor that uniquely identifies a Transaction at a Terminal for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 012 | Time, Local Transaction | n | 6 | DEVICE Time in the format 'HHMMSS'. | M |
| 013 | Date, Local Transaction | n | 4 | DEVICE Date in the format 'MMDD'. | M |
| 015 | Date, Settlement | n | 4 | Acquirer's Reconciliation Date having the format 'MMDD'. | M |
| 018 | Merchant's Type | n | 4 | Merchant Category Code see AS 2805.16 | M |
| 022 | POS Entry Mode | n | 3 | Permissible values '021' - Magnetic Stripe with PIN Entry capability, or '051' - Integrated Circuit Card with PIN Entry capability, or '071' - Contactless Integrated Circuit Card with PIN entry capability. | M |
| 023 | Card Sequence Number | n | 3 | If available, this data should be included | C ³ |
| 025 | POS Condition Code | n | 2 | A limited subset of the codes provided in AS 2805.2 is supported. See clause A.13.3. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|---|----------------|
| 032 | Acquiring Institution Identification Code | n | ..11 | The Acquirer's, Issuer identification number (IIN) issued by ISO through Standards Australia. (see AS 2805.2, clause 4.4.6) | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Acquirer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C |
| 035 | Track 2 Data | z | ..37 | Card Track 2 data field having the format: 'LLTrack2 data' where 'LL' is the data length. | M ⁵ |
| 037 | Retrieval Reference Number | an | 12 | Reference number supplied by the Card acceptor, that remains unchanged for the life of the Transaction, for example the STAN plus transmission time, formatted as SSSSSSHMMSS | M |
| 042 | Card Acceptor Identification Code | ans | 15 | A code uniquely identifying a Merchant location (see AS 2805.2, E3.3 and appendix F) | M |
| 043 | Card Acceptor Name/ Location | ans | 40 | DEVICE location description, formatted as described in clause E6 of AS 2805 part 2. | M |
| 047 | Additional Data, National | ans | ...999 | Terminal Capability Code (see AS 2805.2, 4.4.25.21 and conditionally Card Check value see 0. | M |
| 048 | Additional Data Private | ans | ...999 | Acquiring DEVICE State Code – 'n'. Refer clause A.13.7. | O |
| 052 | PIN Data | b | 64 | PIN encrypted by the PIN Session key. | C ² |
| 053 | Security Related Control Information | N | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 055 | Integrated Circuit Card related data | b | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | C ⁴ |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. | M |

Notes:

1. *This message is used in support of the Pre-authorization Transaction in unattended environments e.g., fuel pumps and card phones. Manual entry of Card details is not supported.*
2. *Required for magnetic-stripe originated Transactions if field 035 present (Card swiped). Not required for ICC originated Transactions if the 'off-line PIN validated by the Card' CVM was used.*
3. *From TAG 5F34 for ICC originated Transactions.*
4. *Not required for magnetic-stripe originated or EMV Phase 1 Transactions.*

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

5. From TAG 57 for ICC originated Transactions.

A.12.2 0110 Authorisation Request Response Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|----------------|
| --- | Message Type | n | 4 | '0110' | |
| --- | Bit Map Primary | b | 64 | | |
| 003 | Processing Code | n | 3 | Echoed from the Financial Transaction Request ('0100') message. | M |
| 004 | Amount Transaction | n | 12 | Issuer approved Transaction limit. | M ³ |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Financial Transaction Request ('0100') message. | M |
| 015 | Date, Settlement | n | 4 | Echoed from the Financial Transaction Request ('0100') message | M |
| 032 | Acquiring Institution Identification Code | n | ..11 | Echoed from the Financial Transaction Request ('0100') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Issuer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C ¹ |
| 038 | Authorisation id Response | an | 6 | An Issuer assigned code indicating approval. | C ² |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | Echoed from the Financial Transaction Request ('0100') message. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | Echoed from the Financial Transaction Request ('0100') message. | M |
| 047 | Additional Data, National | ans | ...999 | Card Check Value response code, see appendix C and AS 2805.2, clause 4.4.25.3. | C |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 055 | Integrated Circuit Card related data | b | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | O ⁴ |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. | M |

Notes:

1. Required if field present in associated 0100 Request message.
2. Required if request approved, may be omitted otherwise.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

3. *Must contain zeroes if request is not approved.*
4. *Not required for magnetic-stripe originated or EMV Phase 1 Transactions or where not provided by the Issuer.*

A.12.3 0200 Financial Transaction Request Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | | |
|-----|--------------------------|--------|------|--|----------------|----------------------------|
| --- | Message Type | n | 4 | '0200' | | |
| --- | Bit Map Primary | b | 64 | | | |
| 002 | Primary Account Number | n | ..19 | PAN having the format: 'LLPAN data' where 'LL' is the data length | C ¹ | |
| 003 | Processing Code | n | 6 | Transaction (Digits 1&2) = '00' for Goods & Services '01' for Cash Withdrawal '09' for Goods & Services with Cash '20' for Refund of Goods & Services '21' for Deposits '31' for Balance Enquiry Source Account (Digits 3&4) = '00' if sub-field unused, '10' if from Savings A/C, '20' if from Cheque A/C, '30' if from a Credit facility10. Destination Account (Digits 5&6) = '00' if sub-field unused, '10' if to Savings A/C, '20' if to Cheque A/C, '30' if to a Credit facility10. See AS 2805.2, clause 4.4.11, only the mentioned codes are supported. | M | Amended effective 21.11.17 |
| 004 | Amount, Transaction | N | 12 | Total Amount in format \$\$\$\$\$\$\$\$cc | M ⁷ | |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M | |
| 011 | Systems Trace Audit No. | n | 6 | A number assigned by the Card acceptor that uniquely identifies a Transaction at a Terminal for at least one calendar day and remains unchanged for the life of the Transaction. | M | |
| 012 | Time, Local Transaction | n | 6 | DEVICE Time in the format 'HHMMSS'. | M | |
| 013 | Date, Local Transaction | n | 4 | DEVICE Date in the format 'MMDD'. | M | |
| 014 | Expiry Date | n | 4 | 'YYMM', Card expiry date Where the PAN is manually entered and the data unavailable, this field may be omitted. | C ² | |
| 015 | Date, Settlement | n | 4 | Acquirer's Business Date having the format 'MMDD' | M | |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|-------------------|
| 018 | Merchant's Type | n | 4 | Merchant Category Code see AS 2805.16 | M |
| 022 | POS Entry Mode | n | 3 | '012' - Manually entered with no PIN Entry capability, or '021' - Magnetic Stripe with PIN Entry, or '051' - Integrated Circuit Card with PIN Entry capability, or '071' - Contactless ICC with PIN Entry capability. | M |
| 023 | Card Sequence Number | n | 3 | If available, this data should be included | C ¹¹ |
| 025 | POS Condition Code | n | 2 | A limited subset of the codes provided in AS 2805.2 is supported. See clause A.13.13. | M |
| 028 | Amount, Transaction Fee | | X+n8 | Fee charged by the ATM Operator for the Transaction activity in the currency of Amount, Transaction (bit 004) | C ^{8,9} |
| 032 | Acquiring Institution Identification Code | n | ..11 | The Acquirer's, Issuer identification number (IIN) issued by ISO through Standards Australia. (see AS 2805.2, clause 4.4.6) | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Acquirer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C ⁴ |
| 035 | Track 2 Data | z | ..37 | Card Track 2 data field having the format: 'LLTrack2 data' where 'LL' is the data length. For manually entered Transactions, this field must not be present. | C ¹ |
| 037 | Retrieval Reference Number | an | 12 | Reference number supplied by the Card acceptor, that remains unchanged for the life of the Transaction, for example the STAN plus transmission time, formatted as SSSSSSHMMSS | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | A unique code identifying the logical Terminal at the Card acceptor location (see AS 2805.2, E3.4) | M |
| 042 | Card Acceptor Identification Code | ans | 15 | A code uniquely identifying a Merchant location (see AS 2805.2, E3.3 and appendix F) | M |
| 043 | Card Acceptor Name/ Location | ans | 40 | DEVICE location description, formatted as described in clause E6 of AS 2805.2. | M ⁶ |
| 047 | Additional Data, National | ans | ...999 | Terminal Capability Code (see AS 2805.2, 4.4.25.21 and conditionally Manual Entry Indicator and optionally Card Check value see Appendix C) | M ^{5,13} |
| 048 | Additional Data Private | ans | 4 | See clause A.13.7. | O |
| 052 | PIN Data | b | 64 | PIN encrypted by the PIN Session key. | C ³ |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--------------------------------------|--------|--------|---|-----------------|
| 055 | Integrated Circuit Card related data | B | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | C ¹² |
| 057 | Amount Cash | n | 12 | The Cash component of the Transaction, zeroes otherwise. | M |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. | M |

Where the Cardholder and Card are present at the time and place of the Transaction, the Card details should be electronically captured by reading them from the Card or in the case of an IC Card retrieved from the Card (Tag 57, Track 2 Equivalent Data). In these cases field 35 should contain the Card information and field 2 must not be present. Additionally, field 52 is required for all Card originated Transactions except, in the case of ICC Transactions, where the Cardholder verified offline CVM is used. Where an IC Card is unable to be read, subject to the requirements of 4.4(h), the Card details should be electronically captured by reading them from the Card's magnetic stripe.

Notes:

1. *Only one of the fields 002 or 035 must be present.*
2. *Required if field 002 present (PAN manually entered).*
3. *Required for magnetic-stripe originated Transactions if field 035 present (Card swiped). Not required for ICC originated Transactions if the 'off-line PIN validated by the Card' CVM was used.*
4. *Required field if an intermediate network node (or nodes) exists in the transmission path between Acquirer and Issuer.*
5. *Required for all Card-read Transactions, if the Card is unable to be read refer to 0 for ICCs.*
6. *Must contain only the words "Medicare Benefit" if a refund Transaction is being used to make a Medicare Claim Refund.*
7. *For ATM Transactions, the amount shown in this field must be exclusive of any ATM Operator Fee, that is, it will represent the amount anticipated to be dispensed to the Cardholder.*
8. *The 'X' portion must contain 'D' to indicate that the fee is due the Acquirer.*
9. *If this field is included in a message, but no direct charge is to apply, then the n8 component of the field must be set to zero.*

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

10. *Recommended for ATM Transactions to/from a Credit facility. For example cash advances from a credit card account.*
11. *From TAG 5F34 for ICC originated Transactions.*
12. *Not required for Deposit, Refund, magnetic-stripe originated and EMV Phase 1 Transactions.*
13. *The population of field 47 is only mandatory subsequent to the interchange link being upgraded to support EMV processing.*

Deleted
effective
21.11.17

A.12.4 0210 Financial Transaction Request Response Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|---|----------------|
| --- | Message Type | n | 4 | '0210' | |
| --- | Bit Map Primary | b | 64 | | |
| 003 | Processing Code | n | 6 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 004 | Amount Transaction | n | 12 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 015 | Date, Settlement | n | 4 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 028 | Amount, Transaction Fee | | X+n8 | Echoed from the Financial Transaction Request (0200) message | C |
| 032 | Acquiring Institution Identification Code | n | ..11 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Issuer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C ¹ |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 047 | Additional Data, National | ans | ...999 | Card Check Value response code, see AS 2805.2, clauses 4.4.25.3. | C ² |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--------------------------------------|--------|--------|---|----------------|
| 055 | Integrated Circuit Card related data | b | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | O ⁴ |
| 057 | Amount Cash | n | 12 | Echoed from the Financial Transaction Request ('0200') message. | M |
| 058 | Ledger Balance | n | 12 | This field has the following format: 'S\$\$\$\$\$\$\$\$cc' – where 'S' = 'D' for a Debit balance and 'C' for a Credit balance. | C ³ |
| 059 | Account Balance, Cleared Funds | n | 12 | This field has the following format: 'S\$\$\$\$\$\$\$\$cc' - where 'S' = 'D' for a Debit balance and 'C' for a Credit balance. | C ³ |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. | M |

Notes:

1. Required if field present in associated 0200 Request message.
2. Optionally required if PAN manually entered and Card Check Value present and sent in the associated 0200 request message.
3. Required field for balance enquiries, at Issuer's discretion for other Transactions.
4. Not required for magnetic-stripe originated Transactions or where not provided by the Issuer.

A.12.5 0220/0221 Financial Transaction Advice Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|------------------------|--------|------|---|----------------|
| --- | Message Type | n | 4 | '0220' - Advice or '0221' - Advice repeat | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | Required if Data Element 90 is present for partial dispense processing. | C |
| 002 | Primary Account Number | n | ..19 | PAN having the format: 'LLPAN data' where 'LL' is the data length. | C ¹ |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | | |
|-----|----------------------------|--------|------|---|----------------|----------------------------|
| 003 | Processing Code | n | 6 | Transaction (Digits 1&2) = '00' for Goods & Services '01' for Cash Wdl '09' for Goods & Services with Cash '20' for Refund of Goods & Services '21' for Deposits Source Account (Digits 3&4) = '00' if sub-field unused, '10' if from Savings A/C, '20' if from Cheque A/C, '30' if from a Credit facility7. Destination Account (Digits 5&6) = '00' if sub-field unused, '10' if to Savings A/C, '20' if to Cheque A/C, '30' if to a Credit facility7. See AS 2805.2, clause 4.4.11, only the mentioned codes are supported. | M | Amended effective 21.11.17 |
| 004 | Amount Transaction | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc' | M | |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M | |
| 011 | Systems Trace Audit Number | n | 6 | A number assigned by the Card acceptor, or the Acquirer, that uniquely identifies a Transaction at a Terminal for at least one calendar day and remains unchanged for the life of the Transaction. | M | |
| 012 | Time, Local Transaction | n | 6 | DEVICE Time in the format 'HHMMSS'. | M | |
| 013 | Date, Local Transaction | n | 4 | DEVICE Date in the format 'MMDD'. | M | |
| 014 | Expiry Date | n | 4 | 'YYMM', Card expiry date Where the PAN is manually entered and the data unavailable, this field may be omitted. | C ² | |
| 015 | Date, Settlement | n | 4 | Acquirer's Processing Date having the format 'MMDD'. | M | |
| 018 | Merchant's Type | n | 4 | Merchant Category Code see AS 2805.16 | M | |
| 022 | POS Entry Mode | n | 3 | '012' - Manually entered with no PIN Entry capability, or '021' - Magnetic Stripe with PIN Entry, or '051' - Integrated Circuit Card with PIN Entry capability, or '071' - Contactless ICC with PIN Entry capability | M | |
| 023 | Card Sequence Number | N | 3 | If available, this data should be included | C ⁸ | |
| 025 | POS Condition Code | n | 2 | A limited subset of the codes provided in AS 2805.2 is supported. See clause A.13.13. | M | |
| 028 | Amount, Transaction Fee | | X+n8 | Fee charged by the ATM Operator for the Transaction activity in the currency of Amount, Transaction (bit 004) | C ⁶ | |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|----------------|
| 032 | Acquiring Institution Identification Code | n | ..11 | The Acquirer's, Issuer identification number (IIN) issued by ISO through Standards Australia. (see AS 2805.2, clause 4.4.6) | M |
| 033 | Forwarding Institution Identification Code | n | .11 | The IIN of the Acquirer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C ³ |
| 035 | Track 2 Data | z | ..37 | Card Track 2 data field having the format: 'LLTrack2 data' where 'LL' is the data length. This data element may mirror the data contained in the original request or advice message or be truncated to include only the Primary Account Number(PAN), Separator, Expiration Date and Service Code in accordance with the requirements of the Payment Card Industry (PCI) Data Security Standard – Version 1.2. | C ¹ |
| 037 | Retrieval Reference Number | an | 12 | Reference number supplied by the Card acceptor, that remains unchanged for the life of the Transaction, for example the STAN plus transmission time, formatted as SSSSSSHHMMSS | M |
| 038 | Authorisation id Response | an | 6 | Echoed from the associated 0110 Authorisation Response message if present (pre-authorized Transaction) | C ⁴ |
| 041 | Card Acceptor Terminal ID | ans | 8 | A unique code identifying the logical Terminal at the Card acceptor location. In accordance with AS 2805.2, E3.4 this field together with the AIIIC and CAIC uniquely identifies a Terminal within Australia. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | A code uniquely identifying a Merchant location (see AS 2805.2, E3.3 and appendix F) | M |
| 043 | Card Acceptor Name Location | ans | 40 | DEVICE location description. | M ⁵ |
| 047 | Additional Data National | Ans | ...999 | Terminal Capability Code (see AS 2805.2, 4.4.25.21 and conditionally Electronic Fallback Indicator and Card Check Value see AS 2805.2, clauses 4.4.25.11 and 4.4.25.3 | M |
| 048 | Additional Data Private | ans | 4 | See clause A.13.7 | O |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 055 | Integrated Circuit Card related data | b | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | C ⁹ |
| 057 | Amount Cash | n | 12 | The Cash component of the Transaction, zeroes otherwise. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|-----------------------------|--------|----|--|---|
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. Mandatory if data element 90 not required, otherwise excluded. | C |
| 090 | Original Data Elements | n | 42 | Required to contain the data elements of the original Transaction for partial dispense processing | C |
| 128 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the Sender's MAC Session key. Mandatory if data element 90 present, otherwise excluded. | C |

Where the Cardholder and Card are present at the time and place of the Transaction, the Card details should be electronically captured by reading them from the Card or in the case of an IC Card, retrieved from the chip (Tag 57, Track 2 Equivalent Data). In these cases field 35 should contain the Card information and field 2 must not be present. Where an IC Card is unable to be read, subject to the requirements of 4.4(h) the Card details should be electronically captured by reading them from the Card's magnetic stripe. The magnetic stripe read is indicated by the value "021" in field 22.

Notes:

1. *Only one of the fields 002 or 035 must be present.*
2. *Required if field 002 present (PAN manually entered).*
3. *Required field if an intermediate network node (or nodes) exists in the transmission path between Acquirer and Issuer.*
4. *Required if the data is present in the associated 0110 Authorisation Response message.*
5. *Must contain only the words "Medicare Benefit" if a refund Transaction is being used to make a Medicare Claim Refund.*
6. *For an ATM Partial Dispense this field must contain zero ('D000000000000') as no ATM Operator Fee can be charged for an ATM Partial Dispense.*
7. *Recommended for ATM Transactions to/from a Credit facility. For example cash advances from a credit card account.*
8. *From TAG 5F34 for ICC originated Transactions.*
9. *Not required for deposit Transactions, Refund Transactions and magnetic-stripe originated and EMV phase 1 Transactions*
- 10.

A.12.6 0230 Financial Transaction Advice Response MessageDeleted effective
21.11.17

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|---|----------------|
| --- | Message Type | n | 4 | '0230' | |
| --- | Bit Map Primary | b | 64 | | |
| 003 | Processing Code | n | 6 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 004 | Amount Transaction | n | 12 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 015 | Date, Settlement | n | 4 | Echoed from the Financial Transaction Request ('0220/0221') message. | M |
| 028 | Amount, Transaction Fee | | X+n8 | Echoed from the Financial Transaction Advice ('0220/0221') message. | C ¹ |
| 032 | Acquiring Institution Identification Code | n | ..11 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Issuer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C ¹ |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 057 | Amount Cash | n | 12 | Echoed from the Financial Transaction Advice ('0220/0221') message. | M |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the sender's MAC Session key. | M |

Note:

1. Required if field present in associated 0220/0221 messages

A.12.7 0420/0421 Acquirer Reversal Advice/Repeat Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|------------------------|--------|------|--|----------------|
| --- | Message Type | n | 4 | '0420' - Advice or '0421' - Advice repeat | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 002 | Primary Account Number | n | ..19 | PAN having the format: 'LLPAN data' where 'LL' is the data | C ¹ |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|----------------|
| | | | | length. | |
| 003 | Processing Code | n | 6 | Echoed from the request or Advice message. | M |
| 004 | Amount Transaction | n | 12 | Echoed from the request or Advice message. | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit No. | n | 6 | Echoed from the request or Advice message. | M |
| 012 | Time, Local Transaction | n | 6 | DEVICE Time in the format 'HHMMSS'. | M |
| 013 | Date, Local Transaction | n | 4 | DEVICE Date in the format 'MMDD'. | M |
| 014 | Expiry Date | n | 4 | 'YYMM' This data element should mirror the data contained in the original 0100 or 0200. | C ² |
| 015 | Date, Settlement | n | 4 | Acquirer's Processing Date having the format 'MMDD'. | M |
| 022 | POS Entry Mode | n | 3 | Echoed from the request or Advice message. | M |
| 025 | POS Condition Code | n | 2 | A limited subset of the codes provided in AS 2805.2 is supported. See clause A.13.3. | M |
| 028 | Amount, Transaction Fee | | X+n8 | Echoed from the Request or Advice message but with X set to 'C' | C ³ |
| 032 | Acquiring Institution Identification Code | n | ..11 | The Acquirer's, Issuer identification number (IIN) issued by ISO through Standards Australia. (see AS 2805 part 2, clause 4.4.6) | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the Acquirer or intermediate network node if one is present. See clause A.13.4 for usage of this field | C |
| 035 | Track 2 Data | z | ..37 | Card Track 2 data field having the format: 'LLTrack 2 data' where 'LL' is the data length. This data element may mirror the data contained in the original request or advice message or be truncated to include the Primary Account Number(PAN), Separator, Expiration Date and Service Code in accordance with the requirements of the Payment Card Industry (PCI) Data Security Standard – Version 1.2. | C ¹ |
| 037 | Retrieval Reference Number | an | 12 | Echoed from the request or Advice message. | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | Echoed from the request or Advice message. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | Echoed from the request or Advice message. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--------------------------------------|--------|--------|---|----------------|
| 043 | Card Acceptor Name Location | ans | 40 | Echoed from the request or Advice message. | M |
| 047 | Additional Data National | ans | ...999 | Echoed from the request or Advice message. | C |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 055 | Integrated Circuit Card related data | b | ...999 | For EFTPOS see clause A.13.13 for the required contents of this field. For ATM see clause A.13.14 for the required contents of this field. | C ⁴ |
| 057 | Amount Cash | n | 12 | Echoed from the request or Advice message | M |
| 090 | Original Data Elements | n | 42 | Original data from the Transaction being reversed: a) Message Type - 'nnnn', b) System Trace Audit No. - 'nnnnnn', c) Local Date & Time - 'MMDDhhmmss', d) Acquiring Institution - 'nnnnnnnnnnn', e) Forwarding Institution - all zeroes | M |
| 128 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the sender's MAC Session key. | M |

Notes:

1. Only one of the fields 002 or 035 must be present.
2. Required if field 002 present (PAN manually entered).
3. Required if present in the original Request message.
4. Not required for Deposit Transactions, Refund Transactions and magnetic-stripe originated and EMV Phase 1 Transactions.

