

Effective 19 December 2011  
Version E004

**AUSTRALIAN PAYMENTS CLEARING ASSOCIATION LIMITED**  
ABN 12 055 136 519

A Company limited by Guarantee

**COMMUNITY OF INTEREST NETWORK (COIN)  
OPERATING MANUAL**

for

**AUSTRALIAN PAPER CLEARING SYSTEM (CS1)  
BULK ELECTRONIC CLEARING SYSTEM (CS2)  
and  
CONSUMER ELECTRONIC CLEARING SYSTEM (CS3)**

Copyright © 2010 - 2011 Australian Payments Clearing Association Limited  
ABN 12 055 136 519

Australian Payments Clearing Association Limited  
Level 6, 14 Martin Place, SYDNEY NSW 2000  
Telephone: (02) 9221 8944 Facsimile: (02) 9221 8057

**COMMUNITY OF INTEREST NETWORK (COIN)**  
**OPERATING MANUAL**  
for  
**AUSTRALIAN PAPER CLEARING SYSTEM (CS1)**  
**BULK ELECTRONIC CLEARING SYSTEM (CS2)**  
**CONSUMER ELECTRONIC CLEARING SYSTEM (CS3)**

<b>PREFACE</b> .....	<b>1.1</b>
<b>1 OVERVIEW, DEFINITIONS AND INTERPRETATION</b> .....	<b>1.1</b>
1.1 Purpose of this Manual .....	1.1
1.2 Interpretation .....	1.1
1.3 Definitions .....	1.2
1.4 Introduction to the COIN .....	1.3
1.5 Permitted Traffic Types.....	1.3
1.6 COIN Termination Points.....	1.4
<b>2 GENERAL STANDARDS</b> .....	<b>2.1</b>
2.1 Security .....	2.1
2.2 Unauthorised Access Prevention.....	2.2
2.3 Incident Management .....	2.2
2.4 Member Change Window .....	2.3
2.5 Member Change Freeze .....	2.3
2.6 Network.....	2.3
2.7 Management Requirements of Authentication Parameters.....	2.4
2.8 Email Exchange of Authentication Parameters .....	2.5
2.9 Host System Requirements .....	2.5
2.10 Contingency .....	2.6
<b>3 COIN MEMBER OPERATING RULES</b> .....	<b>3.1</b>
3.1 Redundant connections .....	3.1
3.2 Connectivity Options .....	3.1
3.3 Availability and Support .....	3.1
3.4 Minimum bandwidth .....	3.1
3.5 QoS.....	3.1
3.6 Separation of test environments .....	3.2
3.7 IP Addressing.....	3.2
3.8 Security Event Management.....	3.3
3.9 Suspension of Connectivity.....	3.3
3.10 Certification .....	3.4
3.11 Default File Transfer Protocol .....	3.4
<b>ANNEX A SECURITY EVENTS, LOGGING, ESCALATION AND CONTINGENCY</b> .....	<b>A.1</b>
A.1 Introduction .....	A.1
A.2 Responding to Security Incidents .....	A.1
A.3 Standards for Security Events and Incidents.....	A.1
A.4 Defence against Security Events and Incidents .....	A.2
A.5 Emergency Response and Fraud Detection Plan .....	A.2
A.6 Recording of Security Events.....	A.2
A.7 Resolving Security Incidents.....	A.3
A.8 Logging Requirements.....	A.3

---

<b>ANNEX B</b>	<b>COIN MEMBER CERTIFICATION CHECKLIST .....</b>	<b>B.1</b>
<b>ANNEX C</b>	<b>MEMBER CONTACT LIST.....</b>	<b>C.1</b>

The next page is 1.1

## **PREFACE**

This initial release of the APCA Community of Interest Network (COIN) operating manual is designed to provide a common set of operating standards that can be universally applied to the operation of the shared network so as to ensure safe, secure and reliable operation of this shared facility.