A.12.8 0430 Acquirer Reversal Advice Response Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--------------------------|--------|----|---|---|
| --- | Message Type | n | 4 | '0430' | |
| --- | Bit Map Primary | b | 64 | | |
| 003 | Processing Code | n | 6 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 004 | Amount Transaction | n | 12 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|---|---|
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 015 | Date, Settlement | n | 4 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 028 | Amount, Transaction Fee | | X+n8 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | C |
| 032 | Acquiring Institution Identification Code | n | ..11 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the intermediate network node if one is present. See clause A.13.4 for usage of this field | C |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 041 | Card Acceptor Terminal ID | ans | 8 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 042 | Card Acceptor Identification Code | ans | 15 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 057 | Amount Cash | n | 12 | Echoed from the Acquirer Reversal Advice ('0420/0421') message. | M |
| 064 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the sender's MAC Session key. | M |

A.12.9 0520/0521 Acquirer Reconciliation Advice/Repeat Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|---|--------|------|---|----------------|
| --- | Message Type | n | 4 | '0520' - Advice or '0521' Advice repeat | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Sequential Number managed by the Acquirer | M |
| 015 | Date, Settlement | n | 4 | Initiator's Processing Date having the format 'MMDD' being the date to be reconciled. | M |
| 032 | Acquiring Institution Identification Code | n | ..11 | The Initiator's, Issuer identification number (IIN) issued by ISO through Standards Australia. (see AS 2805.2, clause 4.4.6). | M ¹ |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 074 | Credits Number | n | 10 | Number of Credit Transactions processed by the Acquirer since the last Settlement. | M |
| 075 | Credit Reversals Number | n | 10 | Number of Credit Reversal Transactions processed by the Acquirer since the last | M |

Australian Payments Network Limited [ABN 12 055 136 519]

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|---|----------------|
| | | | | Settlement. | |
| 076 | Debits Number | n | 10 | Number of Debit Transactions processed by the Acquirer since the last Settlement. | M |
| 077 | Debit Reversals Number | n | 10 | Number of Debit Reversal Transactions processed by the Acquirer since the last Settlement. | M |
| 078 | Transfers Number | n | 10 | Not used, must be zeroes | M |
| 079 | Transfer Reversals Number | n | 10 | Not used, must be zeroes | M |
| 080 | Inquiries Number | n | 10 | Number of Account Balance Inquiry Transactions processed by the Acquirer since the last Settlement. | M |
| 081 | Authorisations Number | n | 10 | Number of Authorisation Transactions processed by the Acquirer since the last Settlement. | M |
| 083 | Credits, Transaction Fee Amount | n | 12 | The sum amount of ATM Operator Fees in all Authorisation, Financial and Reversal Transactions where the fee amount is indicated as a credit. | C |
| 085 | Debits, Transaction Fee Amount | n | 12 | The sum amount of ATM Operator Fees in all Authorisation, Financial and Reversal Transactions where the fee amount is indicated as a debit. | C |
| 086 | Credits Amount | n | 16 | Total amount of Credit Transactions processed by the Acquirer since the last Settlement. | M |
| 087 | Credit Reversals Amount | n | 16 | Total amount of Credit Reversal Transactions processed by the Acquirer since the last Settlement. | M |
| 088 | Debits Amount | n | 16 | Total amount of Debit Transactions processed by the Acquirer since the last Settlement. | M |
| 089 | Debit Reversals Amount | n | 16 | Total amount of Debit Reversal Transactions processed by the Acquirer Since the last Settlement | M |
| 097 | Amount, Net Settlement | x + n | 16 | 'X' is set to 'D' if Net Value is a Debit or 'C' if Net value is a Credit, followed by the Net amount of Debit & Credit Transactions processed by the Acquirer since the last Settlement. | M ² |
| 099 | Settlement Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the reconciliation advice message. | M ¹ |
| 118 | Cash Total Number | n | 10 | Number of Cash Withdrawal Transactions processed by the Acquirer since the last Settlement. | M |
| 119 | Cash Total Amount | n | 16 | Total amount of Cash Withdrawal Transactions processed by the Acquirer since the last Settlement. | M |

Australian Payments Network Limited [ABN 12 055 136 519]

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|-----------------------------|--------|----|---|---|
| 128 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the sender's MAC Session key. | M |

Note:

1. Link reconciliation is performed between the nodes specified in fields 032 and 099.
2. The amount must be inclusive of ATM Operator Fees and the total Transaction value amount.

A.12.10 0530 Acquirer Reconciliation Advice Response Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|---|--------|------|---|---|
| --- | Message Type | n | 4 | '0530' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Acquirer Reconciliation Advice ('0520/0521') message. | M |
| 015 | Date, Settlement | n | 4 | Echoed from the Acquirer Reconciliation Advice ('0520/0521') message. | M |
| 032 | Acquiring Institution Identification Code | n | ..11 | Echoed from the Acquirer Reconciliation Advice ('0520/0521') message. | M |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 053 | Security Related Control Information | n | 16 | '0000000000000001' if Key Set 1 used, '0000000000000002' if Key Set 2 used. | M |
| 066 | Settlement Code | n | 1 | '01' = In balance, '02' = Out of Balance, '03' = Error. | M |
| 074 | Credits Number | n | 10 | Number of Credit Transactions processed by the Issuer for the current reconciliation period. | M |
| 075 | Credit Reversals Number | n | 10 | Number of Credit Reversal Transactions processed by the Issuer for the current reconciliation period. | M |
| 076 | Debits Number | n | 10 | Number of Debit Transactions processed by the Issuer for the current reconciliation period. | M |
| 077 | Debit Reversals Number | n | 10 | Number of Debit Reversal Transactions processed for the current reconciliation period. | M |
| 078 | Transfers Number | n | 10 | Not used, must be zeroes | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|---|---|
| 079 | Transfer Reversals Number | n | 10 | Not used, must be zeroes | M |
| 080 | Inquiries Number | n | 10 | Number of Account Balance Inquiry Transactions processed by the Issuer for the current reconciliation period. | M |
| 081 | Authorisations Number | n | 10 | Number of Authorisation Transactions processed by the Issuer for the current reconciliation period. | M |
| 083 | Credits, Transaction Fee Amount | n | 12 | Total amount, of ATM Operator Fees processed by the Issuer where the fee amount is indicated as a credit. | O |
| 085 | Debits, Transaction Fee Amount | n | 12 | Total amount, of ATM Operator Fees processed by the Issuer where the fee amount is indicated as a debit. | O |
| 086 | Credits Amount | n | 16 | Total amount of Credit Transactions processed by the Issuer for the reconciliation period. | M |
| 087 | Credit Reversals Amount | n | 16 | Total amount of Credit Reversal Transactions processed by the Issuer for the current reconciliation period. | M |
| 088 | Debits Amount | n | 16 | Total amount of Debit Transactions processed by the Issuer for the current reconciliation period. | M |
| 089 | Debit Reversals Amount | n | 16 | Total amount of Debit Reversal Transactions processed by the Issuer for the current reconciliation period. | M |
| 097 | Amount, Net Settlement | x + n | 16 | 'X' is set to 'D' if Net Value is a Debit or 'C' if Net value is a Credit, followed by the Net amount of Debit & Credit Transactions processed by the Issuer for the current reconciliation period. | M |
| 099 | Settlement Institution Identification Code | n | ..11 | Echoed from the Acquirer Reconciliation Advice ('0520/0521') message. | M |
| 118 | Cash Total Number | n | 10 | Number of Cash Withdrawal Transactions processed by the Issuer for the current reconciliation period. | M |
| 119 | Cash Total Amount | n | 16 | Total amount of Cash Withdrawal Transactions processed by the Issuer for the current reconciliation period. | M |
| 128 | Message Authentication Code | b | 64 | MAC of all previous fields generated with the sender's MAC Session key. | M |

A.12.11 0800 Network Management Sign On Request Message

- (a) 0800 Network Management Sign On Request messages are used to establish or re-establish a link.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (b) “Sign On” messages are uni-directional and each node must independently “Sign On” to establish a bi-directional flow of financial messages. “Sign On” messages require a Sign On Response (0810 with Data Element 70 equal to 001). A “Sign On” can be initiated by either node and may be sent at any time.
- (c) “Sign On” messages initiates proof of endpoint processing by sending an enciphered random value in data element 48.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|---|
| --- | Message Type | n | 4 | '0800' | |
| --- | | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | A number assigned by the requestor that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending network node. | M |
| 048 | Additional Data Private | ans | ...999 | Enciphered 64-bit random number used for proof-of-end-point processing. eKEKsV82(RNs), length 8 bytes | M |
| 053 | Security Related Control Information | n | 16 | KEK identifier. See clause A.13.9 for usage of this field. | O |
| 070 | Network Management Information Code | n | 3 | '001' – Sign On. | M |
| 100 | Receiving Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the Sign On request message. | M |

A.12.12 0810 Network Management Sign On Request Response Message

- (a) A Network Management “Sign On” response message is sent in response to a Network Management Sign On Request message (0800 with NMIC equal to 001) to confirm that the link is operational and to complete proof of endpoint processing.
- (b) A Sign On Request Response message contains an enciphered random number in data element 48 with a length of eight bytes.
- (c) The random number returned is the inverse of the random number sent in the corresponding Sign On Request message: RNR = ~RN.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|-----------------|--------|----|----------|--|
| --- | Message Type | n | 4 | '0810' | |
| --- | Bit Map Primary | b | 64 | | |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|---|---|
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Logon/Echo Request ('0800') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |
| 039 | Response Code | an | 2 | '00' = link operational, for other values refer to Response Codes Table. | M |
| 048 | Additional Data Private | ans | ...999 | This data element will contain an eight byte, encrypted random number, created from the inversion of the random number provided by the requestor in the Logon request message. eKEKrV84(RNr) | M |
| 053 | Security Related Control Information | n | 16 | Echoed from the Logon/Echo Request ('0800') message. | O |
| 070 | Network Management Information Code | n | 3 | '001' – Sign On. | M |
| 100 | Receiving Institution Identification Code | n | ..11 | Echoed from the Logon/Echo Request ('0800') message. | M |

A.12.13 0820 Network Management Sign Off Advice Message

- (a) 0820 Network Management Sign Off Advice messages are used to terminate financial message processing on a link.
- (b) "Sign Off" messages cause the immediate termination of all request and advice message traffic on a given link. A "Sign Off" can be initiated by either node and may be sent at any time.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|---|
| --- | Message Type | n | 4 | '0820' | |
| --- | | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | b | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | b | 6 | A number assigned by the requesting node that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |
| 070 | Network Management | n | 3 | '002' - Sign Off. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|---|--------|------|--|---|
| | Information Code | | | | |
| 100 | Receiving Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the Sign Off advice message. | M |

A.12.14 0830 Network Management Sign Off Advice Response Message

A Network Management Sign Off Advice Response message is sent in response to a Network Management Sign On Advice message (0820 with NMIC equal to 002) to complete the logical disconnection of the link.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|----------------------------|--------|----|---|---|
| --- | Message Type | n | 4 | '0820' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Sign Off Advice ('0820') message. | M |

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|---|---|
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending Node. | M |
| 039 | Response Code | an | 2 | '00' = Sign off successful | M |
| 070 | Network Management Information Code | n | 3 | '002' - Sign Off. | M |
| 100 | Receiving Institution Identification Code | n | ..11 | Echoed from the Sign Off advice ('0820') message. | M |

A.12.15 0800 Network Management Echo Request Message

- (a) Network Management Echo Request Messages are sent to confirm link status.
- (b) Network Management Echo Request Messages require a Network Management Echo Response (0810 with data element 70 equal to 301).
- (c) Echo Requests should be sent after one (1) minute of link inactivity.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|-------------------|--------|----|----------|---|
| --- | Message Type | n | 4 | '0800' | |
| --- | | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|---|
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | A number assigned by the requestor that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |
| 070 | Network Management Information Code | n | 3 | '301' - Echo test | M |
| 100 | Receiving Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the Echo Request message. | M |

A.12.16 0810 Network Management Echo Request Response Message

A Network Management Echo Request Response message is sent in response to a Network Management Echo Request message (0800 with NMIC equal to 301). Successful receipt confirms the operational status of the link.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|---|
| --- | Message Type | n | 4 | '0810' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Logon/Echo Request ('0800') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |
| 039 | Response Code | an | 2 | '00' = approved, for other values refer to Response Codes Table. | M |
| 070 | Network Management Information Code | n | 3 | Echoed from the Logon/Echo Request ('0800') message | M |
| 100 | Receiving Institution Identification Code | n | ..11 | Echoed from the Logon/Echo Request ('0800') message. | M |

A.12.17 0820 Network Management (Key Change) Advice Message

- (a) Network Management Advice Messages are used to initiate the replacement of a set of session keys.
- (b) A Network Management Key Change Advice message requires a Network Management Key Change Advice Response message (0830 with NMIC equal to 101).

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (c) Each Node must send a Network Management Key Change Advice message immediately after successful confirmation of a “Sign On” request.
- (d) Subsequently, while ever a Node remains signed on a Network Management Key Change Advice message can be sent by either node at any time.
- (e) Data Element 48 is used to convey the new session keys enciphered under the interchange send, key encrypting key (KEKs).

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|---|
| | Message Type | n | 4 | '0820' | |
| | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | A number assigned by requestor that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |
| 048 | Additional Data Private | ans | ...999 | This field has two alternative constructions, see clause A.13.6. | M |
| 053 | Security Related Control Information | n | 16 | Key Set identifier. See clause A.13.9 for usage of this field. | M |
| 070 | Network Management Information Code | n | 3 | '101' – Key Change | M |
| 100 | Receiving Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the Key Change Advice message. | M |

A.12.18 0830 Network Management Advice (Key Change) Response Message

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|---|
| --- | Message Type | n | 4 | '0830' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | Systems Trace Audit Number | n | 6 | Echoed from the Key Change Advice ('0820') message. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|---|--------|--------|--|---|
| 039 | Response Code | an | 2 | '00' =Keys installed, for other values refer to Response Codes Table. | M |
| 048 | Additional Data Private | ans | ...999 | This field has two alternative constructions, dependent on the number of fields that were present in the request either A nine byte data element containing the calculated Key Verification Codes (KVCs) of the interchange session keys received in the corresponding 0820 message as follows; KVC(KMACs) with length of 3 bytes KVC(KPEs) with length of 3 bytes KVC(KDs) with length of 3 bytes; alternatively; A six byte data element containing the calculated Key Verification Codes (KVCs) of the interchange session keys received in the corresponding 0820 message as follows; KVC(KMACs) with length of 3 bytes KVC(KPEs) with length of 3 bytes | M |
| 053 | Security Related Control Information | n | 16 | Echoed from Key Change Advice ('0820') message. | M |
| 070 | Network Management Information Code | n | ..11 | Echoed from the Key Change Advice ('0820') message. | M |
| 100 | Receiving Institution Identification Code | n | ..11 | Echoed from the Key Change Advice ('0820') message | M |

A.12.19 0820 Network Management (KEK Change) Advice Message

- (a) Network Management Advice Messages are used to initiate the replacement of a Key Enciphering Key (KEK) when Online RSA Key Method is used to change Key Enciphering Keys.
- (b) A Network Management KEK Change Advice message requires a Network Management KEK Change Advice Response message (0830 with NMIC equal to 140).
- (c) Each Node must send a Network Management KEK Change Advice message at least once every 2 years to comply with the interchange requirements specified in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).
- (d) Data Element 112 is used to convey the new Send Key Encipherment Key (KEKs), enciphered under the Interchange Public Key (IPK) of the recipient, which will have been previously provided to the sender via a secure channel.

Amended
effective 1.1.16

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (e) The new KEK may be used after the Network Management Advice Response message (0830) has been received and the KVC validated.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|--------|--|---|
| --- | Message Type | n | 4 | '0820' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss'. | M |
| 011 | System Trace Audit Number | n | 6 | A number assigned by the requestor that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See 4.3.12 for usage of this field. | M |
| 053 | Security Related Control Information | n | 16 | KEK identifier. See clause A.13.9 for usage of this field. | M |
| 070 | Network Management Information Code | n | 3 | '140' | M |
| 100 | Receiving Institution Identification Code | n | ..11 | The Issuer identification number (IIN) of the intended recipient of the Key Change Advice message. | M |
| 112 | Key Management Data | b | ...999 | See clause A.13.12 for usage of this field. | M |

A.12.20 0830 Network Management (KEK Change) Advice Response Message

- (a) A Network Management Advice Response message is sent in response to a Network Management Advice Request message.
- (b) Data Element 112 contains the KVC of the KEK sent in the 0820 request and is used to confirm that it matches the KVC that was built with the KEK.

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|--|--------|------|--|---|
| --- | Message Type | n | 4 | '0830' | |
| --- | Bit Map Primary | b | 64 | | |
| 001 | Bit Map Secondary | b | 64 | | M |
| 007 | Transmission Date & Time | n | 10 | Sender's Message Date & Time in format 'MMDDhhmmss' | M |
| 011 | System Trace Audit Number | n | 6 | A number assigned by the requestor that uniquely identifies a Transaction for at least one calendar day and remains unchanged for the life of the Transaction. | M |
| 033 | Forwarding Institution Identification Code | n | ..11 | The IIN of the sending node. See clause A.13.4 for usage of this field. | M |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| BIT | DESCRIPTION | ATTRIB | | COMMENTS | |
|-----|---|--------|--------|--|---|
| 039 | Response Code | an | 2 | '00' = Keys stored. For other values, refer to Response Codes Table. | M |
| 053 | Security Related Control Information | n | 16 | Echoed from the KEK Change Advice ('0820') message | M |
| 070 | Network Management Information Code | n | 3 | '140' | M |
| 100 | Receiving Institution Identification Code | n | ..11 | Echoed from the Key Change Advice ('0820') message | M |
| 112 | Key Management Data | b | ...999 | KVC of the KEK sent in the 0820 KEK Change Advice. | M |

A.13 Fields

The definitions contained in AS2805 part 2 apply, unless otherwise stated.

A.13.1 Processing Code (field 3)

This field contains a 6-digit processing code constructed from three sub-fields.

| | | |
|---|-------------------|--|
| 1 | Positions 1 and 2 | Describes the specific Transaction as follows 00 = Purchase 01 = Cash Withdrawal 09 = Combined purchase and Cash out 20 = Refund 31 = Balance Enquiry |
| 2 | Positions 3 and 4 | Source Account Type 00 = Field unused 10 = Savings Account 20 = Cheque Account |
| 3 | Positions 5 and 6 | Destination Account Type 00 = Field unused 10 = Savings Account 20 = Cheque Account |

Note: Only the above-specified codes may be used.

A.13.2 Merchant's Type (field 18)

This field must contain the code that best describes the Merchant where the Transaction originated. These codes can be found in the Australian Standard AS 2805.16 as Merchant Category Code and the code selected should be the one that applies to the predominate activity conducted by that Merchant. It must not be replaced by intermediate systems.

A.13.3 Point of Service Condition Code (field 25)

Only the following codes identified in AS 2805.2 may be used:

00 = Normal presentment

04 = Electronic Cash register interface

08 = Mail or telephone order

10 = Customer identity verified

41 = Cash Dispensing Machine i.e., an ATM

42 = Electronic Payment Terminal i.e., a POS Terminal

43 = Card Activated Fuel Dispenser

44 Travel Ticket Vending Machines

A.13.4 Usage of Institution Identification Codes (fields 32, 33)

As described in AS 2805.2, clause 4.4.23, the usage of institution identification codes must be in accordance with the following table.

| For Request or Advice messages | | | | |
|--------------------------------|---|--------|--------|------------------|
| IID | Acquirer to A | A to B | B to C | C to Card Issuer |
| Acquiring Institution | Remains the same throughout the life of the Transaction | | | |
| Forwarding Institution | (Acquirer) | A | B | C |
| Receiving Institution | A | B | C | (Card Issuer) |

| For Response messages | | | | |
|------------------------|---|--------|--------|---------------|
| IID | Issuer to C | C to B | B to A | A to Acquirer |
| Acquiring Institution | Remains the same throughout the life of the Transaction | | | |
| Forwarding Institution | (Card Issuer) | C | B | A |
| Receiving Institution | C | B | A | (Acquirer) |

A.13.5 Service Restriction Code (field 40)

Field 40 is not supported.

A.13.6 Additional data private (field 48) for 0820 Key change Advice message

Field 48, within a 0820 Key Change Advice Message is used to transport the new session keys. As the presence of the data encipherment session key is optional there are two alternative constructions of this field. Note that the Data Encipherment key is unused in this interchange specification.

-
- (a) Without Data Encipherment Session Key
 - Data length - '032'
 - (i) 16 byte encrypted MAC Session Key (KMACs);
 - (ii) 16 byte encrypted PIN Protect Session Key (KPEs).
 - (b) With Data Protect Session Key
 - Data length - '048'
 - (i) 16 byte encrypted MAC Session Key (KMACs);
 - (ii) 16 byte encrypted PIN Protect Session Key (KPEs);
 - (iii) 16 byte encrypted Data Encipherment Session Key (KDs, unused, may be zeroes).

A.13.7 Additional data private (field 48) for 0800/0810 Logon Request/Response messages

- (a) For Logon Request Messages (0800, NMIC 001), field 48 will contain an enciphered, 8 byte, random number used for proof-of-end-point processing.
- (b) For the response message, this field will contain the enciphered, inverted value of the random number provided in the request message.

A.13.8 Additional Data Private (field 48) for Financial Messages (01xx, 02xx, 04xx)

- (a) For details of this field refer to AS 2805.2. Note that many existing Interchanges provide a state code in this field as follows;
- (b) For 01xx, 02xx and 04xx messages, the first byte of this field may contain a single byte state code as follows:

- 0 Reserved for future use
- 1 Australian Capital Territory
- 2 New South Wales
- 3 Victoria
- 4 Queensland
- 5 South Australia

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- 6 Western Australia
- 7 Tasmania
- 8 Northern Territory
- 9 Reserved for future use

- (c) Additional data may follow.
- (d) The inclusion of the state code in this field is deprecated and is not recommended for new Interchanges.

A.13.9 Security Related Control Information (field 53)

- (a) For Sign-on Request Messages (0800, NMIC 001) where Online RSA Key Method is used, field 53 will contain the identifier of the KEK used to generate eKEKsV82(RNs):

‘0000000000000010’ when KEK 1 has been used.

‘0000000000000020’ when KEK 2 has been used.

- (b) For Key Change Advice Messages (0820, NMIC 101) where Online RSA Key Method is not used, field 53 will contain the identifier of the interchange session key set being changed:

‘0000000000000001’ when interchange key set 1 is being changed.

‘0000000000000002’ when interchange key set 2 is being changed.

- (c) For Key Change Advice Messages (0820, NMIC 101) where Online RSA Key Method is used, field 53 will contain the identifier of the KEK used to encipher the interchange session keys and the identifier of the interchange session key set being changed:

‘0000000000000011’ when KEK 1 has been used and interchange key set 1 is being changed.

‘0000000000000012’ when KEK 1 has been used and interchange key set 2 is being changed.

‘0000000000000021’ when KEK 2 has been used and interchange key set 1 is being changed.

‘0000000000000022’ when KEK 2 has been used and interchange key set 2 is being changed.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (d) For KEK Change Advice Messages (0820, NMIC 140) where Online RSA Key Method is used, field 53 will contain the identifier of the KEK being changed:

‘0000000000000010’ when interchange KEK 1 is being changed.

‘0000000000000020’ when interchange KEK 2 is being changed.

A.13.10 Network management information code (field 70)

The following 3 digit network management information codes must be used:

| Position 1 | Positions 2 and 3 | |
|--------------------------|-------------------|------------|
| 0 - System condition | 01 | Sign on |
| 0 - System condition | 02 | Sign off |
| 1 - System security | 01 | Key Change |
| 1 - System security | 40 | KEK Change |
| 3 - System audit control | 01 | Echo test |

A.13.11 Message Authentication Codes (fields 64 and 128)

Message Authentication codes must be constructed in accordance with AS 2805.4.1. The MAC size must be 32-bits and stored left justified, right zero filled in the 64-bit field.

A.13.12 Key Management Data (field 112)

- (a) For KEK Change Advice messages (0820, NMIC 140) where Online RSA Key Method is used, field 112 will contain the new KEK enciphered under the receiver’s Interchange Public Key (IPKr) and the signed hash of the KEK using the sender’s Interchange Secret Key (ISKs).
- (b) The length of the field will be dependent of the key lengths of two RSA keys. The format of the field will be as follows:

| Description | Size |
|-----------------------------------|-----------------------------|
| Field length | 3 bytes |
| KVC of KEK | 3 bytes |
| KEK enciphered under IPKr | Size of the modulus of IPKr |
| Signed hash of the KEK using ISKs | Size of the modulus of ISKs |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

- (c) For KEK Change Advice Response messages (0830, NMIC 140) where Online RSA Key Method is used, field 112 will contain the KVC of the KEK.

| Description | Size |
|--------------|---------|
| Field length | 3 bytes |
| KVC of KEK | 3 bytes |

A.13.13 EMV (Field 55) POS Interchanges

- (a) Field 55 must be formed in accordance with clause 4.4.26 of AS2805.2—2007Amdt 2-2008, as a series of individual data objects, Tag, Length, Value (TLV) encoded as per ISO 7816-6. The order of the data objects is not important.
- (b) The table below identifies the data elements required for each message type.

| TAG | Name | Len | Message Type | | | | | | Comment |
|------|---------------------------------|-------|--------------|------|-------|------|------|-------|---|
| | | | 0100 | 0110 | 02002 | 0210 | 0220 | 04201 | |
| 71 | Issuer Script Template 1 | ..127 | | O | | O | | | |
| 72 | Issuer Script Template 2 | ..127 | | O | | O | | | |
| 82 | Application Interchange Profile | 2 | ✓ | | ✓ | | ✓ | C | |
| 8A | Authorisation Response Code | 2 | | O | | O | O | C | Note 3 |
| 91 | Issuer Authentication Data | ..16 | | O | | O | | | Note 5 |
| 95 | Terminal Verification Result | 5 | ✓ | | ✓ | | ✓ | C | TVR may have changed in 0420 e.g., Issuer authentication failure |
| 9A | Transaction Date | 3 | ✓ | | ✓ | | ✓ | C | |
| 9C | Transaction Type | 1 | ✓ | | ✓ | | ✓ | C | |
| 5F2A | Transaction Currency Code | 2 | ✓ | | ✓ | | ✓ | C | |
| 9F02 | Amount, Authorised | 6 | ✓ | | ✓ | | ✓ | C | |
| 9F03 | Amount, Cash out | 6 | ✓ | | ✓ | | ✓ | C | |
| 9F10 | Issuer Application Data | ..32 | ✓ | | ✓ | | ✓ | C | Note 4. Format is Scheme specific. Reversals may contain updated IAD data |
| 9F1A | Terminal Country Code | 2 | ✓ | | ✓ | | ✓ | C | |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| | | | | | | | | | |
|------|---------------------------------|---|---|--|---|--|---|---|-------------|
| 9F26 | Application Cryptogram | 1 | ✓ | | ✓ | | ✓ | C | |
| 9F27 | Cryptogram Information Data | 8 | ✓ | | ✓ | | ✓ | C | ARQC/TC/AAC |
| 9F33 | Terminal Capabilities | 3 | ✓ | | ✓ | | ✓ | C | |
| 9F34 | CVM results | 3 | ✓ | | ✓ | | ✓ | C | |
| 9F35 | Terminal Type | 1 | ✓ | | ✓ | | ✓ | C | |
| 9F36 | Application Transaction Counter | 2 | ✓ | | ✓ | | ✓ | C | |
| 9F37 | Unpredictable Number | 4 | ✓ | | ✓ | | ✓ | C | |

- (c) The table above lists the minimum required data elements for field 55 by message type. Additional TAGs may be included and must be passed through interchange if valid.

Notes:

1. A reversal must contain the data from the original Transaction.
2. Field 55 is not required for Deposit and Refund Transactions.
3. The Authorisation Response Code is the actual response code used by the Issuer in generating the ARPC cryptogram. Where both TAG 8A and Bit 39 are present, TAG 8A must have precedence and must be passed to the Card unaltered, otherwise a rejection may occur when the ARPC cryptogram is presented to the Card. In the absence of TAG 8A, Bit 39 may be mapped and provided to the Card as TAG 8A. In 0220 messages TAG 8A is a Terminal generated value and must be provided to the Issuer.
4. Issuer application data. Present if provided by ICC in Generate AC command response.
5. Required if on-line Issuer authentication performed.

A.13.14 EMV (Field 55) ATM Interchanges

ICC system related data (DE.55) is a special form, composite data element using ISO 7816-6 TLV coding structures.

Amended effective 1.1.16

- (a) Field 55 must be formed in accordance with clause 4.4.26 of AS2805.2—2007Amdt 2-2008, as a series of individual data objects, Tag, Length, Value (TLV) encoded as per ISO 7816-6. The order of the data objects is not important.
- (b) Table 1 identifies the minimum EMV data elements that must be included in DE.55. Other valid EMV data elements may be included by the Acquirer. Issuers should have the ability to ignore malformed or unwanted data elements without impairing Transaction processing. Note that DE.55 is not present in response messages for contactless transactions.

Amended effective 1.1.16

Amended effective 1.1.16

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

Inserted
effective 1.1.16

| Data Element | EMV Tag | LEN | Message Type | | | | | | Comment |
|--|-------------------|-------|--------------|------------------|-------------------|------|------------------|------|--|
| | | | 0200 | 0210 | 022x ⁶ | 0230 | 042x | 0430 | |
| Transaction currency code | 5F2A | 2 | P | - | P | - | P | - | Present if provided |
| Issuer Script Template 1 | 71 | ..127 | - | C ^{2,3} | - | - | - | - | |
| Issuer Script Template 2 | 72 | ..127 | - | C ^{2,3} | - | - | - | - | |
| Application Interchange Profile | 82 | 2 | M | - | M | - | M | - | |
| Authorisation Response Code | 8A ⁴ | 2 | - | C ^{3,7} | - | - | C ^{3,7} | - | |
| Issuer Authentication Data | 91 | ..16 | - | C ^{1,3} | - | - | - | - | |
| Terminal verification results | 95 | 5 | M | - | M | - | M | - | TVR may have changed in 0420 e.g., Issuer authentication failure |
| Transaction Date | 9A | 3 | M | 0 ³ | M | - | M | - | |
| Transaction type | 9C | 1 | M | - | M | - | M | - | |
| Amount authorised | 9F02 | 6 | M | O | M | - | M | - | Excluding any fees if applicable |
| Amount, other | 9F03 | | M | | M | | M | | Required for cryptogram. |
| DF name | 84 | ..15 | M | - | M | - | M | - | |
| Issuer Application Data | 9F10 | ..32 | M | - | M | - | M | - | Format is scheme specific. |
| Terminal country code | 9F1A | 2 | M | - | M | - | M | - | |
| Application Cryptogram | 9F26 | 8 | M | - | M | - | M | - | |
| Cryptogram Information Data | 9F27 | 1 | M | - | M | - | M | - | |
| Terminal capabilities | 9F33 | 3 | P | - | P | - | P | - | |
| Cardholder Verification Method Results | 9F34 | 3 | P | - | P | - | P | - | |
| Terminal type | 9F35 | 1 | M | - | M | - | M | | 14. Unattended FI controlled |
| Application Transaction Counter | 9F36 ⁵ | 2 | M | - | M | - | M | - | |
| Unpredictable number | 9F37 | 4 | M | - | M | - | M | - | |

Table 1 - DE.55 ICC system related data

M = mandatory, P = preferred, C = conditional, - = not present, O = Optional.

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

Notes:

1. *Mandatory if Issuer authentication performed by Issuer.* Amended effective 1.1.16
2. *Mandatory if script command returned to the ICC by the Issuer.* Amended effective 1.1.16
3. *Not to be present for contactless responses.* Amended effective 1.1.16
4. *The Authorisation Response Code is the actual response code and, depending on the ARPC method implemented by the scheme, may be used by the Issuer in generating the ARPC cryptogram. Where both TAG 8A and DE.39 are present, TAG 8A shall have precedence and shall be passed to the Card unaltered, otherwise a rejection may occur when the ARPC cryptogram is presented to the Card. In the absence of TAG 8A, DE.39 may be mapped and provided to the Card as TAG 8A. In 0220 messages TAG 8A is an ATM generated value and must be provided to the Issuer.* Amended effective 21.11.17
5. *The Issuer host may receive duplicate ATC values for each authorisation when the previous authorisation request resulted in an online PIN failure. Issuers should consider not automatically declining transactions solely due to this condition as an indication of fraudulent activity.* Amended effective 21.11.17
6. *For 022x messages, TAG values should be taken from the original 0200 transaction with the exception of TAG 8A which is an ATM generated value and must be passed to the Issuer unaltered.* Amended effective 21.11.17
7. *Mandatory if 8A is used to generate the ARPC cryptogram in contact responses.* Inserted effective 21.11.17

A.14 Response Codes**A.14.1 Response Codes Table**

| Code | Meaning | Action |
|-------------|------------------------------|------------------------------------|
| 08 | Honour with signature | Approve after signature validation |
| 12 | Invalid Transaction | Decline Transaction |
| 13 | Invalid Amount | Decline Transaction |
| 14 | Invalid Card Number | Decline Transaction |
| 15 | No such Issuer | Decline Transaction |
| 19 | Re-enter Transaction | Decline Transaction – retry |
| 21 | No action taken | Unmatched reversal processing |
| 30 | Format Error | Decline Transaction |
| 31 | Bank not supported by switch | Decline Transaction |
| 33 | Expired Card | Decline Transaction, retain Card |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| Code | Meaning | Action |
|------|---|--|
| 34 | Suspected fraud | Decline Transaction, retain Card |
| 36 | Restricted Card | Decline Transaction, retain Card |
| 38 | Allowable PIN tries exceeded | Decline Transaction, retain Card |
| 40 | Requested Function Not supported | Decline Transaction |
| 41 | Lost Card | Decline Transaction, retain Card |
| 43 | Stolen Card | Decline Transaction, retain Card |
| 44 | No Investment account | Decline Transaction |
| 51 | Not sufficient funds | Decline Transaction |
| 52 | No Cheque account | Account requested not attached –declined |
| 53 | No Savings account | Account requested not attached –declined |
| 54 | Expired Card | Decline Transaction |
| 55 | Invalid PIN | Decline Transaction, Request PIN again |
| 56 | No Card record | Decline Transaction |
| 57 | Transaction not permitted to Cardholder | Decline Transaction |
| 58 | Transaction not permitted to Terminal | Decline Transaction |
| 61 | Exceeds withdrawal amount limits | Decline Transaction |
| 64 | Original amount incorrect | Decline Transaction |
| 65 | Exceeds Withdrawal Frequency Limit | Decline Transaction |
| 67 | Hot Card | Decline Transaction, retain Card |
| 91 | Issuer not available | Decline Transaction |
| 92 | Financial Institution/Intermediate network not found for routing. | Decline Transaction |
| 94 | Duplicate transmission | Decline Transaction |
| 95 | Reconcile error | |
| 96 | System malfunction | Decline Transaction |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| Code | Meaning | Action |
|------|---|---|
| 97 | Settlement date advanced by 1 and totals reset. Accompanied by '1' totals in balance or '2' (totals out of balance) in Bit 66 settlement Code | Complete - approved Transaction |
| 98 | MAC error | Decline Transaction. Request Key change |

A.14.2 Permitted Response Codes

| | | 0210 | 0230 | 0430 | 0530 | 0810 | 0830 |
|--------------------------------------|----|------|------|------|------|------|------|
| Successful | 00 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Refer to Card Issuer | 01 | ✓ | | | | | |
| Pick up Card | 04 | ✓ | | | | | |
| Do not honour | 05 | ✓ | | | | | |
| Error | 06 | | | | | | |
| Honour with signature | 08 | ✓ | | | | | |
| Invalid Transaction | 12 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Invalid Amount | 13 | ✓ | | | | | |
| Invalid Card number | 14 | ✓ | | | | | |
| No such Issuer | 15 | ✓ | ✓ | | | | |
| Re-enter Transaction | 19 | ✓ | | | | | |
| No action taken (unmatched reversal) | 21 | | | ✓ | | | |
| Format error | 30 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bank not supported by switch | 31 | ✓ | ✓ | ✓ | | | |
| Expired Card | 33 | ✓ | | | | | |
| Suspected fraud | 34 | ✓ | | | | | |
| Restricted Card | 36 | ✓ | | | | | |
| Allowable PIN retries exceeded | 38 | ✓ | | | | | |
| Requested function not supported | 40 | ✓ | | | | | |
| Lost Card | 41 | ✓ | | | | | |
| Stolen Card | 43 | ✓ | | | | | |
| No investment account | 44 | ✓ | | | | | |
| Not sufficient funds | 51 | ✓ | | | | | |
| No cheque account | 52 | ✓ | | | | | |
| No savings account | 53 | ✓ | | | | | |

ANNEXURE A. STANDARD INTERCHANGE SPECIFICATION

| | | 0210 | 0230 | 0430 | 0530 | 0810 | 0830 |
|---|----|------|------|------|------|------|------|
| Expired Card | 54 | ✓ | | | | | |
| Invalid PIN | 55 | ✓ | | | | | |
| No Card record | 56 | ✓ | | | | | |
| Transaction not permitted to Cardholder | 57 | ✓ | | | | | |
| Transaction not permitted to Terminal | 58 | ✓ | | | | | |
| Exceeds withdrawal amount limits | 61 | ✓ | | | | | |
| Original amount incorrect | 64 | | ✓ | | | | |
| Exceeds withdrawal frequency limit | 65 | ✓ | | | | | |
| Hot Card | 67 | ✓ | | | | | |
| Issuer not available | 91 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| No route | 92 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Duplicate transmission | 94 | ✓ | ✓ | ✓ | | | |
| Reconcile Error | 95 | | | | ✓ | | |
| System malfunction | 96 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Settlement Date advanced | 97 | | | | ✓ | | |
| MAC error | 98 | ✓ | ✓ | ✓ | ✓ | | |

Next page is B.1

ANNEXURE B. INTERCHANGE BIT MAP

| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
|--------------------------------------|----------|---|---|---|---|---|---|---|---|---|---|---|---|
| | B | 2 | 2 | 2 | 2 | 4 | 4 | 5 | 5 | 8 | 8 | 8 | 8 |
| | I | 0 | 1 | 2 | 3 | 2 | 3 | 2 | 3 | 0 | 1 | 2 | 3 |
| | T | 0 | 0 | X | 0 | X | 0 | X | 0 | 0 | 0 | 0 | 0 |
| Bit Map Extended | 1 | — | — | C | — | M | — | M | M | M | M | M | M |
| Primary Account Number | 2 | C | — | C | — | C | — | — | — | — | — | — | — |
| Processing Code | 3 | M | M | M | M | M | M | — | — | — | — | — | — |
| Amount, Transaction | 4 | M | M | M | M | M | M | — | — | — | — | — | — |
| Transmission Date & Time | 7 | M | M | M | M | M | M | M | M | M | M | M | M |
| System Trace Audit Number | 11 | M | M | M | M | M | M | M | M | M | M | M | M |
| Time, local Transaction | 12 | M | — | M | — | M | — | — | — | — | — | — | — |
| Date, local Transaction | 13 | M | — | M | — | M | — | — | — | — | — | — | — |
| Date, expiry | 14 | C | — | C | — | C | — | — | — | — | — | — | — |
| Date, settlement | 15 | M | M | M | M | M | M | M | — | — | — | — | — |
| Merchant's type | 18 | M | — | M | — | — | — | — | — | — | — | — | — |
| POS Entry Mode | 22 | M | — | M | — | — | — | — | — | — | — | — | — |
| Card Sequence Number | 23 | C | — | C | — | — | — | — | — | — | — | — | — |
| POS Condition Code | 25 | M | — | M | — | M | — | M | — | — | — | — | — |
| Amount, Transaction Fee | 28 | — | — | — | — | — | — | — | — | — | — | — | — |
| Acquiring Institution ID code | 32 | M | M | M | M | M | M | M | M | — | — | — | — |
| Forwarding Institution ID code | 33 | C | C | C | C | C | C | — | — | M | M | M | M |
| Track 2 data | 35 | C | — | C | — | C | — | — | — | — | — | — | — |
| Retrieval Reference Number | 37 | M | M | M | — | M | — | — | — | — | — | — | — |
| Authorisation ID Response | 38 | — | — | M | — | — | — | — | — | — | — | — | — |
| Response Code | 39 | — | M | — | M | — | M | — | M | — | M | — | M |
| Card Acceptor Terminal ID | 41 | M | M | M | M | M | M | — | — | — | — | — | — |
| Card Acceptor ID Code | 42 | M | M | M | M | M | M | — | — | — | — | — | — |
| Card Acceptor Name/Location | 43 | M | — | M | — | M | — | — | — | — | — | — | — |
| Additional Data - National | 47 | C | C | C | — | C | — | — | — | — | — | — | — |
| Additional Data - private | 48 | O | — | O | — | O | — | — | — | M | M | M | M |
| PIN Data | 52 | C | — | — | — | — | — | — | — | — | — | — | — |
| Security Related Control Information | 53 | M | M | M | M | M | M | M | M | — | — | C | C |
| Amount Cash | 57 | M | M | M | M | M | M | — | — | — | — | — | — |
| Ledger Balance | 58 | — | C | — | — | — | — | — | — | — | — | — | — |
| Account Balance, cleared funds | 59 | — | C | — | — | — | — | — | — | — | — | — | — |
| Mac | 64 | M | M | C | M | — | M | — | — | — | — | — | — |
| Settlement Code | 66 | — | — | — | — | — | — | — | M | — | — | — | — |
| Network management Information Code | 70 | — | — | — | — | — | — | — | — | M | M | M | M |
| Credits, Number | 74 | — | — | — | — | — | — | M | M | — | — | — | — |
| Credit Reversals, number | 75 | — | — | — | — | — | — | M | M | — | — | — | — |
| Debits, Number | 76 | — | — | — | — | — | — | M | M | — | — | — | — |
| Debit Reversals, Number | 77 | — | — | — | — | — | — | M | M | — | — | — | — |
| Transfers, Number | 78 | — | — | — | — | — | — | M | M | — | — | — | — |
| Transfer Reversals, Number | 79 | — | — | — | — | — | — | M | M | — | — | — | — |
| Inquiries, Number | 80 | — | — | — | — | — | — | M | M | — | — | — | — |
| Authorisations, Number | 81 | — | — | — | — | — | — | M | M | — | — | — | — |
| Credits, Transaction Fee Amount | 83 | — | — | — | — | — | — | — | — | — | — | — | — |

ANNEXURE B. INTERCHANGE BIT MAP

| | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|--------------------------------|-----|---|---|---|---|---|---|---|---|---|---|---|---|
| B | | 2 | 2 | 2 | 2 | 4 | 4 | 5 | 5 | 8 | 8 | 8 | 8 |
| I | | 0 | 1 | 2 | 3 | 2 | 3 | 2 | 3 | 0 | 1 | 2 | 3 |
| T | | 0 | 0 | X | 0 | X | 0 | X | 0 | 0 | 0 | 0 | 0 |
| Debits, Transaction Fee Amount | 85 | — | — | — | — | — | — | — | — | — | — | — | — |
| Credits, Amount | 86 | — | — | — | — | — | — | M | M | — | — | — | — |
| Credit Reversals, Amount | 87 | — | — | — | — | — | — | M | M | — | — | — | — |
| Debits, Amount | 88 | — | — | — | — | — | — | M | M | — | — | — | — |
| Debit Reversals, Amount | 89 | — | — | — | — | — | — | M | M | — | — | — | — |
| Original Data Elements | 90 | — | — | — | C | — | M | — | — | — | — | — | — |
| Amount, Net Settlement | 97 | — | — | — | — | — | — | M | M | — | — | — | — |
| Settlement Institution ID Code | 99 | — | — | — | — | — | — | M | M | — | — | — | — |
| Receiving Institution ID Code | 100 | — | — | — | — | — | — | — | — | M | M | M | M |
| Cash, Total Number | 118 | — | — | — | — | — | — | M | M | — | — | — | — |
| Cash, Total Amount | 119 | — | — | — | — | — | — | M | M | — | — | — | — |
| MAC | 128 | — | — | — | C | — | M | — | M | M | — | — | — |

This table specifies fixed formats for all messages. "M" signifies that a data element is mandatory, "C" signifies that it is conditional, while "□" signifies that it is not permitted. Optional data elements are signified by the letter "O".