## **1 OVERVIEW, DEFINITIONS AND INTERPRETATION**

### **1.1 Purpose of this Manual**

This Manual sets out general standards (Part 2) and operating rules (Part 3) that need to be met by all COIN Members and prospective members.

Compliance with these standards and rules (as reviewed from time to time) on a uniform basis through APCA will contribute to the continued integrity of all CECS interchanges and the clearing and settlement of file-based exchanges in Australia. In particular these COIN standards and rules seek to ensure that:

- Current quality levels are not compromised by:
  - Inferior operations;
  - Low quality network services and associated equipment; or
  - Inadequate security;
- Customer service is maintained at the highest possible level; and
- The general public continues to have confidence in the ability of their financial institutions to protect the privacy and security of their funds.

### **1.2 Interpretation**

In this Manual

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

- (f) words defined in the Corporations Law have, unless the contrary intention appears, the same meaning in this Manual;
- (g) words defined in the COIN Regulations have, unless the contrary intention appears, the same meaning in this Manual;
- (h) this Manual has been determined by the COIN Management Committee and takes effect on the date specified by the Chief Executive Officer pursuant to Regulation 1.6; and
- (i) headings are inserted for convenience and do not affect the interpretation of this Manual.

### 1.3 Definitions

Words used in this Manual that are defined in the COIN Regulations have the meaning given to them in that document.

“**AES**” means the Advanced Encryption Algorithm as specified in ISO 18033-3.

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

“**Authentication Parameter**” means a network value used to authenticate each end of a communications link.

“**Contingency**” means any Disabling Event and any other event or circumstance specified by any of the Management Committees of an Approved Clearing System.

“**DEA2**” means an encryption algorithm as specified in AS 2805 part 5.2. DEA2 is also known as RSA.

“**DEA3**” means an encryption algorithm as specified in AS 2805 part 5.4. DEA3 is also known as triple DES or 3DES.

“**Disabling Event**” means any;

- (a) processing, communications or other failure of a technical nature;
- (b) inaccessibility (total or partial) of facilities by means of which exchanges are conducted; or
- (c) manifestation of industrial action,

which affects, or may affect, the ability of any COIN Member to participate to the normal and usual extent in interchange and/or clearing and settlement.

“**Electronic presentment and dishonour files**” means all of the files required by appendices E and F of the APCS Procedures for the purposes of electronic presentment and dishonour.

**“Encrypted Pre-shared Secret”** means a router configuration option that results in all authentication parameters retained within the device, being maintained in an encrypted form such that their value is not readily discernable.

**“Interchange, Interchange Agreement, Interchange Link and Interchange Line”** have the meanings given to them in the CECS Regulations and CECS Manual.

**“ISO”** means the International Standards Organisation.

**“Plain Text Pre-shared Secret”** means a router configuration that results in authentication parameters retained in the device being kept in plain text and therefore readily discernable.

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

#### **1.4 Introduction to the COIN**

The COIN is a high availability, managed network used by Members for the exchange of CECS Items (CS3), CECS reports (CS3), Items contained within DE Files (CS2) and Electronic Presentment and dishonour files (CS1), as well as related settlement items exchanged with the Reserve Bank.

The COIN is an optional alternative to point-to-point connectivity between Members. The requirements for Interchange Links and Interchange Lines as specified in the CECS Manual clause 2.2 apply to CS3 Interchanges constructed via the COIN where applicable.

As the COIN provides any-to-any connectivity between connecting Members, the responsibility for limiting connectivity to only COIN Members rests with all COIN Members and shall be accomplished through the establishment of distinct Virtual Private Network connections for each individual bilateral link.

#### **1.5 Permitted Traffic Types**

The COIN is available for the transmission of the traffic types identified below. In addition other payment or settlement related traffic may be carried if agreed bilaterally and the requirements of Part 5.2 of the COIN Regulations continue to be met.

(a) **CS1 Participation**

The COIN is available to CS1 members for the exchange of Electronic Presentment and Dishonour and other related CS1 files. Additionally the COIN is available to CS1 members for the exchange of settlement data with the Collator/Reserve Bank.