Next page is C.1

ANNEXURE C. TECHNOLOGY FALLBACK**C.1 Introduction**

The specifications that are outlined here are to be used where the Terminal through a malfunction of the ICC interface device (IFD) or the ICC, is unable to read the track 2 information from the ICC.

C.2 Technology Fallback

Technology fallback is not permitted subsequent to a successful application select command.

C.3 Field 47

Field 47 must contain the Faulty Card Read indicator FCR\ to indicate that an unsuccessful attempt was made to read the ICC.

C.4 Terminal Capability Code (047)

The message must contain an indicator in field 47 to define the capabilities of the Terminal. The value "TCCnn\" must be present and coded in accordance with AS 2805-2 clause 4.4.25.21 (amendment 2 to AS 2805.2-2007).

Next page is D.1

ANNEXURE D. COMMUNICATIONS PHILOSOPHY

There are a number of statements which together may be seen as encapsulating the philosophy for communications between any two Interchange parties.

- (a) A communications link will be maintained between the two interchange nodes for testing purposes. This link will remain in place indefinitely after testing the initial implementation to enable bilateral testing of modifications and enhancements.
- (b) Sufficient lines will be provided between the parties production sites such that, should any single line become inoperative, the remaining lines will be able to carry the anticipated peak load of Interchange Transactions at that time.
- (c) The parties will seek to have production Interchange line connected by alternative routes to minimise the impact of single communication network failures.
- (d) The parties will regularly ensure that each Interchange Link installed is operational, so that the loss of one Interchange Link will not cause a total loss of service.
- (e) Triple DES, line encryption must be used across all production lines.

Next page is E.1

ANNEXURE E. STANDARD INTERCHANGE TERMS

E.1 Application to Third Party Agreements

To the extent that performance of these Standard Interchange Terms depends upon the actions of a third party who is represented by An IA Participant, the IA Participant must ensure that the third party agreement imposes obligations on the third party to perform those actions. The IA Participant remains responsible for ensuring that the obligations under these Standard Interchange Terms are met.

E.2 Approved Cards

- (a) Each Acquirer shall accept Cards of Approved Cardholders at its ATMs for the purpose of making ATM Transactions.
- (b) Each IA Participant (Issuer) warrants to each other IA Participant (Acquirer) that:
 - (i) reasonable care and diligence has been taken in investigating the integrity of its Approved Cardholders;
 - (ii) all details of all current ATM Cards issued by it or a third party which it represents (including lost and stolen Cards) are updated daily within the relevant computer system to enable authorisation requests to be answered promptly; and
 - (iii) there will not be any terms and conditions imposed upon Approved Cardholders in conflict with this Code.

E.3 Promotions and Advertising

- (a) Each IA Participant may display signage at its respective ATM locations which indicates the ATM Cards of IA Participants that are acceptable for ATM use. Each IA Participant will bear its own expenses in displaying such signage.
- (b) Each IA Participant authorises each other IA Participant to use its mark, logo and name for the purpose of promoting ATM interchange to their respective Approved Cardholders.

E.4 Indemnity and Limitation of Liability

- (a) For the purposes of this clause “**Interchange Facility**” means the combination of hardware, software, communications lines and operational procedures which enables the exchange, authorisation and reconciliation of ATM Transactions between IA Participants or, where an IA Participant is a Clearing/Settlement Agent, between the IA Participant and the third party they represent in accordance with the third party agreement (the **Interchange Facility**).

- (b) Each IA Participant warrants to each other IA Participant that the Interchange Facility which it operates or controls:
 - (i) will comply in all material respects with the requirements of this Framework and any technical requirements specified by the Company from time to time; and
 - (ii) will be operated competently.
- (c) If an IA Participant commits any error or omission in the operation of the Interchange Facility, or fails or is unable for any reason to furnish, deliver or transmit an ATM Transaction as provided for by this Code, or in so supplying, delivering or transmitting an ATM Transaction, or operating the Interchange Facility commits an error or omission or does any act or thing incidental thereto which causes the other party to suffer loss or damage, the maximum liability or responsibility towards the affected IA Participant shall be:
 - (i) to correct the operation of the Interchange Facility or ATM Transaction; or
 - (ii) to furnish and transmit the ATM Transaction to the affected IA Participant as soon as is reasonably practical.
- (d) Each IA Participant agrees to indemnify each other IA Participant against direct losses which are the result of any person's negligent or fraudulent use of an ATM Card and PIN issued by the indemnifying IA Participant, to effect an ATM Transaction. However, the indemnifying IA Participant is not responsible for losses that occur:
 - (i) even though the indemnifying IA Participant did not authorize the ATM Transaction; and/or
 - (ii) as a result of another IA Participant's non-compliance with any requirement of this Code or the IAC Manual.

E.5 Direct Charging

- (a) Subject to paragraph (b), an Issuer may, at its absolute discretion, decline an ATM Transaction.
- (b) An Issuer must not decline an ATM Transaction solely because it is subject to a Direct Charge.

E.6 Variation

IA Participants may bilaterally agree to vary a Standard Interchange Term.

Next page is F.1

ANNEXURE F. DIRECT CHARGING RULES

This Annexure F contains the rules and standards that must be followed by:

- (a) Acquirers who acquire ATM Transactions involving an ATM Operator Fee; and
- (b) Issuers who engage in Interchange with an Acquirer with respect to such ATM Transactions.

Note: the Standard Interchange Terms in Annexure E oblige parties to ATM Interchange to comply with the rules specified in this Annexure F.

F.1 General Principles

An Acquirer may charge an ATM Operator Fee if it complies with:

- (a) this Annexure F and, in particular, the obligation to disclose to the Cardholder the amount of the ATM Operator Fee at a time that allows the Cardholder to cancel the Transaction without incurring the ATM Operator Fee (or any other fee); and
- (b) any other applicable provisions in this Code.

For the avoidance of doubt this Annexure F has no application to 'on-us' ATM Transactions.

F.2 Amount and Variation of the ATM Operator Fee and Declines

This Annexure F does not in any way restrict:

- (a) the amount of the ATM Operator Fee that an Acquirer may charge a Cardholder;
- (b) the right of an Acquirer to vary the amount of its ATM Operator Fees; or
- (c) the right of an Issuer to decline an ATM Transaction.

F.3 When Cardholders may be charged an ATM Operator Fee

F.3.1 Cash Withdrawal and Balance Inquiries

Acquirers may charge Cardholders an ATM Operator Fee for a Cash Withdrawal or a Balance Inquiry.

F.3.2 When an ATM Operator Fee may not be charged

No ATM Operator Fee may be charged if:

- (a) a Cash Withdrawal or a Balance Inquiry is declined by the Issuer;

- (b) a Cash Withdrawal results in a Partial Dispense; or
- (c) a Cash Withdrawal or a Balance Inquiry is not completed successfully.


F.4 Disclosure Rules

F.4.1 Pre-transaction (Idle State) On Screen Display of ATM Operator Fees

Inserted effective
31.3.17

- (a) The minimum ATM Operator Fee and maximum ATM Operator Fee that may be directly charged by the ATM Operator for Cash Withdrawals and Balance Inquiries initiated by Cardholders using domestically-issued Cards must be displayed on an ATM Screen in the ATM Terminal's screen rotation in idle state (**Idle State Fee Display**).
- (b) The Idle State Fee Display:
 - (i) may be displayed with other messages or material displayed on that rotation screen, but must be presented in a font type and size that is clear and legible; and
 - (ii) must specify that the minimum and maximum ATM Operator Fees which may be charged by the ATM Operator are direct charges; but
 - (iii) is not required to include any reference to ATM Operator Fees that may be charged by the ATM Operator in relation to Cash Withdrawals and Balance Inquiries initiated by Cardholders using international Cards.

As an example:




Fees may apply to the use of this ATM.

Cash withdrawals and balance inquires at this ATM are free to our customers and our partners' customers.

A maximum direct charge of \$X.XX may apply to transactions initiated by customers of other Australian financial institutions using Australian cards.

OR

Direct charges of between \$X.XX and \$X.XX apply to cash withdrawals and balance inquiries initiated by users with Australian cards at this ATM.



-
- (c) Each ATM Framework Participant must provide written confirmation of its compliance with the requirements in clause F.4.1, and any details of material non-compliance, within 10 Business Days of request from the Secretary.
 - (d) Each ATM Framework Participant authorises and consents to the disclosure by the Secretary of the compliance information described in clause F.4.1(c) to the RBA.

F.4.2 On Screen

The Cardholder must be advised of any ATM Operator Fee that will apply to a Cash Withdrawal or Balance Inquiry. This advice must:

- (a) be given on the ATM Screen as early as possible in the Transaction sequence;
- (b) clearly and unambiguously display the ATM Operator Fee at a time that allows the Cardholder to cancel the requested Cash Withdrawal or Balance Inquiry without incurring the ATM Operator Fee or any other fee;
- (c) comply with the following minimum requirements:
 - (i) inform the Cardholder he or she will be charged the ATM Operator Fee if he or she proceeds with the Transaction;
 - (ii) display the amount of the ATM Operator Fee that will be charged (Note: the display must show the amount of the fee in dollars and cents. Displaying a percentage value of the Transaction amount is not permitted);
 - (iii) display the entity responsible for managing Cardholder enquiries concerning the ATM Operator Fee (not the Issuer) including contact details, which must take the form of a contact number or URL;
 - (iv) state that the Issuer may also charge the Cardholder a fee;
 - (v) indicate how to CANCEL the Transaction; and
- (d) indicate how to ACCEPT the ATM Operator Fee and proceed with the Transaction; and
- (e) if a Cardholder performs more than one ATM Transaction in a single session then the requirements in (a), (b) and (c) above must be complied with for each ATM Transaction in respect of which the Cardholder will be charged an ATM Operator Fee.

(Note: each Acquirer should consider the GST law and how it may apply to ATM Operator Fees. Whether or not an ATM Operator Fee is being levied by an Authorised Deposit Taking Institution may be a relevant consideration.)

For example:

If you continue with this transaction, you will be charged
\$X.XX
by the [institution responsible for the transaction and contact
number or url]

Your card Issuer may also
charge you a fee for using this ATM

Continue

Cancel

F.5 Record of Transaction

If the Cardholder elects to receive a Record of Transaction (that is, a receipt) then the Record of Transaction must comply with the following minimum requirements (in addition to those specified in Part 4, clause 4.3(c)):

- (a) the ATM Operator Fee must be itemised as a discrete item and not be bundled together with any withdrawal amount;
- (b) the ATM Operator Fee must be described as an “ATM Operator Fee” or similar; and
- (c) the recipient of the ATM Operator Fee or the entity responsible for managing Cardholder enquires regarding the fee (that is either the Acquirer or the ATM Deployer) must be displayed, including contact details, which must take the form of a contact number or URL.

For example:

TRANSACTION RECORD

| | | |
|-------------------|---------------|---------------------|
| DATE: xx/xx/xx | TIME xx:xx | TERMINAL ATMXXXX |
|-------------------|---------------|---------------------|

Card Number 501233*****123
Seq. Number 000123

| | |
|--------------------------|-----------------|
| Withdrawal | \$XXX.xx |
| ATM Operator Fee | \$X.xx |
| Available Balance | \$XXX.xx |
| Current Balance | \$XXX.xx |

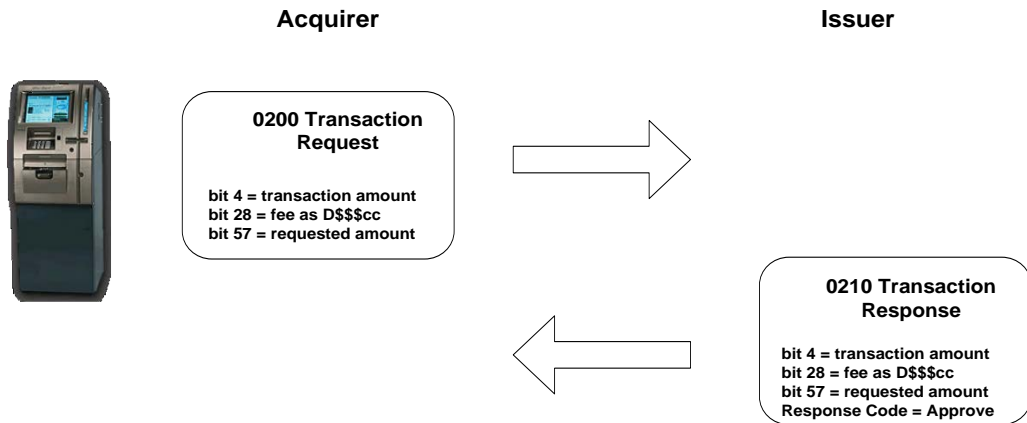
Thank you for using “ACQUIRER NAME”

Please contact us at www.ACQUIRERNAME.com.au or 1800 123 321

F.6 Message Flow

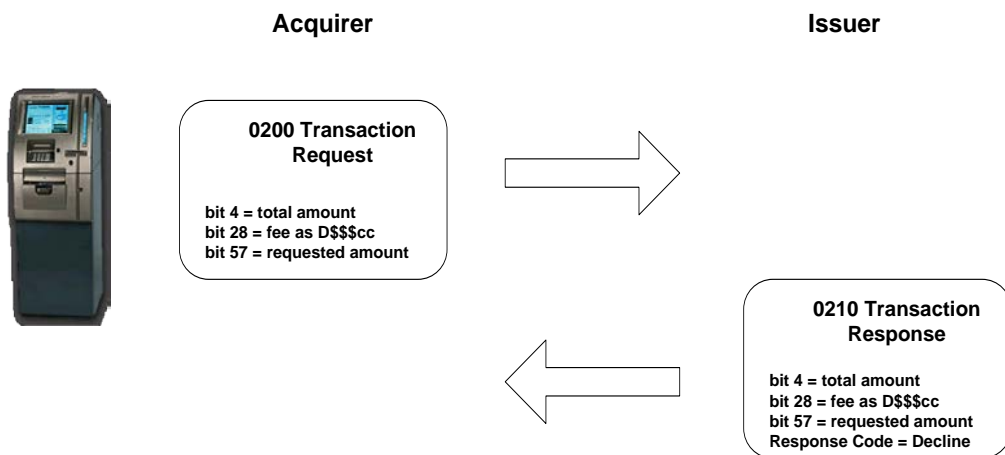
F.6.1 Cash Withdrawal

The ATM Operator Fee is to be contained in bit 28 as an 'X + n8' field of the Financial Transaction Request and Response messages (see AS 2805 -2:2007 clause 4.4.5). The 'X' portion of the fee data element will contain a 'D' to indicate that the fee is due the Acquirer. Standard, error free, message flow is illustrated below.



F.6.2 Declined ATM Transactions

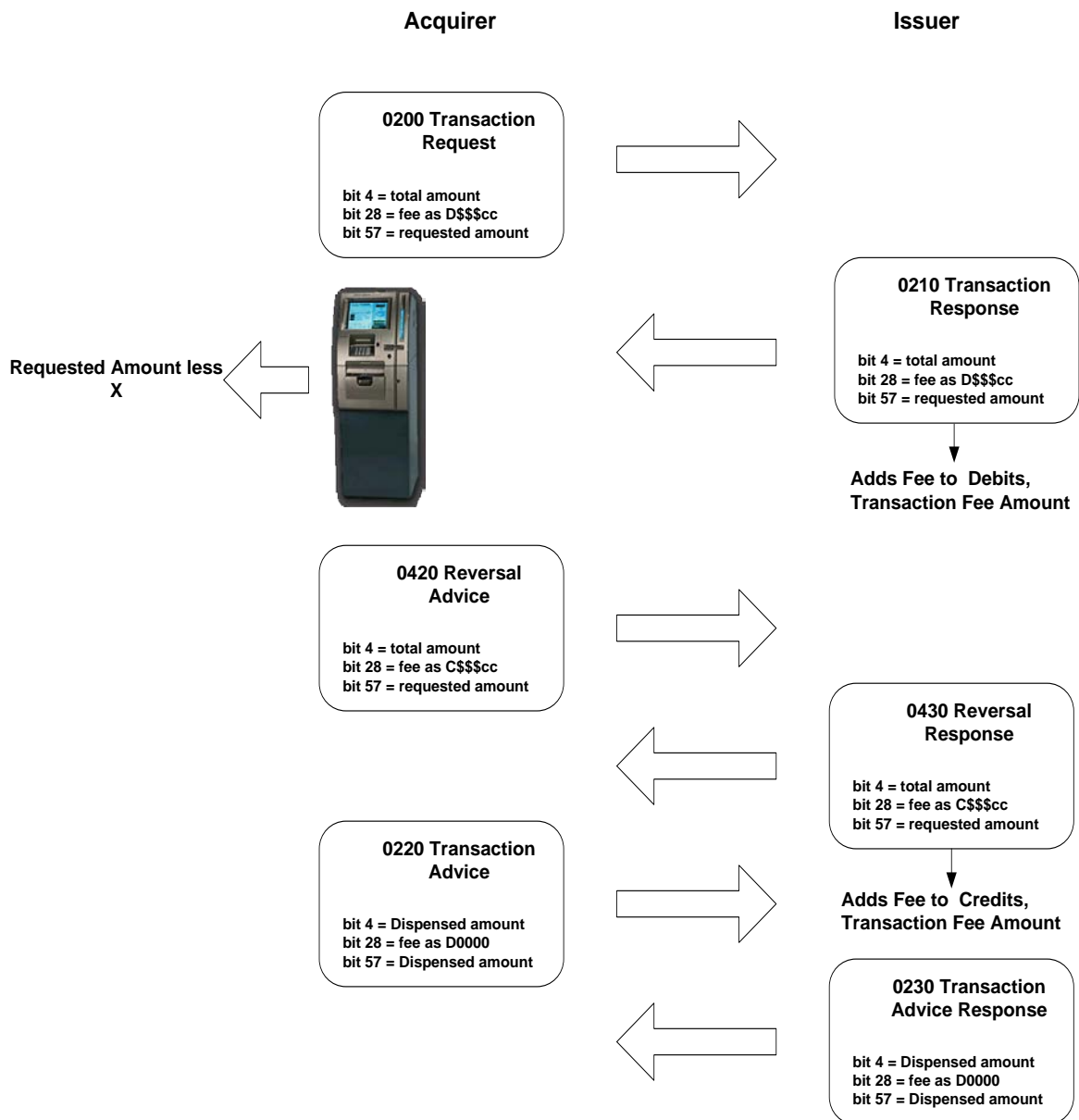
No fees are to be levied on failed or declined ATM Transactions. In the case of a decline, bit 28 will contain (as an echo) the fee amount from the Transaction request message, acquirers must take care that such fees are not accumulated. The message flow is illustrated below.



F.6.3 Partial Dispense and Fees

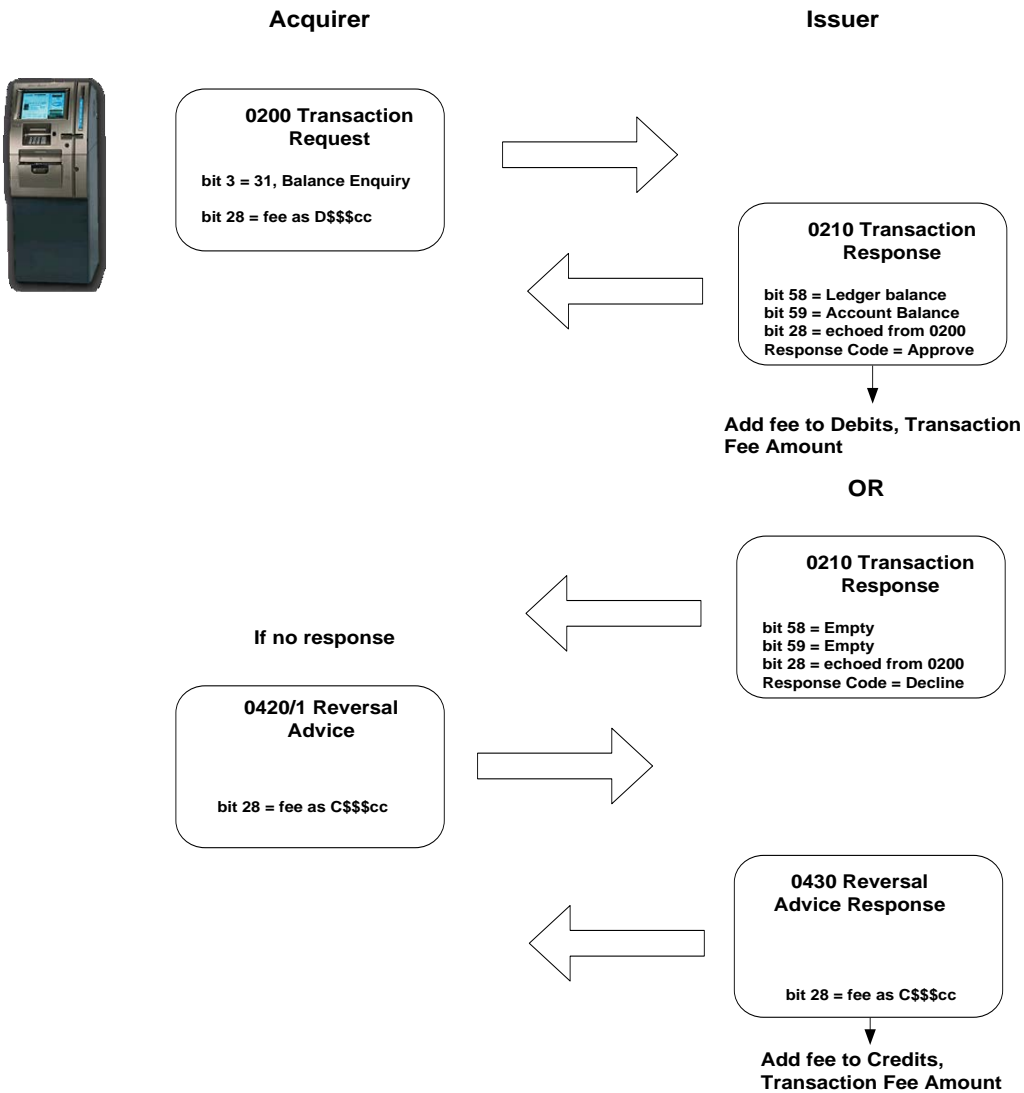
The operation of a Partial Dispense is illustrated below. The essential features are:

- (a) The Acquirer will initiate an 0420 Reversal Advice Message with bits 4 (Amount, Transaction) and bit 57 (Amount, cash) identical to the 0200 Request message. Bit 28 (Amount, Transaction Fee) will be identical to the same field in the request message but with the indicator digit 'X' set to 'C' for credit.
- (b) In the subsequent Transaction Advice message, bit 4 and 57 will contain identical amounts and be equal to the actual amount dispensed by the ATM. In the Transaction Advice message bit 28 must be set to zero ('D000000000000') as no ATM Operator Fee is applicable in this case (see clause F.4.2 above).



F.6.4 Balance Inquiries

- (a) ATM Operator Fees may be levied on Balance Inquiries. To prevent the ATM Operator Fee overdrawing the account Issuers may, in cases where this could occur, decline the Transaction (response Framework = 51 – insufficient funds).
- (b) The balance returned must reflect the impact of the ATM Operator Fee.
- (c) The inclusion of an ATM Operator Fee converts a Balance Inquiry Transaction to a financial Transaction (previously a non-financial Transaction) as such the fee value must be included in daily Interchange Settlement Reports.
- (d) Acquirers must ensure that full reversal processing is available on Balance Inquiries. Bit 28 of the 0420 message shall contain the same value as in the 0200 message but with the indicator 'X' set to 'C' indicating the value is owed to the Issuer.



F.6.5. Use of Bit 28 when no ATM Operator Fee is being levied

Bit 28 is a conditional field that does not have to be present for every ATM Transaction. If an ATM Operator Fee is being levied then it must be included in the 0200 message and all subsequent messages (as described above). However if an ATM Operator Fee is not being levied then bit 28 can either be omitted or included with the n8 component being set to zero. Issuer systems must accommodate both possibilities.

F.7 Settlement of ATM Operator Fees

ATM Operator Fees must be included in daily settlement figures and settled in accordance with IAC Code Set Volume 5 (Settlement).

Amended
effective 1.1.16

F.8 Transition

For a period of 3 months commencing on the ATM Direct Charging Date an Acquirer may comply with the rules in this clause F.8 in lieu of compliance with the disclosure rules in clause F.3.

F.9 Damages for Non-compliance with Direct Charging Rules

- (a) This clause F.8 applies to Direct Charging Systems Error. In this Code, a Direct Charging Systems Error is a systems error that:
- (i) causes material non-compliance with these Direct Charging Rules; and
 - (ii) affects 10 or more ATM Transactions.
- (b) Each IA Participant agrees that the amount of \$7,500.00 is a conservative and genuine pre-estimate of the total loss that all IA Participants that are ATM Issuers will suffer as a result of a Direct Charging Systems Error.
- (c) If a Direct Charging Systems Error occurs, then:
- (i) the loss suffered by each IA Participant that is an Issuer (Issuer Framework Participant) as a result is presumed to be \$7,500 multiplied by the IA Participant's Issuing Share where "Issuing Share" means an IA Participant's Cards Market Share (as defined in the Company's Constitution) attributable to its activities as an Issuer; and
 - (ii) the IA Participant responsible for the ATMs affected by the Direct Charging System Error ("Responsible Framework Participant") must:
 - (A) pay Company the sum of \$7,500.00 multiplied by the IA Participant's Issuing Share; and

- (B) rectify the Direct Charging Systems Error as soon as practicable.
- (d) All sums received by the Company pursuant to sub-clause (c) (A) above must be applied by the Company to operating costs and expenses which would otherwise be borne by Framework Participants pursuant to the IAC Regulations.
- (e) The presumption in sub-clause (c)(i) above will cease to apply between the Responsible Framework Participant and an Issuer Framework Participant if either of them establish (to the satisfaction of the other or by Dispute Resolution pursuant to Part 12 of the IAC Regulations) that the liability of the Responsible Framework Participant to the Issuer Framework Participant differs from the amount prescribed by sub-clause (b). If this occurs then any amounts received by the Issuer Framework Participant pursuant to sub-clause (c) must be taken into account in determining the amount due and payable between the Responsible Framework Participant and the Issuer Framework Participant.
- (f) Issuers will not seek additional compensation for any loss suffered as a result of a Direct Charging Systems Error from the Responsible Framework Participant pursuant to Part 12 of the IAC Regulations.
- (g) Nothing in this clause F.8 affects the right of the Responsible Framework Participant to seek contribution and/or compensation for a Direct Charging Systems Error from a party with whom it has a third party agreement.

F.10 Prohibition on hindering or preventing Direct Charging

- (a) Where an Acquirer wishes to Direct Charge in respect of ATM Transactions with a Cardholder of an ATM Issuer, the Issuer must not engage in conduct that hinders or prevents that Acquirer from Direct Charging.
- (b) For the avoidance of doubt, clause F.9(a) does not prevent an Issuer from charging its Cardholders a fee for an ATM Transaction.

Next page is G.1

ANNEXURE G. EMV@ATM TERMINAL STANDARDSInserted effective
1.1.16**G.1 Cards****G.1.1 Identification of Australian IC Cards**

Australian IC cards are those in which the EMV Issuer Country Code data element (tag 5F28) is equal to "036" (Australia).

G.2 Card Acceptance

Acquirers should endeavour to support all Card types and applications commonly used by Australian Issuers. At a minimum AIDs of all Approved Card Payment Systems should be supported for the purpose of clause 4.5(a)(ii)(B). A list of Approved Card Payment Systems is published on the Company's extranet.

Amended effective
21.11.17**G.2.1 PAN sequence number**

As Issuers may choose to link multiple accounts to single PAN through the use of the EMV data element PAN Sequence Number (TAG 5F34), ATMs and Acquirers must ensure that this data element, if present in the Card, is sent to the Issuer in DE.23 (Card sequence number) to ensure successful processing of the Transaction.

G.3 Transactions support and processing

Mandatory supported Transactions are:

- (a) withdrawal;
- (b) balance; and
- (c) reversals of above.

Support for other Transaction types for "on-us Transactions" e.g., purchase, transfer, bill payment and top up is optional at Issuer discretion.

For cash withdrawal Transactions ATMs must adhere to the EMV protocol as defined in Book 3 of the EMV specifications for transaction type "cash".

For Balance Inquiry, and for Transfer and Deposit Transactions, (if supported), the ATM must adhere to the recommendations contained in the EMVCo document "Recommendations for EMV Processing for Industry-Specific Transaction Types". Other Transactions types e.g., bill payment and top up are to be defined and processed as Purchase Transactions.

G.4 Terminal Processing**G.4.1 ICC precedence**

ATM Transaction initiation must ensure that where Cards contain both a chip and a magnetic stripe, the chip is given precedence. If a magnetic stripe is read that includes either of the service codes 2xx or 6xx the Cardholder must be requested to insert the Card into the ICC reader and the ATM must not proceed with the Transaction, until such an action has occurred.

Where the ATM contains a motorised, combined magnetic-stripe and ICC reader the ATM must give precedence to the ICC, if present.

Where the Cardholder payment device contains both a contact and contactless interface the Cardholder may choose either of these interfaces without precedence subject to the ATM ensuring that any re-presentation of the Card is through an ICC interface.

G.4.2 Application name display

For contact Transactions the ATM must support the ability to allow the Cardholder to select an application or to confirm the application proposed by the terminal. When the ATM displays an application to the Cardholder, it shall display:

- (a) the Application Preferred Name (Tag 9F12), if present and if the Issuer Code Table Index (Tag 9F11) indicating the part of ISO/IEC 8859 to use is present and supported by the terminal (as indicated in Additional Terminal Capabilities); and
- (b) otherwise the Application Label, if present, by using the common character set of ISO/IEC 8859 (see Book 4 Annex B).

G.4.3 Candidate list filtering

Prior to displaying the candidate list to the Cardholder, the terminal shall look for any matching applications that contain the eftpos RID A000000384.

If found, then the candidate list will be further examined and any applications matching the AIDs identified in Table 2 shall be removed from the list prior to its presentation to the Cardholder.

| RID | PIX | AID | Application |
|------------|------|----------------|--------------------|
| A000000003 | 8010 | A0000000038010 | Visa Plus |
| A000000004 | 3060 | A0000000043060 | Mastercard Maestro |
| A000000004 | 6000 | A0000000046000 | Mastercard Cirrus |

Table 2 – Filtered AIDs

G.4.4 Application selection

Where there is only a single entry in the candidate list, such as for a single application Card, application selection must be automatic and transparent to the Cardholder.

For multiple application Cards, if using a contact interface, the candidate list containing all mutually supported applications should be presented to the Cardholder and the Cardholder offered the opportunity to select the application to use for the Transaction.

For multiple application Cards, when using a contactless interface, the highest priority application on the Card should be selected automatically.

G.4.5 Account selection**(a) Australian IC Cards – auto application selection**

Account selection is required for all single application Australian IC Cards. Accounts offered should include savings, cheque and credit. Account selection shall not be offered for all multiple application Australian IC Cards.

(Note: the above clause is applicable to all contact card reads, if contactless Cards are accepted, account selection is mandatory).

The account type code 1 (DE.3-2) (AS 2805-2 bit 3, positions 3 & 4) for these Transactions should be set to:

- 10 – where Account selected is Savings
- 20 – where Account selected is Cheque
- 30 – where Account selected is Credit

(b) Australian IC cards – Cardholder Application Selection

Account selection shall not be offered for all multiple application Australian IC Cards where contact card read occurs.

The account type code 1 (DE.3-2) (AS 2805-2 bit 3, positions 3 & 4) for these Transactions should be set to:

- 10 – where application selected is A00000038410 (eftpos Savings)
- 20 – where application selected is A00000038420 (eftpos Cheque)
- 00 – (Default Account) where application selection is other AID.

(c) International IC cards

Account selection for International Cards should follow the relevant Card scheme rules where these are known. In the absence of specific requirements account selection should not be offered.

The account type code 1 (DE.3-2) (AS 2805-2 bit 3, positions 3 & 4) for these Transactions should be set to 00 – (Default Account) where Account Selection is not specifically offered.

The account type code 1 (DE.3-2) (AS 2805-2 bit 3, positions 3 & 4) for these Transactions should be set to:

- 10 – where Account selected is Savings
- 20 – where Account selected is Cheque
- 30 – where Account selected is Credit

G.4.6 Account selection and downgrade

For the purposes of transition to full EMV capability on Interchange Links, where it becomes necessary to downgrade a Transaction, e.g., if the bilateral link is unable to forward DE55 (chip data) and field DE.3-2 is equal to default (00) the Acquirer should, examine the application used to create the Transaction (TAG 84 in DE55) and set the account type code 1 (DE.3-2) (AS 2805-2 bit 3, positions 3 & 4) as follows:

- 10 – where application used was A00000038410 (eftpos Savings)
- 20 – where application used was A00000038420 (eftpos Cheque)
- 30 – (Credit account) where application selection is other AID.

Further, the ATM may retrieve the Track Two Equivalent Data from the IC data. The Track Two Equivalent Data formatted in accordance with AS 3524 and clause 9.11.3 (Data Element 35) may be used to construct a Financial Request Message, which must be forwarded to the Issuer in accordance with magnetic stripe processing formats and rules (as contained in Annexure A of this ATM System Code).

Where this is done the POS entry mode must accurately reflect the source of the card information. If Track Two Equivalent Data is obtained from an Australian IC Card then POS entry code “051” (contact interface) or POS entry code “071” (contactless interface) must be used in the Financial Request Message.

G.4.7 Card verification

ATMs are not required to support any form of offline data authentication so it is strongly recommended that Issuers validate the ARQC as a fraud mitigation measure.

G.4.8 Authorisation response code

Where both TAG 8A and DE.39 are present, TAG 8A shall have precedence and shall be passed to the Card unaltered.

G.4.9 Chip decline

Should the chip return an AAC (Decline) in response to the second GENERATE AC command for an Issuer approved Transaction, the Transaction is to be declined and a reversal message forwarded to the Issuer.

G.4.10 Transaction certificates [Deleted]

Deleted effective
21.11.17

G.4.11 Chained transactions

ATMs may support additional Transactions without requiring the reinsertion of the Card. Single application Cards should return to the Transaction Type Selection step and use the saved encrypted PIN in any subsequent Transactions.

To avoid PIN verification failures, session key changes for PIN encryption keys should not occur during any chained sequence.

Further chained Transactions are not permitted subsequent to Card removal.

Note that this is in contravention of PCI-DSS requirements which do not allow a PIN to be stored even if encrypted subsequent to authorisation and that PCI requirements for ATMs are currently under review such that changes may be required in the future.

Multiple application Cards are, after clearing the encrypted PIN, to return to the Application selection step of the EMV processing cycle.

The prompt for "Further transactions" must also provide for a short duration timeout to ensure that the PIN is erased even if the Cardholder walks away from the ATM at that prompt.

G.4.12 PIN retention

To support chained Transactions, an encrypted PIN may be retained and reused in the subsequent Transaction if requested by the Cardholder. The encrypted PIN must be deleted at the end of the Cardholder session.

G.5 Technical Fallback

Where the chip data cannot be read due to a chip failure or IFD fault, the Transaction may continue using data read from the magnetic stripe only where no Cardholder action is required to transition from chip read to magnetic stripe read. Technical Fallback is not permitted subsequent to successful application selection.

Such Transactions are denoted to the Card Issuer by presence of FCR code in DE47. See clause C.3 of the IAC Code Set Volume 6 (Technology Fallback) for details.

As this feature may be removed at a future time, Acquirers and deployers should endeavour to ensure this feature can be readily disabled should that be required in the future.

G.5.1 Fallback

Inserted effective
21.11.17

There is only one type of fallback at ATM, it occurs when a chip Card, presented at a chip terminal, cannot be read due to a technical issue with the chip read which results in the technology “falling back” to a magnetic stripe transaction.

Valid reasons for a fallback transaction include;

1. a defective or scratched chip
2. a chip reader that is defective
3. a chip intentionally damaged so it cannot be read, on a counterfeit card encoded with magnetic data stolen from a chip card.
4. a card without a chip, encoded with magnetic data stolen from a chip card.

An ATM Terminal’s inability to recognise a particular application (AIDs that should be supported if that scheme is accepted by an Acquirer) is not a valid reason for a fallback transaction.

The following table G.5.1 sets out various scenarios of ICC card usage and the expected field values and guidance about potential liability outcomes.

Inserted effective
21.11.17

Refer to clause 4.5 for liability in the case of Counterfeit ATM Transactions. The transfer of liability to the acquirer only applies in those cases of counterfeit fraud of ICC Cards.

| Use Case Scenarios | Field 47 | | Field 22 | Field 55 | Card Service Code | Liability for Fraudulent Txns | Comments |
|---|----------|-------------|-------------------------|-------------|-------------------|---|---|
| | TCC | FCR | POS Entry Mode | EMV Data | | | |
| #1) Terminal not EMV Compliant | 01 | Not Present | 021 | Not present | 201/601 | Acquirer | Example: Terminal is EMV capable of VISA, however not EMV capable for ACe. An ACe Only card is presented. in the ATM. |
| #2) Downgrade @ Acquirer | 02-07 | Not Present | 051 or 071 | Not present | 201/601 | Party most responsible for non-compliance | Terminal compliant but either Acquirer/Issuer or bilateral link is not compliant |
| #3) Downgrade @ Switch (Hub) | 02-07 | Not Present | 051 or 071 | Not present | 201/601 | Issuer | |
| #4) Fallback due to faulty card read | 02-07 | FCR/ | 021 or 621 | Not present | 201/601 | Issuer | |
| #5) Fraudulent card service code rewritten | 02-07 | Not Present | 021 or 621 | Not present | 101 | Issuer | Acquirer cannot identify card as a chip card |
| #6) Fraudulent Card Blank card populated with stolen mag-stripe data | 02-07 | FCR/ | 021 or 621 | Not present | 201/601 | Issuer | |
| #7) Terminal without specific app support | 02-07 | Not Present | 021 ¹ or 621 | Not present | 201/601 | Acquirer | |
| | | | | | | | |

¹ We understand proprietary arrangements may use a value of 801 under this condition

Inserted effective
21.11.17

| Use Case Situations | Field 47 | | Field 22 | Field 55 | Card Service Code | Liability for Fraudulent Txns | Comments |
|---------------------------------------|----------------------------------|-------------|----------------|--|-------------------|-------------------------------|---|
| | TCC | FCR | POS Entry Mode | EMV Data | | | |
| #8) Full Compliance Contact interface | 02-07 | Not Present | 051 | 82,84,95,9A,9C,9F02,9F03,9F10,9F1A,9F26,9F27,9F35,9F36,9F37 ² | 201/601 | Issuer | |
| #9) Full Compliance contactless | 02-07 | Not Present | 071 | 82,84,95,9A,9C,9F02,9F03,9F10,9F1A,9F26,9F27,9F35,9F36,9F37 ³ | 201/601 | Issuer | |
| #10) Invalid messaging (1) | Absent or incorrect ⁴ | Not Present | 021 or 621 | Not present | 201/601 | Acquirer | IAC Rules require TCC represent the combined hardware and software functionality of the ATM |
| #11) Invalid messaging (2) | Absent ⁵ | | 021 or 621 | Not present | 201/601 | Issuer ⁶ | If Issuer unable to receive or process DE.47 they are unable to detect fallback txns so are also unable to determine valid claims |
| #12) Invalid ATM configuration | 02-07 | FCR/ | 021 or 621 | Not present | 201/601 | Acquirer | ATM unable to support a specific app and inappropriately submits it as fallback. |

² Other TAGs may be present see clause A.13.14 Volume 6, IAC Code Set. The TAGs would be present in both auth request and responses.

³ Other TAGs may be present see clause A.13.14 Volume 6, IAC Code Set. The TAGs would be present only in auth request, not in responses.

⁴ 02-07 if ATM is configured with EMV hardware and possibly incomplete app support

⁵ Field 47 is mandatory for all interchanges subsequent to EMV upgrade see IAC Code Set Volume 6 see clause A.12.3

⁶ Field 47 is mandatory for all interchanges subsequent to EMV upgrade see IAC Code Set Volume 6 see clause A.12.3

G.5.2 Identification of fallback transactions

An issuer may use a combination of fields to identify a fallback transaction. A typical fallback transaction request message (0200) should be coded as follows. Please note that 0220 advice messages are not used in the ATM environment for fallback.

Field 47 Additional Data National

Field 47 should contain the faulty card read flag FCR\ (clause G.5) and also the Terminal Capability Code TCCnn\ should be present with a value of “nn” between 2 and 7. The FCR\ flag indicates that an unsuccessful attempt was made to read the chip and the TCCnn\ indicates that the terminal has chip read capability.

| | |
|----|--|
| 00 | Unknown |
| 01 | Mag-stripe reader |
| 02 | Contact ICC reader |
| 03 | Magnetic-stripe and contact ICC readers |
| 04 | Contactless ICC reader |
| 05 | Magnetic-stripe and contactless ICC readers |
| 06 | Contact and contactless ICC readers |
| 07 | Magnetic-stripe, contact and contactless ICC readers |

Table 7 - TCCnn\ Values

Note that this value does not just represent the hardware capabilities of the ATM, rather TCC should be set to correctly represent both the hardware and software capabilities of the ATM.

Field 22 Point of sale entry mode

For a correctly coded fallback transaction field 22 should have a value of “621” indicating magnetic-stripe read in an ICC capable ATM.

Service Code (from track 2)

The expected service code encoded on the card must be 2xx or 6xx indicating the card is an ICC card. Note the acquirers will not be able to identify a counterfeit card where the fraudster has changed the value of the service code (provided they have also recalculated the LRC- Longitudinal Redundancy Check).

G.5.3 Fallback rates

Acquirers should endeavour to maintain fallback rates of less than 3% of the total transaction volumes processed over a month.

Faulty card and counterfeit card transactions should be excluded when considering fallback rates. An Issuer may notify AusPayNet if it considers that an Acquirer is consistently exceeding the recommended fallback rate.

G.6 Receipts

In addition to the requirements of clause 2.1.2 of Volume 3 (Acquirers Code) of the IAC Code Set, the value of the AID shall be printed or displayed on the receipt. The application label may be used as an alternative to the AID.

Amended effective 21.11.17

G.7 ATM configuration

The Terminal Type (TAG 9F35) shall be set to 14 or Unattended, On-line only, for all ATMs.