(b) CS2 Participation

The COIN is available to CS2 members for the exchange of Direct Entry and Direct Entry Summary files. Additionally the COIN is available to CS2 members for the exchange of settlement data with the Collator/Reserve Bank.

(c) CS3 Participation

The COIN is available to CS3 members for the exchange of AS2805 financial transaction messages and associated report files.

Additionally the COIN is available to all CS3 members for the exchange of settlement data with the Collator/Reserve Bank.

## **1.6 COIN Termination Points**

The COIN is a domestic network and all end-points (i.e., IPsec VPN) must be terminated within Australia.

**The next page is 2.1**

---

## 2 GENERAL STANDARDS

### 2.1 Security

(a) Information Security Policy

Where appropriate existing national and international standards that relate to shared financial networks shall be incorporated into a COIN Member's security policy. In this context ISO 27001 is seen to be highly relevant.

(b) Cryptographic Key Management – General

All cryptographic key management practices shall conform to AS 2805 part 6.1.

For the purposes of this document Pre-shared secret passwords and similar authentication values are not to be regarded as cryptographic keys and the following sub-clauses do not apply.

(c) Key Sizes, Algorithms and Life Cycles

The following sub-clauses specify the permitted cryptographic algorithms and minimum key sizes that must be used to protect data within the COIN.

(i) Data Protection Keys

Data Protection Keys are those keys used to provide confidentiality and/or authenticity to data transmitted across the COIN (e.g., session keys).

(ii) Approved Algorithms for Data Protection Keys

Triple DES (DEA3) and AES are the only approved algorithms for the protection of data.

(iii) Minimum Key Length for Data Protection Keys

The minimum key-length for Data Protection keys is 112-bits.

(iv) Transport Keys (Key Encryption Keys)

Transport keys are those keys used to protect another cryptographic key when it is necessary to transport the underlying key.

(v) Approved Encryption Algorithms for Transport Keys

DEA2, DEA3 and AES are the only approved algorithms for the protection of keys in transport.

(vi) Minimum Key Length for Transport Keys

DEA2 key lengths must be equal to or greater than 2048 bits in length.

Triple DES (DEA 3) may use either 112-bit or 168-bit key sizes.

AES shall use a minimum key size of 128-bits.

(vii) Key Life Cycle Practices for Transport Keys

AES and DEA3 Key Transport Keys are single use keys only.

They must be freshly generated to protect keys in transport and then securely destroyed after use.

At the time of publication, DEA2 keys of size equal to or in excess of 2048 bits are deemed acceptable for a key change interval (life time) of two (2) years.

(viii) Domain Master Keys (DMK/LMK)

These keys are used within a financial institution to protect keys stored internal to the organisation.

(ix) Minimum Key Length for Domain Master Keys

Domain Master Keys shall be DEA3 keys with a minimum length of 128-bits (112 effective).

## 2.2 Unauthorised Access Prevention

All COIN Members, including any third parties engaged by a COIN Member in the delivery of COIN services and any intermediate network entities must maintain procedures for detecting and preventing any unauthorised access to or use of, the COIN through their own hardware, software, lines and operational procedures which enable the exchange of authorisation and reconciliation of financial messages.

## 2.3 Incident Management

Members must implement and use controls in the COIN and any associated networks/equipment:

- (a) to prevent fraud;
- (b) to allow for the timely and effective detection of activities indicative of fraud; and
- (c) to allow fraud and other security incidents to be responded to on a timely and effective basis.

Incidents or potential incidents associated with the COIN or COIN infrastructure of a security nature must be reported in a timely manner to the COIN Administrator.

COIN Members must provide an incident report to the COIN Administrator if there is an unplanned outage of more than 30 minutes which affects a Member's ability to continue exchanges across the COIN. The incident report needs to be available within two weeks of the outage and cover the cause, impact, sequence of events and resulting action items.

The COIN Administrator will maintain a register of all COIN incidents and produce an annual report for the COIN Management Committee.