G.7.1 Terminal Capabilities (TAG 9F35)

Encoding of the Terminal capabilities (TAG 9F33), typically 0x60,0x40 or 0x20, is illustrated in Table 3 to Table 5 below. For additional details see EMV Book 4 Annex A.

| B8 | B7 | B6 | B5 | B4 | B3 | B2 | B1 | Meaning |
|----|----|----|----|----|----|----|----|-------------------------|
| 0 | X | X | X | X | X | X | X | Manual Key Entry |
| x | 1 | X | X | X | X | X | X | Magnetic Stripe |
| X | X | 1 | X | X | X | X | X | IC Reader with contacts |
| X | X | X | 0 | 0 | 0 | 0 | 0 | RFU |

Table 3 - Terminal Type Byte 1

| B8 | B7 | B6 | B5 | B4 | B3 | B2 | B1 | Meaning |
|----|----|----|----|----|----|----|----|--------------------------------|
| 0 | X | X | X | X | X | X | X | Plain text PIN – IC verify |
| x | 1 | X | X | X | X | X | X | Enciphered PIN – online verify |
| X | X | 0 | X | X | X | X | X | Signature |
| X | X | X | 0 | X | X | X | X | Enciphered PIN – ICC verify |
| X | X | X | X | 0 | X | x | x | No CVM Required |
| X | X | X | X | X | 0 | 0 | 0 | RFU |

Table 4 - Terminal Capabilities - Byte 2

| B8 | B7 | B6 | B5 | B4 | B3 | B2 | B1 | Meaning |
|----|----|-----|----|----|----|----|----|--------------|
| 0 | X | X | X | X | X | X | X | SDA |
| x | 0 | X | X | X | X | X | X | DDA |
| X | X | 0/1 | X | X | X | X | X | Card Capture |
| X | X | X | 0 | X | X | X | X | RFU |
| X | X | X | X | 0 | X | x | x | CDA |
| X | X | X | X | X | 0 | 0 | 0 | RFU |

Table 5 – Terminal Capabilities – Byte 3

G.7.2 ATM mandatory physical features

ICC Readers are required in all ATMs. These readers or Interface devices (IFD) must be capable of reading ISO/IEC 7816 compliant ICC cards with contacts. Additionally these readers must be EMVCo. Level 1 type approved (see G.7.3).

The provision of contactless ICC support is optional but where provided the reader must be capable of reading Cards compliant to ISO/IEC 10536-1, ISO/IEC 14443-1 or ISO/IEC 15693-1, as appropriate. Additionally these readers must be EMVCo. Level 1 type approved (see G.7.3).

G.7.3 EMV compliance

All ICC readers (EMV – IFD) must be type approved (Level 1) by EMVCo prior to deployment.

All contactless readers (EMV – proximity coupling device or PCD) must be type approved (Level 1) by EMVCo prior to deployment.

All Kernels must be EMVCo Level 2 type approved prior to deployment. For details of these approval requirements see <http://www.emvco.com/faq.aspx?id=40>.

All Kernels providing contactless reader support must conform to the requirements of EMVCo. – EMV Contactless Specification for Payment Systems – Book C 1,2,3 & 4 and be Card scheme approved. In addition, it must be ensured that all contactless kernels in an ATM must ensure the following Level 2 functions are provided for the acceptance of contactless Cards:

- (a) Device type unattended, online only, Operation control by financial institution;
- (b) Online only;
- (c) Only allowed Cardholder Verification Method (CVM) is online PIN;
- (d) Transactions supported are cash withdrawal, inquiry. Transfer, payment, cash deposit, and purchases are optional;
- (e) No support for offline data authentication (SDA, DDA, CDA); and
- (f) Device will decline Transaction in the case where online is not available.

G.7.4 CVM support

The only Card Holder Verification Method (CVM) to be supported is online encrypted PIN.

All devices must decline all Transactions if online is not available.

The only acceptable algorithm for PIN encipherment is DEA 3 (TDES) as specified in AS 2805 part 5.4.

G.7.5 Transaction sequencing

Optionally, at the end of a Transaction sequence the Cardholder may be prompted for another Transaction. In the case of ICC Cards the action to be taken will vary according to whether the Card has a single application or multiple applications (see clauses G.8.1 to G.8.4).

To support Transaction chaining, an encrypted PIN may be retained and reused in the subsequent Transaction if one is requested by the Cardholder. This encrypted PIN must be deleted at the end of the Cardholder session.

Chained Transactions are not permitted subsequent to Card withdrawal.

G.8 Preferred transaction flows

The preferred transaction flows reference “not on-us” Card processing requirements only and vary in accordance with the Card type – domestic or International, single or multi-application. Each of the possible permutations is illustrated in the following figures. Although these are the preferred flows, these rules place no restriction on Acquirers implementing other flows or sequences.

G.8.1 Single app International card

The preferred Transaction flow when an international ICC Card is presented to a chip enabled ATM where such results in only a single entry in the candidate list is illustrated in Figure 1. In this case application selection is to proceed without Cardholder interaction, Account selection should follow individual scheme requirements and where further transactions are requested to flow should return to the "Select Transaction Type" step.

Allowable Transactions types are limited to Cash Withdrawal and Balance Inquiry.

Where account selection has not been offered the *account type code 1* (DE.3-2) is to be set to 0x00 or Default. (AS 2805-2 bit 3, positions 3 & 4).

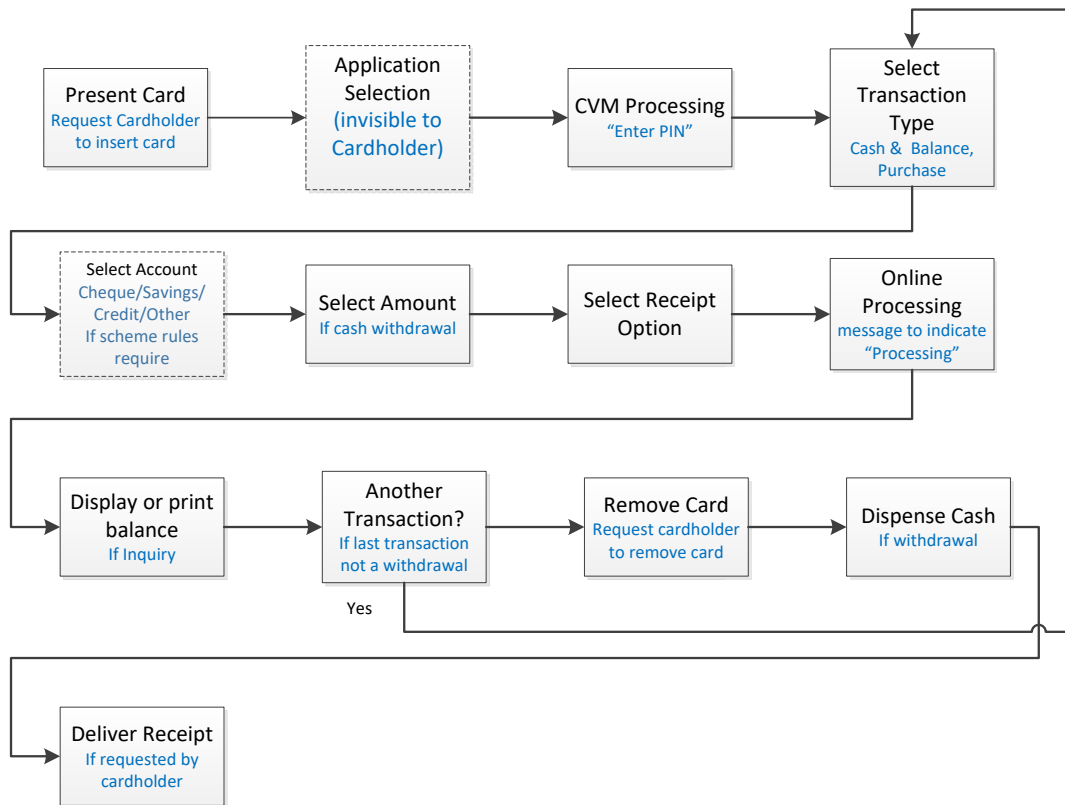


Figure 1- Single Application International Card

G.8.2 Multiple application International card

The preferred Transaction flow when an international ICC Card is presented to a chip enabled ATM where such results in multiple entries in the candidate list is illustrated in Figure 2. In this case application selection will require Cardholder interaction, Account selection is to be omitted unless required by individual Card scheme requirements. Where further Transactions are requested the flow should return to the "Application Selection" step, requiring the Cardholder to re-enter the PIN.

Allowable transactions types are limited to Cash Withdrawal and Balance Inquiry.

The *account type code 1* (DE.3-2), for these Transactions is to be set to 0x00 or Default. (AS 2805-2 bit 3, positions 3 & 4)

(Note that Card scheme rules may require account selection, in which case the scheme rules are to take precedence).

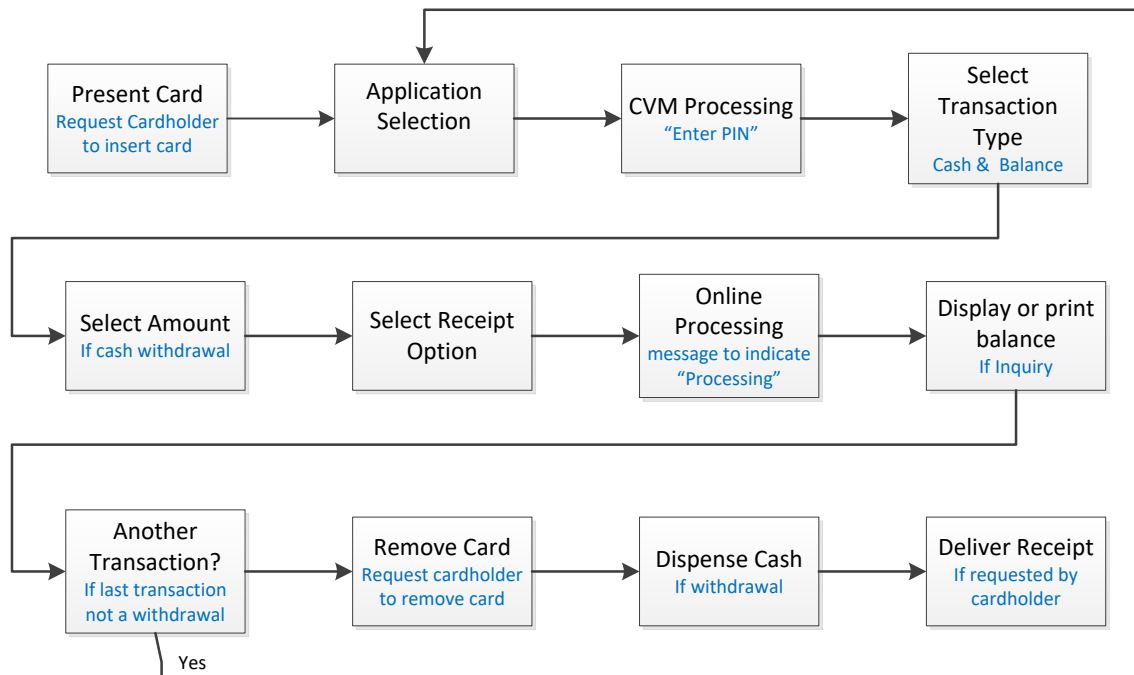


Figure 2- Multiple Application International Card

G.8.3 Single Application, Australian IC Card

The preferred Transaction flow when an Australian IC Card is presented to a chip enabled ATM where such results in a single entry in the candidate list is illustrated in Figure 3.

In this case application selection is to proceed without Cardholder interaction, Account selection is to be included and where further Transactions are requested to flow should return to the "Select Transaction Type" step.

Mandatory Transactions types are limited to Cash Withdrawal and Balance Inquiry.

The *account type code 1* (DE.3-2), for these transactions is to be set according to *account type code 1*. (AS 2805-2 refer to clause 4.4.11 of AS 2805.2-2007)

For domestic Cards the Issuer may need to select the account based on both the PAN and Pan Sequence Number if that option has been chosen by the Issuer, in which case the processing code is to be ignored.

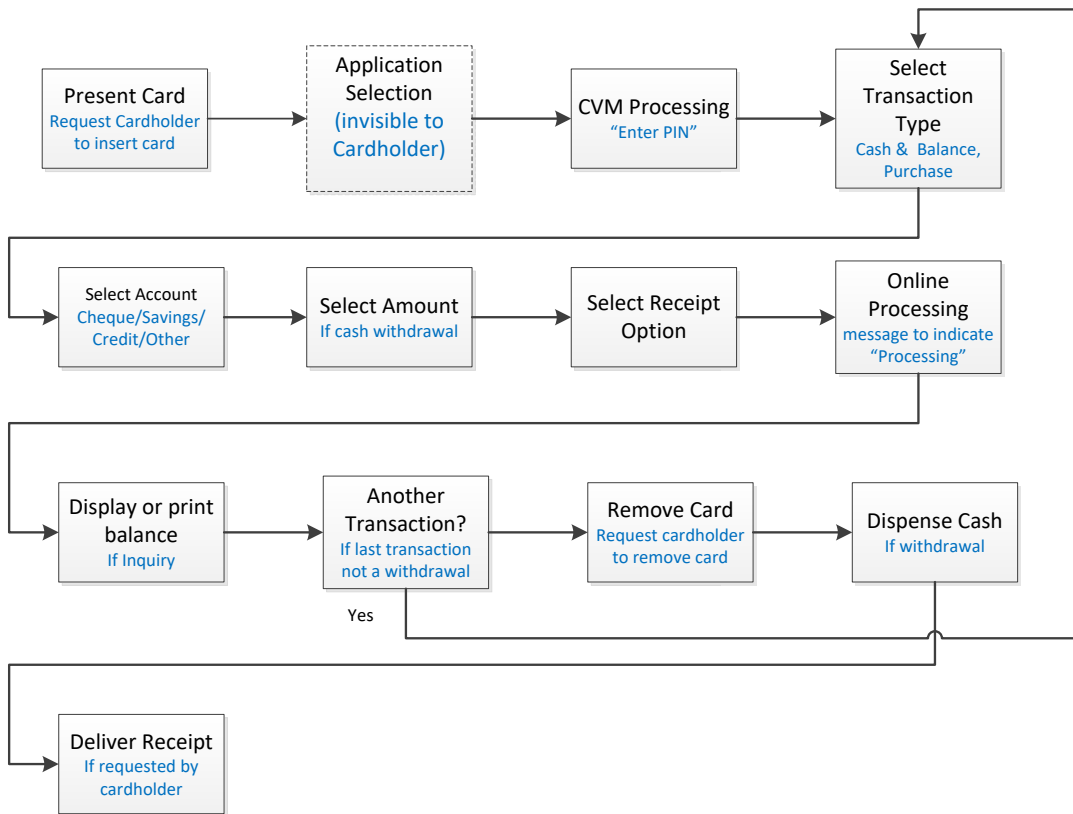


Figure 3- Single Application, Australian IC card

G.8.4 Multiple application Australian IC Card

The preferred Transaction flow when a domestic ICC Card is presented to a chip enabled ATM where such results in multiple entries in the candidate list is illustrated in Figure 4.

In this case application selection will require Cardholder interaction, Account selection is not required and where further Transactions are requested to flow should return to the "Select Application Type" step.

Mandatory Transactions types are limited to Cash Withdrawal and Balance Inquiry.

The *account type code 1* (DE.3-2), for these transactions is to be set according to *account type code 1*. (AS 2805-2 refer to clause 4.4.11 of AS 2805.2-2007)

For domestic Cards the Issuer may need to select the account based on both the PAN and Pan Sequence Number if that option has been chosen by the Issuer, in which case the processing code is to be ignored.

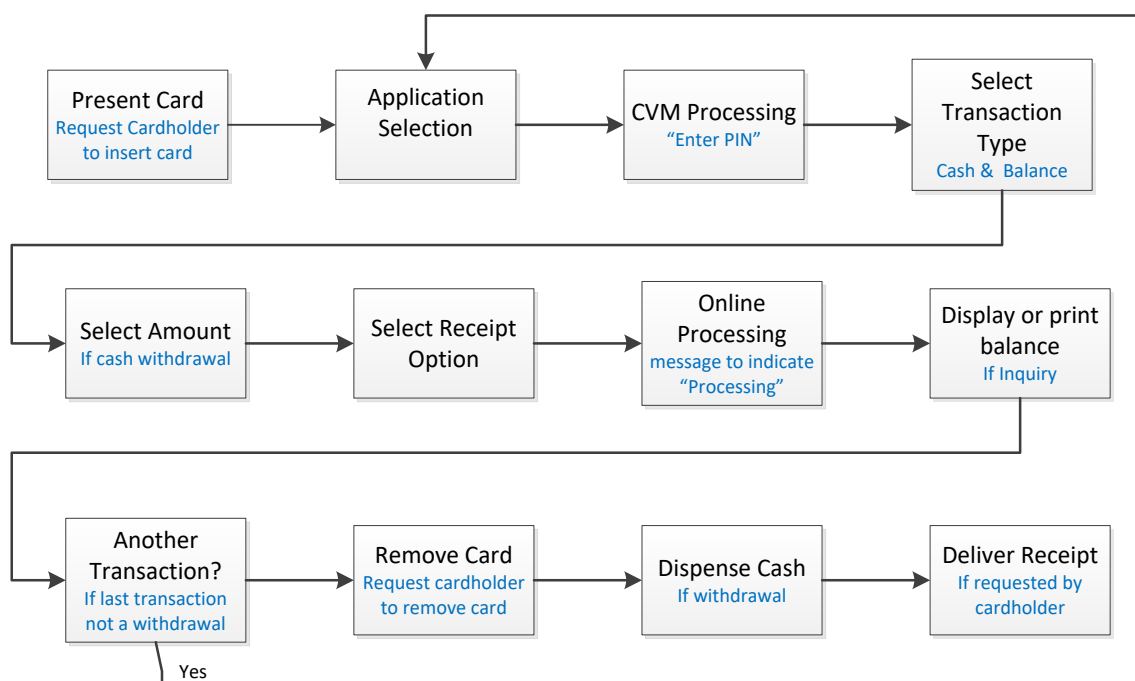


Figure 4 - Multi app Australian IC Card

G.9 Contactless Requirements

G.9.1 Card features

(a) PPSE usage

All Australian IC Cards providing a contactless interface must contain a PPSE.

(b) Application Priority Indicator

Issuers must use the Application Priority Indicator (TAG 87) in the PPSE to show the preferred priority of all contactless applications on the Card, different priorities must be set for each application.

(c) Application Preferred Name

Issuers are encouraged to personalise the Application Preferred Name (Tag 9F12) and Issuer Code Table (tag 9F11) with suitable meaningful names.

(d) Off-line PIN verify

Issuers are strongly encouraged not to socialise the off-line PIN verify command via the contactless interface.

(e) Cardholder Name

Contactless Cards must not include the Cardholder name in the data read through the contactless interface.

(f) **Service Codes**

It is recommended that Issuers personalise IC Cards with the same service code in all places in which it appears e.g.,

On the magnetic-stripe track 1 and 2

Track 1 data (Tag 56) when accessed via the contactless interface

Track 2 data (Tag 9F6B) when accessed via the contactless interface

Track 2 equivalent data (Tag 57) when accessed via the contactless interface

Track 2 equivalent data (Tag 57) when accessed via the contact interface

Nothing in this clause is intended to limit the Issuer in prescribing service codes appropriate to the application and its intended usage e.g., service code indicating domestic usage only).

(g) **Cryptogram validation**

As the Transaction amount (DE4) may not be available to the Card for cryptogram generation, cryptogram verification shall use TAG 9F02 amount authorised, from DE55 which shall be populated by the Acquirer (ATM) to reflect the actual value provided to the Card for cryptogram generation.

(h) **Contactless mode**

Australian IC Cards providing a contactless interface shall support Contactless-EMV mode.

(i) **Second presentment**

Cards should be personalised to not require second presentment.

G.9.2 Issuer features

Neither Issuer Identification Data nor Issuer scripts are to be returned in the response message to an ATM Transaction initiated through the contactless interface.

As ATMs may not validate the card settings, Issuers should be aware that they may receive ATM Transactions even if:

- (i) Support for ATMs is not included in the Application Usage Control
- (ii) Support for on-line PIN is not included in the CVM list

(a) **Card Management**

The Issuer should manage the offline counters and parameters for the contactless interface during the authorisation response to a contact chip transaction. They cannot be managed during a contactless Transaction as the Issuer Authentication Data from the authorization response is never delivered to the Card.

G.9.3 Terminal Features

ATM Terminals should perform application selection using the PPSE on the Card.

Partial AID matching is recommended for all ATM Terminals.

ATM Terminals are not required to perform off-line card authentication.

ATM Terminals are not required to support second presentment.

(a) **Application Selection**

The highest priority available payment application must be selected automatically by the ATM terminal, when a contactless Card is presented. ATM Terminals, for such Transactions must support application selection without Cardholder assistance. If priorities have not been set in the Card, then the application selected will be determined by the terminal.

Terminals must maintain an independent list of AIDs accepted by the terminal for contactless payments.

(b) **Off-line PIN verification**

As on-line Cardholder verification is required for all ATM Transactions, The ATM's contactless interface should not support off-line PIN verification (see G7.4).

(Note: this means that support for Device Cardholder Verification (Mastercard), Mobile Pin or mPIN shall not be provided.)

(c) **Cryptogram generation**

The amount authorised, provided to the Card for cryptogram generation shall be reflected in TAG 9F02, amount authorised and passed to the Issuer in DE55.

(d) **Data Usage**

Contactless Acquirers must only use data read from the contactless interface for contactless Transactions. Data obtained from the contactless interface must not be used for any another purpose or Transaction type.

(e) **Receipts**

The application preferred name (Tag 9F12) may be printed on the receipt in lieu of the AID if the code table is supported.

G.9.4 Messaging

(a) **POS Entry Mode (DE22)**

Transactions initiated via the contactless interface shall set positions 1 and 2 of the Point of service entry mode (DE22) to 07, Contactless ICC (see AS2805-2 clause 4.4.10)

(b) **Response Codes (DE39)**

Response codes 01 – Refer to Card Issuer and 04 – Pick up Crd should not be used for contactless Transactions.

(c) **Processing Code**

As a contactless Transaction may occur before any service has been selected, i.e., to wake up the ATM, the value of the Transaction Type (Tag 9C in DE.55) may differ from the processing code sent in DE3.

ATMs must be able to generate Transactions where the value of Transaction Type (Tag 9C) is different from the value of the Processing Code in DE.3.

If a contactless Transaction (tap) is used to wake up the ATM before any ATM service has been selected, the ATM must use a value of 93 for the Transaction Type (tag 9C) sent in the Generate AC command.

G.9.5 Transaction Processing

This clause contains an overview of the preferred processing flows for contactless Transactions. These are examples only and alternative flows are permitted. The requirements include ATM wake-up and chained contactless Transactions.

(a) **ATM Wake-up**

The preferred Transaction flow, where ATM processing commences by the Cardholder selecting a particular ATM option, and then entering the requested amount is shown in Figure 5 below. In this case the ATM subsequently requests the Cardholder to tap, then using the highest priority application on the Card, the ATM initiates a full EMV withdrawal Transaction by requesting an ARQC with the Transaction amount (tag 9F02) equal to the requested cash amount and the Transaction type (tag 9C) equal to cash withdrawal (01).

On successful completion of the contactless exchange the ATM completes its existing processes for Card validation and online PIN entry and sending a financial transaction request message (0200). No further interaction with the Card is required. The ATM returns to the idle state once the process is complete.

The preferred Transaction flow where the ATM is opened by presenting the contactless Card (tapping) is shown in Figure 6 below. The ATM moves from the idle state when the Card or device enters the reader's field. The ATM should select the highest priority application and initiate a default amount value Transaction by requesting an ARQC with the Transaction amount (tag 9F02) set to the ATMs configured default amount else zero and the Transaction type (tag 9C) set to 93 to indicate a contactless Transaction.

ANNEXURE G. EMV@ATM TERMINAL STANDARDS

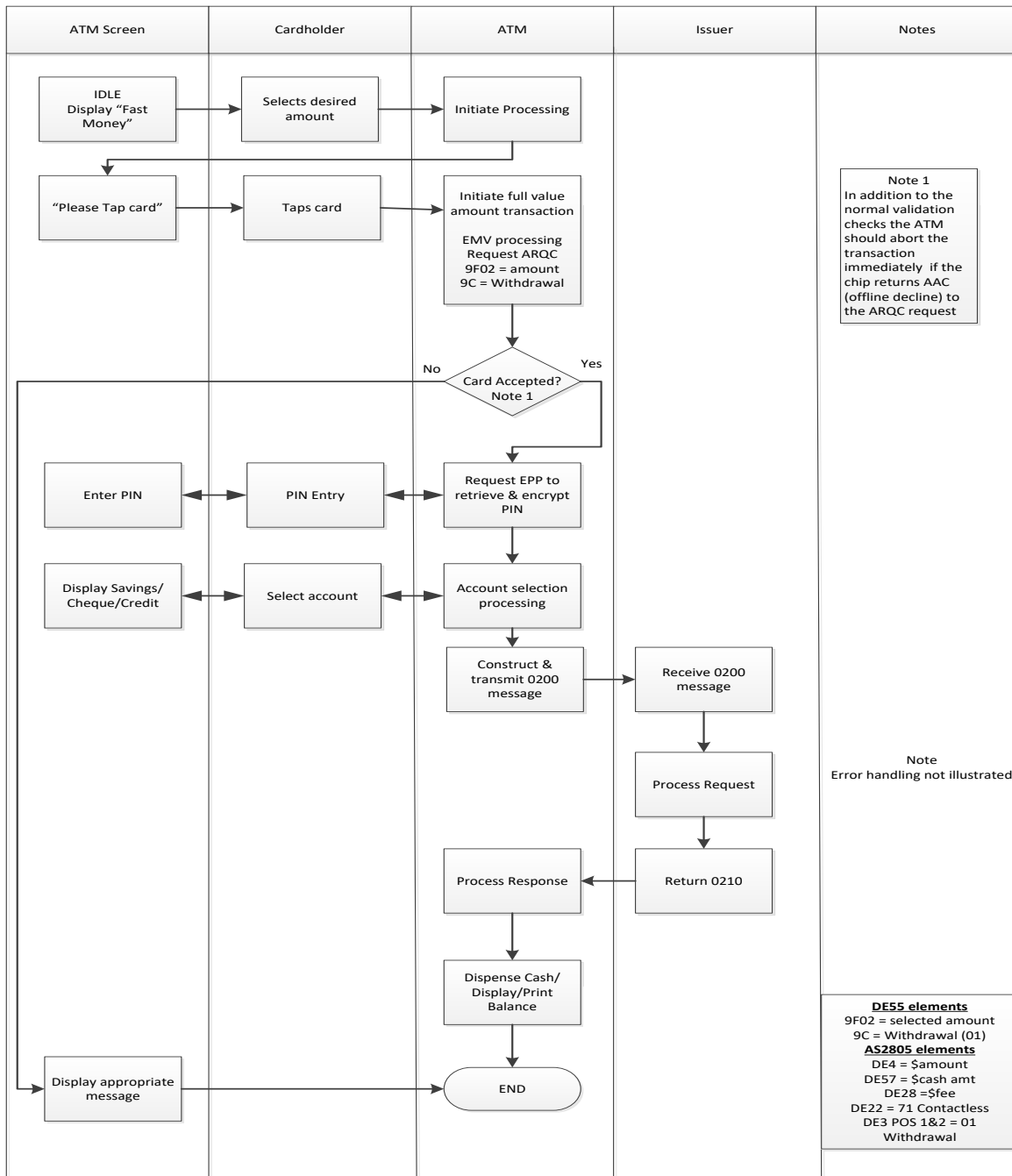


Figure 5 Press to wake up

ANNEXURE G. EMV@ATM TERMINAL STANDARDS

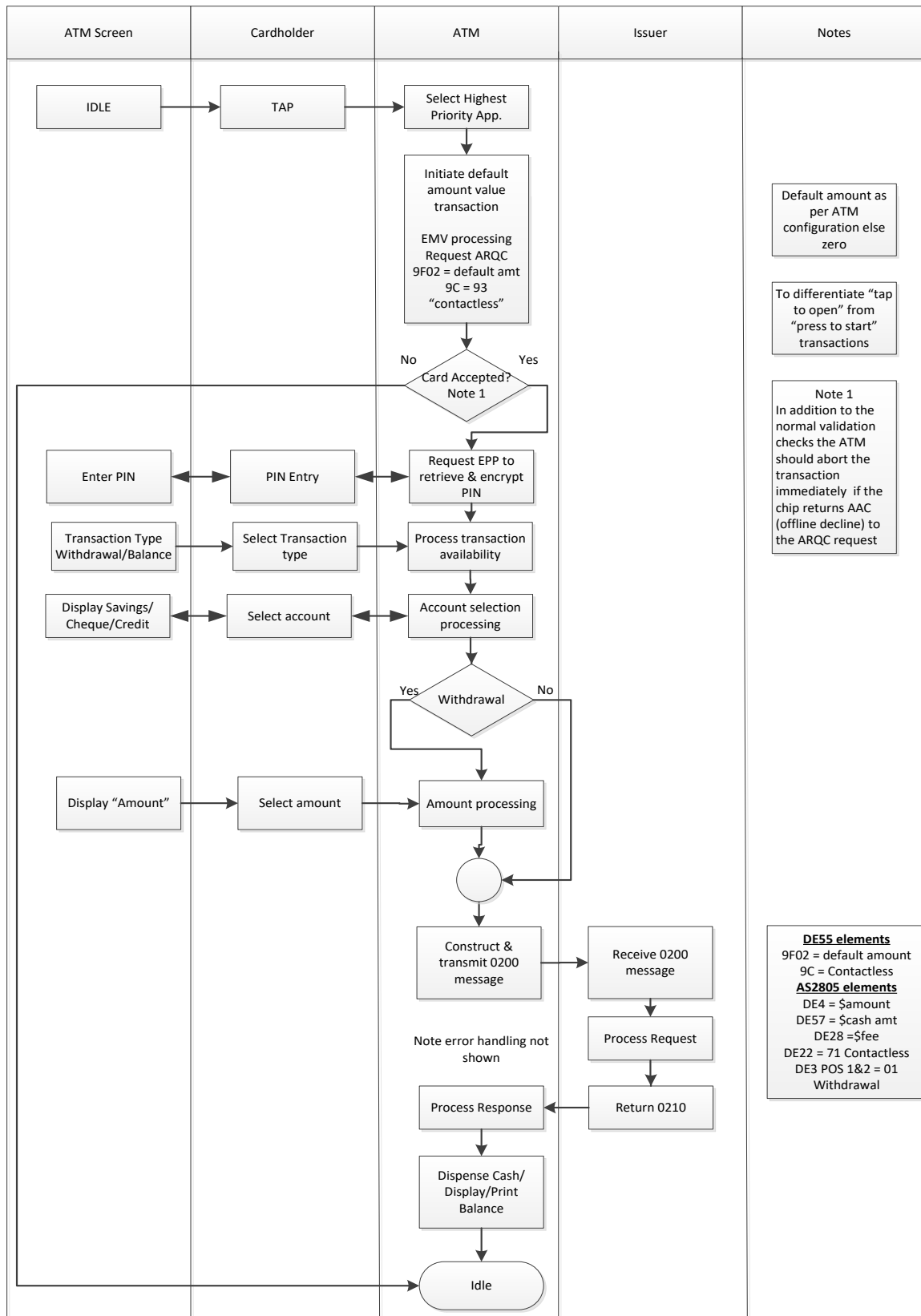


Figure 6 Tap to Start

(b) Chained Transaction support

Chained Transaction support for contactless Transactions, as illustrated in Figure 7 and Figure 8 requires that the Cardholder's identity is reconfirmed before initiating any subsequent Transactions. This may be accomplished by requiring that the Cardholder re-tap the Card or preferably, by re-entering their PIN. The purpose of this second confirmation is to prevent opportunistic fraud which happens when a second user is standing behind a Cardholder who is using contactless requests another service such as withdrawal, when the first Cardholder has left the ATM but the ATM has not returned to an idle state.

In the preferred flow opportunistic fraud is further avoided by not permitting chained Transactions subsequent to a withdrawal.

(c) PIN re-entry

If PIN re-entry is required, either through an incorrect PIN or for Cardholder re-confirmation the Cardholder should not be requested to re-tap the card. The original Transaction information should be re-used for subsequent PIN validation attempts.

(d) Cryptographic Data

If chained Transactions are to be supported for contactless Transactions, the ATM must be able to reuse the same contactless Card generated cryptographic data for multiple consecutive Transaction requests.

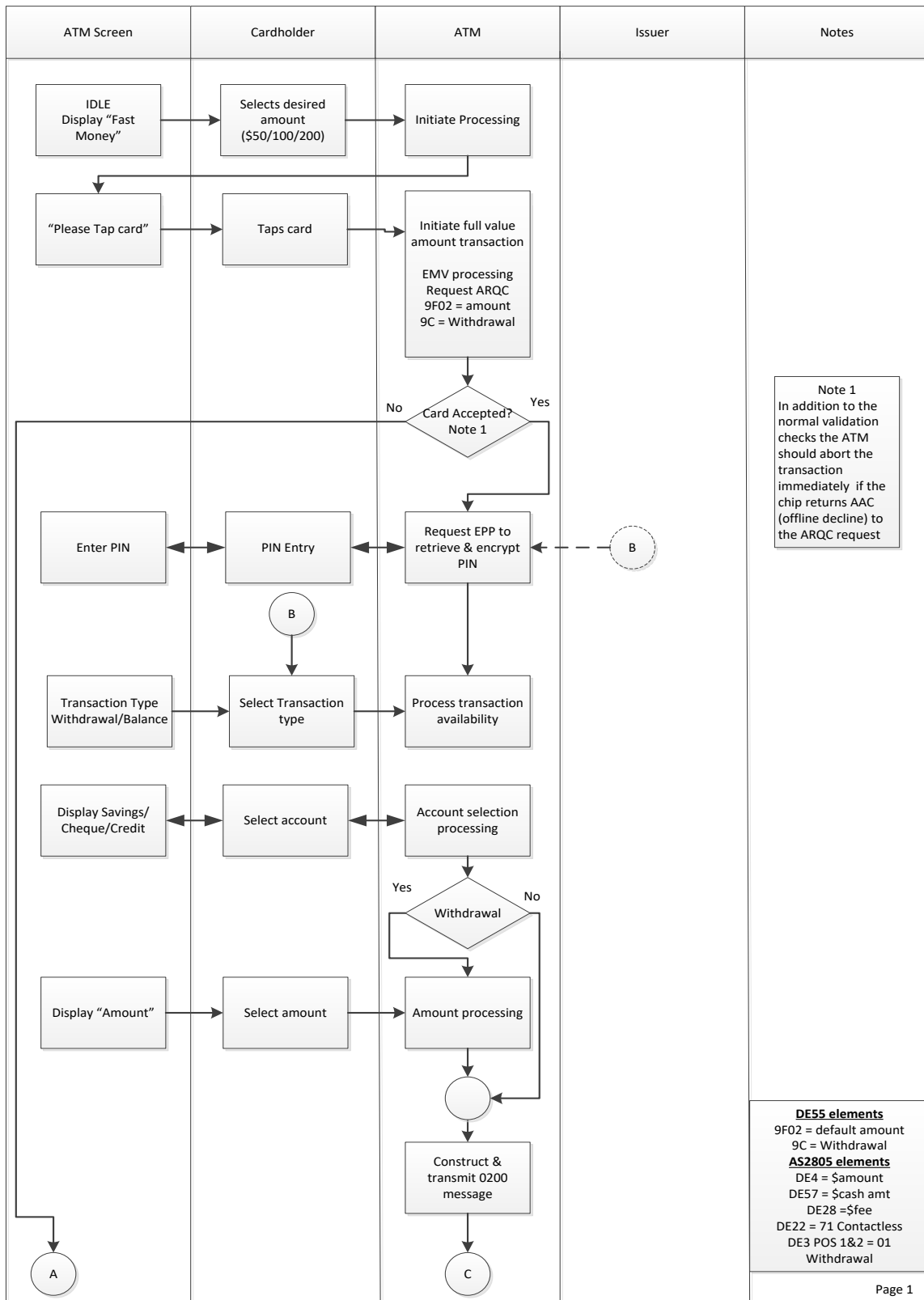


Figure 7 Chained Transaction Support – part 1

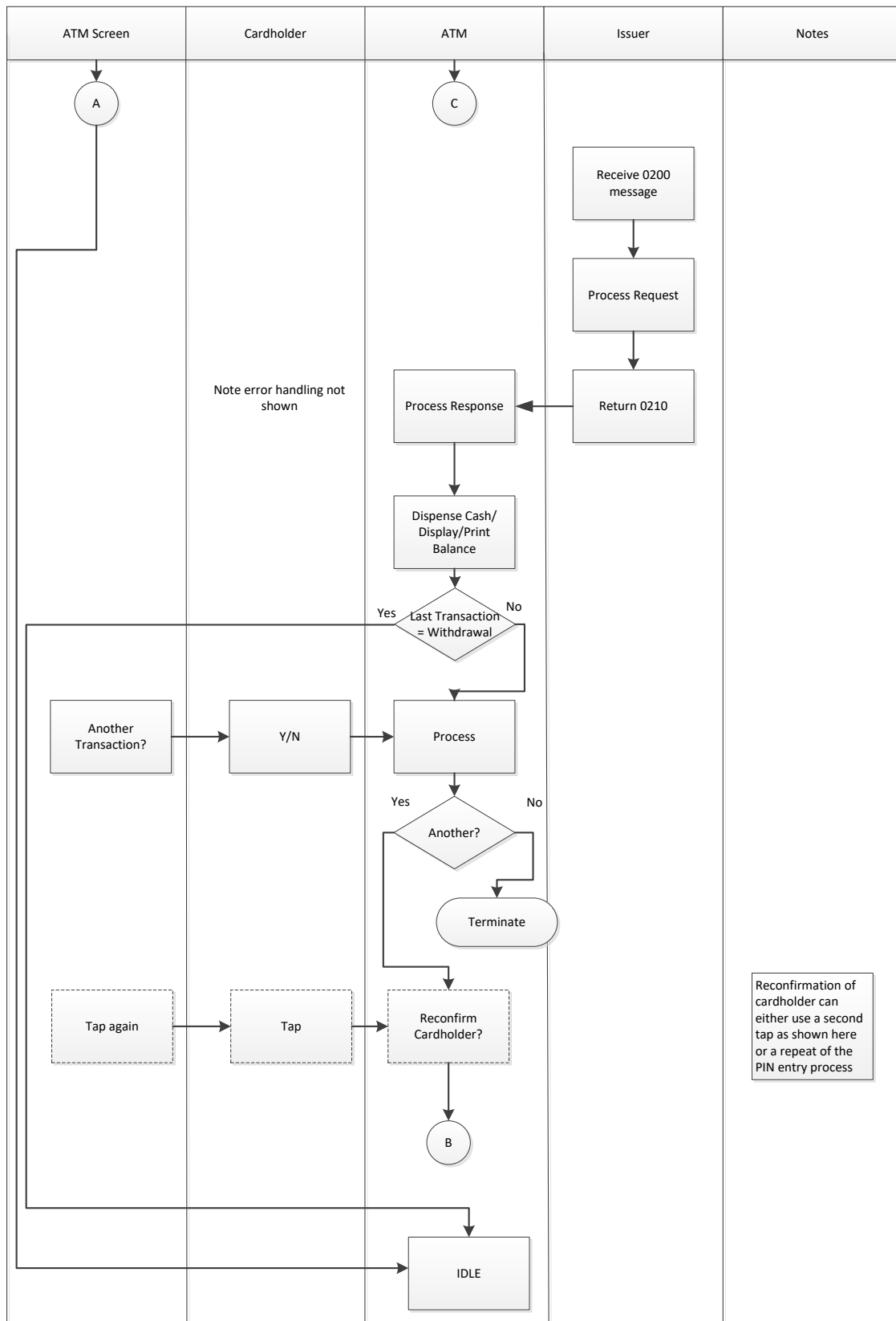


Figure 8 Chained Transaction Support – part 2
Next page is H.1

ANNEXURE H. ESCALATION PROCEDURE

H.1 Objective

This Annexure H aims to define the escalation procedure to be used in managing and resolving any production problems affecting the ATM and/or the ATM Interchange Link between any two IA Participants. This will ensure that all problems will be managed in accordance with an agreed production problem process between the two parties to an Interchange.

H.2 Escalation Process

- (a) The proposed ATM Interchange escalation procedures are as defined in the attached escalation table. The table displays the maximum elapsed resolution time (after report of the problem) for each of the three severity levels and three levels of escalation. It is recommended that this process be applied 7 days a week 24 hours a day.
- (b) Escalation service levels will be based on severity levels determined and confirmed by the [Title of Responsible Officer] for XXXX, and the [Title of Responsible Officer] for Xxxx, at the time of notification of the problem.

H.3 Severity levels are as follows:

- (a) 1 – (Critical):

The product/service is unusable or unavailable.

- (i) System/online/network component down
- (ii) Product/service unavailable
- (iii) No bypass available
- (iv) Any customer service impact – full, impending or limited

- (b) 2 – (Medium)

The product service is useable, but operations are restricted and a level of exposure exists.

- (i) Limited/no access by network devices
- (ii) Product/service degraded or restricted (i.e., 1 of 2 communications links down)

(c) 3 – (Low)

The product service is useable, but operations are restricted and a level of exposure exists.

- (i) Day to day issue
- (ii) Problem Identified
- (iii) No customer impact
- (iv) Resolution available

(d) Although this process applies 24 hours a day / 7 days a week, only Severity 1 and Severity 2 problems would be notified to the interchange partner and vice versa after business hours. Any Severity 3 problems which occur after hours can be notified on the next working day and will be tracked as normal problem record.

(e) The response by the first level of escalation to problems notified will be an indication of the steps (or at least the next step) which will be followed in order to develop a solution, and if possible, an indication of the timeframe involved. This response will be given to XXXX and Xxxx as the case maybe:

- (i) Severity Level 1: raise PMS (problem) record; response within 30 minutes of notification of the problem.
- (ii) Severity Level 2: raise PMS (problem) record; response within 60 minutes of notification of the problem
- (iii) Severity Level 3: raise PMS (problem) record; response by 5.30 pm on the next working day.

H.4 Escalation of Call

- (a) If the problem CANNOT be resolved within 30 mins (for Severity 1) or 60 mins (for Severity 2) after first being reported, then it must be escalated to the Second Escalation Level. In all cases [Title of Responsible Officer] from XXXX and [Title of Responsible Officer] for Xxxx will take the role of Problem Situation Manager.
- (b) Support staff from each Interchange party must continue to resolve the problem while the problem is being escalated.

- (c) Every problem will be treated on its own merit(s). The contact points in each escalation level will manage information flow from both parties and ensure that sufficient information is passed on to the business areas concerned. If the resolution is taking longer than anticipated, the severity of the problem may be changed with the concurrence of both parties. On exceptional situations regardless of the severity of the problem [Title of Responsible Officer] (XXXX) and [Title of Responsible Officer] (Xxxx) after consultation with the Second Escalation Level must make an informed decision as to whether to escalate the problem to the Third Escalation Level.
- (d) Situation management may be invoked by both parties based on the severity of the problem. Depending on where the problem resides A situation manager must be appointed by the [Title of Responsible Officer] for XXXX or [Title of Responsible Officer] Xxxx to manage Severity 1 (in some cases Severity 2) problems. The situation manager may appoint a number of Support and/or Area Managers to co-ordinate activities across departments during a SEV 1 situation. Responsibilities include;
- (i) Manages problem definition and resolution through Support managers.
 - (ii) Chairs checkpoint meetings (follows to agenda and tracks actions).
 - (iii) Puts recommendations/actions to [Title of Responsible Officer] and Business owner.
 - (iv) Communications to all involved parties in technology and IT team as appropriate.
 - (v) Allocation of technical resources required.
 - (vi) Adherence to situation management process.
 - (vii) Liaison between support managers and [Title of Responsible Officer]/Business.
 - (viii) Reporting progress to the [Title of Responsible Officer]

H.5 ATM Interchange Escalation Table

(XXXX-Xxxx)

| LEVEL | ESCALATION LEVEL | SEVERITY 1+ | SEVERITY 2+ | SEVERITY 3+ | CONTACT DETAILS | | | |
|--------|--|-------------------|-------------------|----------------------------|---|---|--------------------------------------|--------------------------------------|
| | | RESOLUTION TIME * | RESOLUTION TIME * | RESOLUTION TIME * | XXXX | Xxxx | SITUATION MANAGEMENT | |
| | | | | | | | XXXX | Xxxx |
| FIRST | XXXX OPERATOR TO Xxxx OPERATOR [Title of Responsible Officer] to [Title of Responsible Officer] | 30 MINS | 60 MINS | RESPONSE BY 5:30 PM | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers | [Title of Responsible Officer] | [Title of Responsible Officer] |
| SECOND | XXXX OPERATOR TO Xxxx OPERATOR [Title of Responsible Officer] to [Title of Responsible Officer] | 60 MINS | 4 HOURS | NEXT WORKING DAY. | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers, pager number, home and mobile | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers, pager number, home and mobile | [Title of Responsible Officer] | [Title of Responsible Officer] |
| THIRD | XXXX OPERATOR TO Xxxx OPERATOR [Title of Responsible Officer] to [Title of Responsible Officer] | 4 HOURS | 1 DAY | | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers, pager number, home and mobile | Contact Details: Including Area Name, Title of Responsible Officer & 24 hour phone numbers, pager number, home and mobile | [Title of Responsible Officer] | [Title of Responsible Officer] |

NOTE:

Indicative MAXIMUM ELAPSED TIME (AFTER REPORT OF PROBLEM) FOR RESOLUTION BEFORE NEXT ESCALATION FOR ACTION.