#### **2.4 Member Change Window**

Unless bilaterally agreed otherwise, and subject to any overarching APCA clearing system rules: Changes which may impact a COIN Member's production connectivity to the COIN and associated Member infrastructure for CS3 transaction messages, other than for emergency remedial repair shall only be made to the COIN during approved change windows which are between the hours of 00:01 to 02:00 on Monday morning, Sydney time.

Changes which may impact a COIN Member's production connectivity to the COIN and associated Member infrastructure for other exchanges, other than for emergency remedial repair, shall only be made during approved change windows which are after final exchanges Saturday mornings and before 02:00 on Monday mornings, Sydney time.

#### **2.5 Member Change Freeze**

No changes, alterations or additions, other than emergency remedial repair, shall be made to a COIN Member's production connectivity during times of peak usage. Currently these times are the two weeks immediately prior to and including Easter, and the four weeks preceding Christmas day.

The Management Committees of Approved Clearing Systems may designate other such times as it may determine provided a minimum of four weeks notice is provided to all COIN Members.

#### **2.6 Network**

Each separate bilateral link within the COIN must be transported within a distinct, IPSec protected Virtual Private Network (VPN) connection between the two communicating COIN Members.

The minimum IPSec VPN requirements include:

- (a) the system must be configured to use Encapsulating Security Payload, authentication must be HMAC-SHA-1;

- 
- (b) data encryption must use DEA-3 with either a 112-bit or 168-bit key length or AES with a minimum key length of 128-bits;
  - (c) the data stream must be fully encrypted with the exception of communication headers;
  - (d) either certificates or Encrypted Pre-shared Secrets must be used (Plain Text Shared Secrets are not acceptable);
  - (e) key management if used, must comply with AS 2805 part 6.1;
  - (f) VPN tunnel termination points must be within the COIN Member's or their trusted agent's facilities;
  - (g) the facility must be supported by documented device management procedures with identified roles and responsibilities and subject to internal audit as prescribed by the COIN Member's security policy;
  - (h) split tunnelling is not to be used, that is no VPN bypass shall be provided by the network;
  - (i) the minimum Diffie-Hellman MODP group size is 1536-bits;
  - (j) IPSec Security Association lifetimes must not exceed 24 hours; and
  - (k) IKE, if used, must be configured to only use main mode, specifically aggressive mode must NOT be used.

## 2.7 Management Requirements of Authentication Parameters

The management practices adopted for any Authentication Parameter (e.g., an IPSec Encrypted Pre-shared Secret) shall be such as to ensure that:

- (a) it is known only to the minimum number of people required to meet availability and business requirements;
- (b) it is constructed from two distinct vectors each with a minimum length of 16-alphanumeric characters;
- (c) the individual characters must be created by a random or pseudo random process;
- (d) each COIN Member will provide one of the vectors and the two parts shall be concatenated to form the final Authentication Parameter;
- (e) both component vectors of the pre-shared secret shall be securely stored and managed by the recipient Member;
- (f) access to the vectors shall be controlled and all access logged in an auditable manner;

Amended  
effective date  
19.12.11

- (g) the authentication parameter is unique, except by chance, between each pair of communicating COIN Members;
- (h) the exchange of the authentication vectors is performed in a secure manner such as to prevent disclosure of the value to other than the intended recipient (e.g., PGP encrypted email); and
- (i) the authentication value is replaced on a three-yearly basis with a new value not related to the current value.

## **2.8 Email Exchange of Authentication Parameters**

The use of encryption is mandatory if the Authentication Parameters are to be transmitted over a public network such as the Internet.

The size of any keys used in a public key cipher system used to provide file encryption (e.g., RSA) must be a minimum of 2048 bits.

The size of any key used in a private key cipher system used to provide file encryption (i.e., 3DES) must be a minimum of 112 bits.

The email security package if used must, at a minimum, include the following encryption features:

- (a) the ability to prevent viewing of email and its attachments by outside parties other than the intended recipient;
- (b) the ability to prevent the email and its attachments being read by unauthorised persons within your organisation;
- (c) the ability to securely send the email and its attachments 'locked' with a public key;
- (d) the ability of the recipient to open the email and its attachments by 'unlocking' the transmission with a securely generated private key; and
- (e) the ability of the sender to digitally sign the email transmission.

A central repository of a COIN Member's Custodian's public key may be found on the Company's extranet.

## **2.9 Host System Requirements**

As the COIN will be used by some COIN Members for the transportation of card and PIN data, it is to be considered a highly confidential network. Consequently close attention must be paid to minimising any risk exposures and maintaining a high level of security. At a minimum the following requirements apply to any host or network carrying COIN traffic or providing COIN services.

- (a) Stateful firewalls must protect all external entry points to the COIN Member's host environment;
- (b) Financial messages, associated with the COIN, must be conveyed over secure, logically protected networks that are separate from other generic networks within the COIN Member's environment that provide internal or external access;
- (c) COIN Members employing Security Control Modules shall ensure that Security Control Modules are accessible only to authorized hosts and authorized applications. Where connected via TCP/IP they must be on a separate, stand-alone, network;
- (d) The host environment shall provide, at a minimum, an IPS or IDS between the perimeter network firewall and the host; and
- (e) The host system must support appropriate threat management techniques relevant to the hosts operating platform, such as malware protection with up-to-date signatures and maintenance, vulnerability patching, etc.

## **2.10 Contingency**

- (a) Responsibility

COIN Members have a responsibility to each other and to APCA as a whole, to co-operate in resolving any processing difficulty including during a Contingency.

To the extent that such co-operation does not adversely affect its own processing environment, a COIN Member receiving a request for assistance may not unreasonably withhold such assistance.

**The next page is 3.1**

---

### 3 COIN MEMBER OPERATING RULES

#### 3.1 Redundant connections

Each COIN Member must maintain two distinct connections to the COIN network. Sufficient redundancy must be provided to ensure that no single point-of-failure exists within the network components under each Member's control. An active-active configuration is preferred for Members with large clearing volumes (i.e., greater than 5% in any Approved Clearing System).

Amended  
effective date  
19.12.11

As a minimum, two of the distinct COIN connections must meet the minimum bandwidth requirements set out in clause 3.4.

#### 3.2 Connectivity Options

No ADSL or wireless access to the COIN is permitted. Otherwise COIN Members may choose their own type of connections. However the Business Digital Subscriber Line (BDSL) connectivity option, due to its reduced support window, is only acceptable for test connections and test traffic.

#### 3.3 Availability and Support

A COIN Member's COIN infrastructure and support arrangements shall be such as to meet the availability requirements of the payment system being transported or the bilateral Agreement to Exchange, whichever is the greater.

Furthermore, as a minimum, Telstra's Express 4 Plus service level must be taken up. For Members using IPMAN connections, it is strongly recommended that Telstra's Express 2 Plus service level is selected.

Inserted effective  
date 28/07/10

#### 3.4 Minimum bandwidth

Sufficient bandwidth should be provided on each COIN connection link to ensure that the transmission and/or reception of the largest file size likely to be received or transmitted is such as to ensure that any ensuing delay to CS3 transaction messages does not exceed 1 second.

Each COIN Members systems and network connections must be able to transmit all inbound and outbound clearing files (from host to host) in a peak day in under 2 hours. This should be based on projected volumes 2 years into the future.

#### 3.5 QoS

Quality of Service (QoS) prioritisation is a key measure to prevent bulk payment transfers (e.g. CS2 file transfers) impacting on higher priority traffic such as card related real-time traffic.

Amended  
effective date  
19.12.11

The COIN network will honour QoS with reduced packet loss, reduced jitter and greater allocated bandwidth based on COS marking in the IP header.

The COIN network will support Differentiated Services architecture (RFC 2745) and inbound traffic must be marked by the COIN Member prior to ingress into the COIN and in accordance with RFC 2474 and Table 1 which illustrates the settings of the TOS field in the IP header for each of the supported traffic types. The highest setting is reserved for real-time card-related traffic and the lowest for all test traffic with file transfers and non-card real time traffic occupying intermediate positions.