Next page is I.1

ANNEXURE I. ATM INSTALLATION CHECKLISTS

[Informative]

Annexure I is confidential

Next page is J.1

**ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL
ARRANGEMENTS FOR COMBO CARDS****[Informative]****J.1 Purpose**

These guidelines are designed to assist acquirers and ATM vendors in the development of suitable solutions to the "combo card problem" that will arise during the transition period between EMV upgrades to cards, ATMs and the bilateral interchanges. These guidelines are designed to produce a reliable cardholder experience whilst acknowledging that there is likely to be no suitable single technical solution applicable to all acquirers and/or ATM vendors.

It is envisaged that these guidelines will be updated overtime as new potential solutions are developed and become available

J.2 Problem statement

- (a) There are two seemingly unique features of the Australian ATM environment;
 - (i) Cash advances (from credit cards) are often, but not always, switched bilaterally rather than through the card scheme networks.
 - (ii) The existence of chipped combo cards that is cards carrying a valid EMV application (typically for credit/scheme debit) must also provide access to a bilaterally switched debit account across a non-EMV capable interchange link.
- (b) As a general rule, ATMs do not selectively process cards, other than perhaps for "on us" transactions. Further it is assumed that EMV upgrades to the bilateral interchange links will lag EMV updates to ATMs requiring a "phase 1" like solution to allow debit account transactions and cash advances from a (credit) card to be processed as magnetic-stripe (like) from a "chipped" card as the appropriate interchange link will be incapable of accommodating EMV data.
- (c) This requirement is complicated by the following factors;
 - (i) There is no consistent model of how credit card originated cash advances are switched (whether via scheme or bilaterally).
 - (ii) There is likely to be a strong desire to maintain existing arrangements for handling cash advances.
 - (iii) It will be transitional arrangement as the bilateral interchange links are gradually upgraded to accommodate EMV data necessitating frequent updates

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

- (iv) ATM software is expensive to modify and vendors are likely to be reluctant to develop proprietary versions.
- (v) Other than for "on us" cards, ATMs generally apply a single, consistent, processing model to all cards (no BIN tables).
- (vi) Between issuers there may be no consistency in how Combo cards are personalised such as the requirement for issuer authentication.

J.3 Requirements

Any solution must;

- (a) Must support full EMV processing for chip cards;
- (b) Must be capable of selectively generating a magnetic-stripe like transaction, from either magnetic-stripe or chip derived track 2 equivalent data, on a BIN by BIN basis;
- (c) Must support withdrawals from debit and combo cards and selectively cash advances from credit cards on the bilateral links on an issuer-by-issuer basis;
- (d) Must be transparent to the cardholder;
- (e) Must operate independently of the card's customisation especially for issuer authentication;
- (f) Must be capable of migration to full EMV as interchanges and cards are selectively migrated;
- (g) Must be capable of advising the issuer of source of the card data (chip or magnetic stripe card); and
- (h) Must be Scheme card and application agnostic.

J.4 Possible solutions

Previous workshops have identified and examined various solutions; they generally fall into one of two broad categories:

- (a) Standard ATM software
- (b) Modified ATM software

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

J.5 Solutions using standard ATM software**J.5.1 Option 1 – ATM selective processing driven by BIN number**

- (a) In this solution the ATM performs EMV processing selectively based on card prefix (BIN/IIN). Typically the ATM would read the magnetic-stripe, then based on the BIN and FIT either move the card into the chip card reader and proceed with EMV processing or alternatively simply continue to process as magnetic-stripe.
- (b) It is assumed that;
 - (i) The ATM contains a Financial Institution Table (FIT), and table driven software that can be selectively controlled by that table.
 - (ii) The ATM is able to read either (or both) the magnetic-stripe or the chip and is capable of overriding the card's service code.
- (c) The benefits of this proposed solution include;
 - (i) Given the assumptions noted, only standard ATM and switch software would be required.
 - (ii) Will not interfere with the card's EMV processing (e.g., Transaction Counter will remain in sync with host – no fraud detection system problems)
- (d) Measures working against this proposed solution include;
 - (i) Development and maintenance of FIT tables, and associated ATM tables will be required and ongoing (as Issuers transition to full EMV) – expensive for acquirers.
 - (ii) Size of FIT tables may be a limitation (e.g., NCR FIT table is limited to 999 entries and AusPayNet BIN table currently has 627 entries)
 - (iii) Six digit BINs (IINs) may not be sufficient to accommodate issuer requirements, and ATMs may have limitations on how much of the PAN may be used to selectively process in the FIT tables. (Mastercard allows up to 11 digits for BIN splits).
 - (iv) May not be universally adoptable (low-cost ATMs may not contain suitable functionality as standard).
 - (v) For ATMs without download capability, costs associated with the transition phase may be deemed excessive (requiring multiple site visits to the ATM to update the tables).
 - (A) Not all ATMs may have combined (automatic) magnetic-stripe and IC readers requiring additional cardholder interactions.

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

J.5.2 Option 2 – Switch conversion to (pseudo) magnetic-stripe.

- (a) In this proposed solution the ATM will perform standard EMV processing up to the point of generating the online request message. On receipt of the request the switch will determine how to proceed based on some form of table. If magnetic-stripe the EMV data will be dropped and a magnetic-stripe like transaction constructed and forwarded to the issuer.
- (b) Typically the ATM would be configured to perform partial EMV processing (up to the point of generating the online request message) if a chip card is present. The switch/host would then make the decision to fulfil/complete the transaction based on EMV or Magnetic-stripe capabilities of the issuer/interchange. If magnetic-stripe capability only is available, based on a table in the switch, then the switch will drop the EMV data; construct a magnetic-stripe transaction this may be based on either the real magnetic-stripe information or the track II equivalent data from the IC. Assuming a magnetic-stripe transaction, on receipt of the issuer's response message the switch will craft a "terminate EMV" instruction with the appropriate action codes to fulfil the issuer's instructions for delivery to the ATM.
- (c) It is assumed that the ATM has a command (e.g., NCR's CAM5) that can prematurely terminate EMV processing and command the ATM to dispense (nor not dispense) cash irrespective of either the card's or EMV processing rules.
- (d) The benefits of this proposed solution include;

Only standard ATM software required.
- (e) Measures working against this proposed solution include;
 - (i) Modifications to the switch software will be required to:
 - (A) Build logic to determine whether the transaction is to be forwarded to issuer as EMV or not.
 - (B) If not to be processed as a full EMV transaction forward as Non- EMV (Magnetic-stripe) to issuer and reply to ATM with CAM5 to indicate to complete as Magnetic-stripe transaction.
 - (ii) Will likely require interchange modifications to Bit 22 – Point of Sale Entry Mode to advise issuer of source of card data (iCCV/CCV)
 - (iii) Issuer host changes to support alternate CCV/iCCV processing
 - (iv) May cause difficulties with the card's internal logic e.g., Application Transaction Counter getting out of step with the Issuer's host and consequential problems with the fraud detection logic.

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

- (v) Negates any advantage (fraud) that EMV processing provides (e.g., potentially no card authentication etc.)
- (vi) Provides an opportunity for the acquirer to over-ride issuer instructions, may require consideration of liability provisions.

J.5.3 Option 3 - Downgraded authorisation

- (a) The EMV specification provides a mechanism that can be used in the absence of issuer authentication data (IAD), as would occur if a non-EMV capable interchange link was used. Specifically in clause 12.2.2 of [1] the recommended action to take in the absence of issuer authentication data is called a downgraded authorisation and is simply to continue with processing the transaction. The full process is described below.
 - (i) "When the authorisation response received by the terminal does not contain the Issuer Authentication Data, the terminal must not execute the EXTERNAL AUTHENTICATE command and must set the "Issuer authentication was performed" bit in the Transaction Status Information (TSI) to 0, as described in Book 3. The terminal must continue processing based on the Authorisation Response Code returned in the response message as described in section 6.3.6 of [1].
 - (ii) Note: If the acquirer or the intermediate network is unable to support ICC messages, the terminal should send messages compliant with current payment system specifications. Payment systems will determine compliance requirements for message content."
- (b) The benefits of this proposed solution include;

Only standard ATM software required.
- (c) Measures working against this proposed solution include;

A card's response to the absence of IAD is subject to the card's application and individual personalisation and it may well refuse to authorise the transaction thereby impacting the cardholder.

J.6 Solutions involving modified ATM software**J.6.1 Option 4 – Selective processing based on (ATM determined) Issuer Country Code**

- (a) This potential solution is similar to EFTPOS Phase 1, after application selection, card data is read and if the Issuer's Country Code is "036". EMV processing is aborted and a pseudo magnetic-stripe instruction is created.

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

- (b) The benefits of this proposed solution include;
 - Utilizes experience gained from EFTPOS EMV Phase 1
- (c) Measures working against this proposed solution include;
 - Will require customized ATM software.

J.6.2 Option 5 – Selective processing based on card data and switch tables

- (a) In this proposed solution the ATM is configured to obtain some EMV (or magnetic-stripe) data such as PAN/BIN and to then send this data to the switch prior to normal transaction processing. The switch can then determine (based on internal tables) how the transaction should be fulfilled and respond to the ATM with appropriate instructions.
- (b) The benefits of this proposed solution include;
 - May reduce the number of ATM site visits required during transition
- (c) Measures working against this proposed solution include;
 - (i) Customized ATM and messaging software (costly to implement)
 - (ii) Negates any advantage (fraud) that EMV processing provides (e.g., potentially no card authentication etc.)
 - (iii) Increased transaction time due to multiple interactions between ATM and switch.
 - (iv) Acquirer switch modifications required to:
 - (A) Build logic to determine whether to process as EMV or Non-EMV at the switch/host.
 - (B) Define the ATM transaction flow to implement multiple transaction requests using logic at the host to instruct the ATM to process as either Magnetic-stripe or EMV

J.7 Recommended framework solution

- (a) This framework does not provide implementation details and is agnostic to the implementation method as there is likely to be no single suitable solution applicable to all acquirer/ATM vendor combinations. That said the key features of the required solution are;
 - (i) Must, on a bilateral and BIN by BIN basis, be capable of forming a magnetic-stripe transaction from a chip based card for both withdrawals and cash advances (implies the use of tables);

ANNEXURE J. EMV AT AUSTRALIAN ATMS – TRANSITIONAL ARRANGEMENTS FOR COMBO CARDS

- (ii) Must not impact full EMV processing, including that for cash advances, for non-domestically issued cards;
 - (iii) Must provide the issuer with a means of identifying the source of the data, that is whether chip or magnetic-stripe (POS entry mode set to 051 for chip);
 - (iv) When chip data is used the Track Two Equivalent Data, formatted in accordance with AS 3524 and clause 5.10.2 (Data Element 35), must be used to construct a Financial Request Message, which must be forwarded to the Issuer in accordance with magnetic stripe processing formats and rules (as contained in this IAC Code Set); and
 - (v) Must work for all cardholders irrespective of the issuers requirement for IAD (most likely negates the use of downgraded authorisation).
- (b) From the above requirements it can be inferred that only options 1 and 2 (or various combinations of the two) are likely to be suitable. The location of the tables will be dependant on the ATMs capabilities (e.g., existence of FIT tables) and/or acquirers switch capabilities. Option 2 requires that the ATM be capable of terminating normal EMV processing prematurely and of taking appropriate action in response to issuer provided response code irrespective of the chip's determination.
- (c) Issuers must accept that adopting a "phase 1" solution for ATMs will not achieve the full fraud reduction capabilities of EMV and that by implementing these solutions we are providing an explicit opportunity for an acquirer to override the chip's (issuer's) decision making capability. Issuer's attention is also drawn to the possibility of the chip's application transaction counter becoming out of synchronization with expected values and consequentially problems with fraud detection software.

Amended
effective 1.1.16**J.8 Bibliography**

- [1] EMV V4.2 Book 4, Cardholder, attendant, and acquirer interface requirements

Next page is K.1

ANNEXURE K. SUBSCRIPTION FORM

(Operator Member/Affiliate – Part 2, clause 2.2(b))

The IAC Secretary
Australian Payments Network Limited
Level 23
Tower 3, International Towers Sydney
300 Barangaroo Avenue
SYDNEY NSW 2000

Dear Secretary

SUBSCRIPTION TO ATM SYSTEM CODE

We, [SUBSCRIBER], have been, or will in due course be, admitted as a Framework Participant within the meaning of the IAC Regulations.

We, [SUBSCRIBER], hereby subscribe to the ATM System Code and agree to use reasonable endeavours to engage activities to promote the objects of the ATM System Code and all of its obligations (as amended or modified from time to time).

We acknowledge that our subscription will become effective upon receipt by the Secretary.

EXECUTED by [SUBSCRIBER] in accordance with section 127 of the Corporations Act:

Signature of Director

Signature of Director/Secretary

Name of Director

Name of Director/Secretary

Note: Subscription notice may be executed by the Subscriber under Power of Attorney.

Next page is L.1

ANNEXURE L. COUNTERFEIT ATM TRANSACTION CLAIM NOTICE

Deleted
effective 3.7.17

[Deleted]

Next Page is M.1

ANNEXURE M. DISPUTED AND SETTLED FILE TECHNICAL SPECIFICATION

ANNEXURE M. DISPUTED AND SETTLED FILE TECHNICAL SPECIFICATION

Annexure M
in its entirety
replaced
effective
21.11.16

File Name Convention

Files should adhere to the below defined file naming convention:
ABCXYZDDMMYYF.xlsx

Where:

ABC = AusPayNet mnemonic of the sending institution

XYZ = AusPayNet mnemonic of the receiving institution

DDMMYY = date on which the file is sent

F = D or S, being the file type, D for disputes or S for settled. Note if a Disputed file has been rejected it will be a Disputed file and details for its rejection would be detailed within the excel file

.xlsx denotes an excel file type.

File Format Convention

| File Type | Field | Attributes | | Comments | Condition | Reference |
|--|------------------------------------|------------|----|---|-----------|--|
| Disputed and Settled Disputed Transaction File | Originating Bank | a | 3 | Must be an approved financial institution abbreviation (Refer to AusPayNet publication BSB numbers in Australia) | M | BECS Procedures – Appendix C1 DE File User Item Specifications |
| Disputed and Settled Disputed Transaction File | Originating Bank Reference | an | 18 | | M | |
| Disputed and Settled Disputed Transaction File | Card Number | n | 19 | | M | |
| Disputed and Settled Disputed Transaction File | Suspense BSB Claim to be paid into | an | 7 | Must be numeric with a hyphen eg 999-999 Identifier issued by AusPayNet (Refer to AusPayNet publication BSB Numbers in Australia) | M | BECS Procedures – Appendix C1 DE File User Item Specifications |
| Disputed and Settled Disputed Transaction File | Suspense Claim to be paid into | n | 9 | Alpha (26 letters of the alphabet), numeric, hyphens & blanks only are valid. Must not contain all blanks or all zeros. Leading zeros, which are part of an account numbers must be shown. (Some Financial Institutions have leading zeros in valid account numbers, ie 00-1234). Edit out hyphens where account number exceeds nine characters. Right justified. Blank filled. | M | BECS Procedures – Appendix C1 DE File User Item Specifications |
| Disputed and Settled Disputed Transaction File | Terminal Number | an | 8 | Card acceptor terminal | M | AS2805 – Part 2 |
| Disputed and Settled Disputed Transaction File | Terminal Name | an | 40 | Card acceptor name/location | M | AS2805 – Part 2 |
| Disputed and Settled Disputed Transaction File | Transaction Date | n | 6 | Date in the format 'MMDDYY'. | M | |

Australian Payments Network Limited [ABN 12 055 136 519]

ANNEXURE M. DISPUTED AND SETTLED FILE TECHNICAL SPECIFICATION

| File Type | Field | Attributes | | Comments | Condition | Reference |
|--|------------------|------------|----|--|-----------|---|
| Disputed and Settled Disputed Transaction File | Transaction Time | n | 6 | Time in the format 'HHMMSS' | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Disputed and Settled Disputed Transaction File | STAN | n | 6 | A number assigned by the Card acceptor that uniquely identifies a Transaction at a Terminal for at least one calendar day and remains unchanged for the life of the Transaction. | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Disputed and Settled Disputed Transaction File | Amount Requested | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc'. | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Disputed and Settled Disputed Transaction File | Amount Received | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc'. | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Disputed and Settled Disputed Transaction File | Difference | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc'. | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Disputed and Settled Disputed Transaction File | Dispute Type | a | 20 | Drop down | M | N/A |
| Disputed and Settled Disputed Transaction File | Rejection Reason | a | 23 | Drop down | M | N/A |
| Disputed and Settled Disputed Transaction File | Charge Back | a | 3 | Drop down | M | N/A |
| Disputed and Settled Disputed Transaction File | Charge Back Date | n | 6 | Date in the format 'MMDDYY' | O | |

ANNEXURE M. DISPUTED AND SETTLED FILE TECHNICAL SPECIFICATION

| File Type | Field | Attributes | | Comments | Condition | Reference |
|-----------------------------------|---------------------------|------------|----|--|-----------|---|
| Settled Disputed Transaction File | Amount Paid | n | 12 | Amount in format '\$\$\$\$\$\$\$\$cc'. | M | IAC Framework Volume 6, Annexure A – Standard Interchange Specification |
| Settled Disputed Transaction File | Date Payment Sent | n | 6 | Date in the format 'MMDDYY' | M | |
| Settled Disputed Transaction File | Responding Bank Reference | an | 18 | | O | |

Notes:**File Type**

Disputed and Settled Disputed Transaction File

These fields appear in both the Disputed Transaction and the Settled Transaction Files

Settled Disputed Transaction

These fields appear only in the Settled Disputed Transaction Files

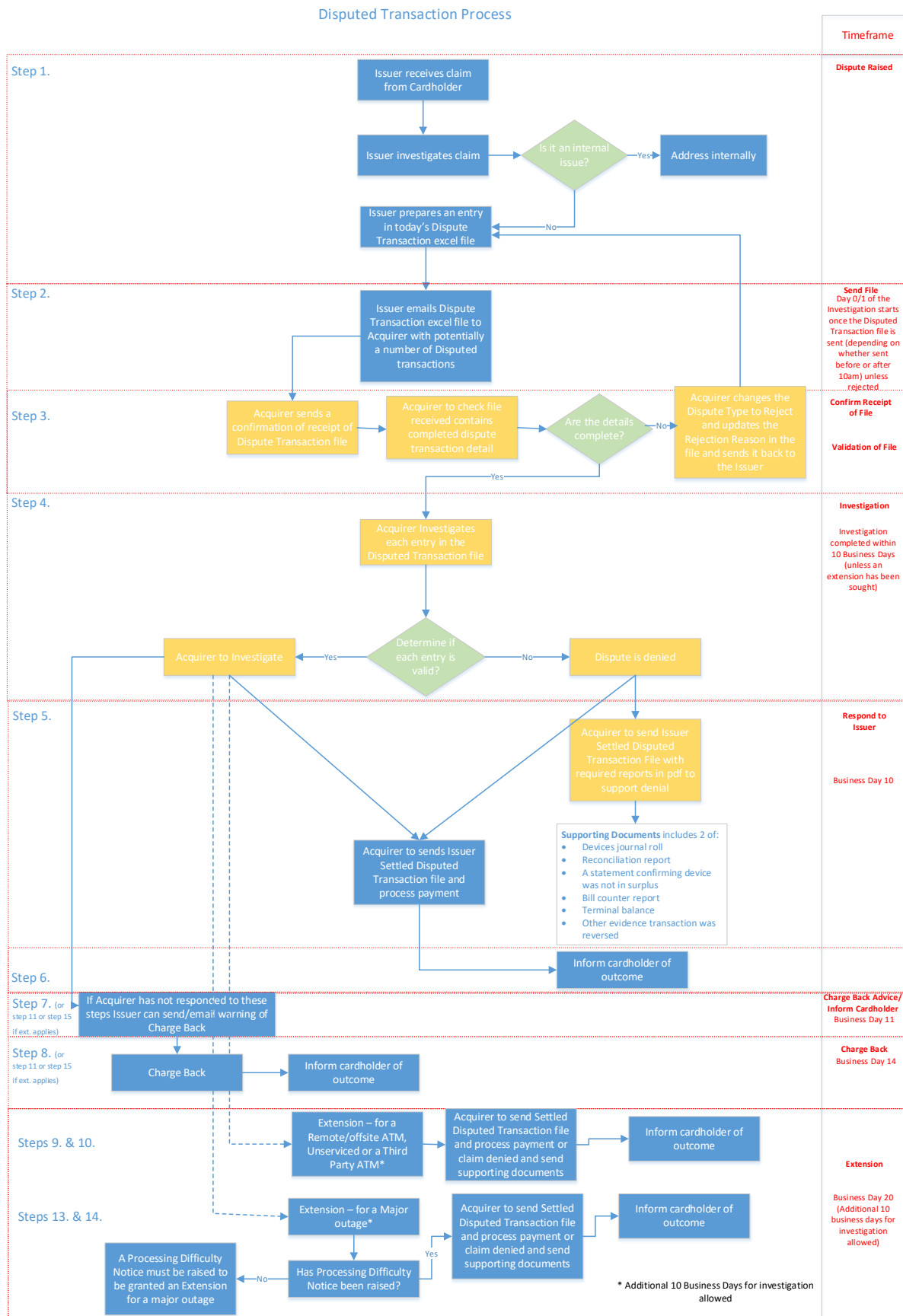
File formatting Standards:

- Left justified: start input in the first character position of that field.
- Right justified: end input in the last character position of that field.
- Blank filled: fills the unused portion of that field with blank spaces.

Next Page is N.1

ANNEXURE N. DISPUTED TRANSACTION PROCESS

Inserted effective 21.11.16



END