Amended effective date 19.12.11

Amended effective date 19.12.11

TOS Byte (IPv4)											
IP Precedence											
DCSP						Flow Ctl					
b7	b6	b5	b4	b3	b2	b1	b0	PHB	DSCP (decimal)	TOS (decimal)	Usage
0	0	0	0	0	0	0	0	Default	0	0	Test
0	0	1	0	0	0	0	0	CoS1	8	32	File Transfers/batch
0	1	0	0	0	0	0	0	CoS2	16	64	Reserved
0	1	1	0	0	0	0	0	CoS3	24	96	Non-card real time
1	0	0	0	0	0	0	0	CoS4	32	128	Card-related real time

**Table 1 assigned DSCP Values**

All approved traffic must comply with the CoS usage model shown.

Amended effective date 19.12.11

### 3.6 Separation of test environments

COIN Members must ensure that security is enforced between their internal application(s) and the COIN, so that an unauthorized copy of an application, (e.g., a test version, may not accidentally send messages through the network to the production system of another COIN Member.)

Test systems must be explicitly separated from production environments through distinct IP address assignments.

Test traffic of all types, shall use a DSCP value of "0" (see Table 1) unless bilaterally agreed otherwise and specifically for the purposes of testing QoS. In all cases attention must be paid to ensuring that production traffic is not impacted in any material way by the use of test systems and the transmission of test traffic.

Amended effective date 28/07/10

### 3.7 IP Addressing

Telstra will be responsible for the assignment of IP addresses. Separate pools will be maintained for host and IPSec termination points. Both host and IPSec addresses will be public addresses assigned from the class A address space 29.x.x.x with a minimum network range of /28.

As this address range is an assigned InterNIC range, COIN Members must ensure that these addresses are terminated within COIN infrastructure and are not propagated throughout the member's general network.

The use of other public addressing for host addressing is permitted using InterNIC addressing allocated to the COIN member.

### **3.8 Security Event Management**

Each COIN Member must implement processes and procedures to address the threat of security events and their response to these events. Listings of event types that are to be addressed are documented in Appendix ANNEX A.

Members must also meet logging requirements for security events, escalation requirements, response requirements and contingency arrangement requirements as specified in Appendix ANNEX A.

Members must respond to security events with an urgency that corresponds to their severity. In general, prudent business judgment must be used to determine the timing and use of resources for solving any problem.

A Member must immediately notify any other Member, the COIN Administrator and APCA's Risk and Compliance Manager of any security event where another Member may be at risk.

Members must have a documented plan to deal with emergency response and fraud detection issues. This plan must identify the triggers for invoking the plan, the escalation process, key contacts and the actions that will be taken.

### **3.9 Suspension of Connectivity**

Where in the reasonable opinion of a COIN Member or other intermediate network entity, excessive response times or traffic volumes from another party are causing a downgrading of the service level in the COIN the first affected party may temporarily suspend its services for such period or periods as it shall think fit to restore the service level to the normal level. Such suspension of services shall be accomplished by blocking at the network layer the offending source IP address(es).

The first affected party shall notify the other party and the COIN Administrator prior to suspending the service if practical or at the earliest opportunity after suspending the service.

### 3.10 Certification

Constant developments in new equipment and network processes require security and operational standards and guidelines to be reviewed to maintain a high standard of security and operational procedures in the COIN environment. At any one time there will be current and draft future standards. Current industry standards will be subject to an ongoing process of review and the COIN Management Committee will upgrade and re-issue applicable standards on a rolling triennial basis.

(a) Requirement for Certification

Each COIN Member who wishes to participate in the transmission and/or reception of data over the COIN must arrange for Certification before it commences transmission.

(b) Certification

Certification means that a person (being an existing or a prospective COIN Member confirms by completing and submitting to the Company a Certification Checklist (satisfactory to the Company) that when it operates in the COIN with other Members, it is able to, and does, meet the COIN requirements in force at that time.

### 3.11 Default File Transfer Protocol

The file transfer protocol to be used within the COIN is to be agreed bilaterally. The industry default file transfer protocol is Connect Direct. All COIN Members must be capable of supporting this protocol as it is to be used where bilateral agreement cannot be reached.

It is recommended that compression is turned on for all outbound traffic sent using Connect Direct.

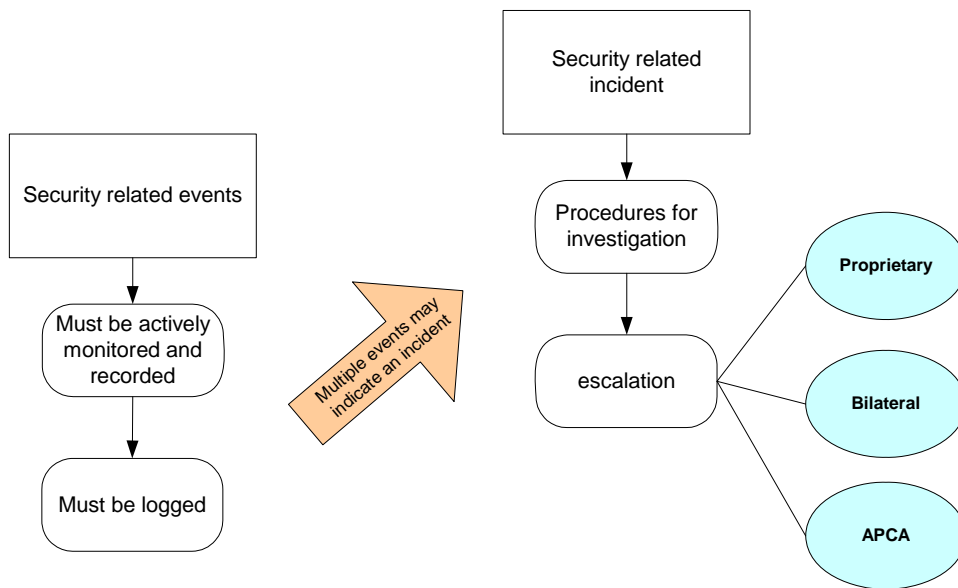
Inserted effective  
19.12.11

**The next page is A.1**

## ANNEX A SECURITY EVENTS, LOGGING, ESCALATION AND CONTINGENCY

### A.1 Introduction

Members must implement processes and procedures to ensure that Security Incidents occurring within or directed at COIN infrastructure are protected against, detected, logged, escalated, and responded to.



### A.2 Responding to Security Incidents

COIN Members must respond to Security Incidents with an urgency that corresponds to their severity. In general, prudent business judgment must be used to determine the timing and use of resources for solving any problem. A COIN Member must immediately notify any other COIN Member, the COIN Administrator and APCA's Risk and Compliance Manager of any Security Incident where another Member may be at risk.

### A.3 Standards for Security Events and Incidents

#### (a) Security Events Definition

The following are considered Security Events:

- (i) automated Key distribution errors;
- (ii) incorrect Message Authentication Code (MAC) Value, data used to calculate the MAC is different;
- (iii) invalid PIN Block, ANSI PIN block is incorrect;

- (iv) PIN translation errors;
- (v) connection attempts to unassigned ports;
- (vi) connection attempts from unauthorised IP addresses;
- (vii) port scanning attacks;
- (viii) denial of service attacks;
- (ix) messages without a MAC where a MAC is expected; and
- (x) other incidents that in the expert opinion of the COIN Member may constitute a threat or likely threat to the COIN infrastructure.

(b) Security Incidents Definition

The following are considered Security Incidents

- (i) any known or suspected compromise of cryptographic Key security;
- (ii) successful connection attempts to other than assigned ports;
- (i) any attempted or successful Denial-of-Service attack;
- (iii) repeated port scanning attacks; and
- (iv) multiple connection attempts from unauthorised IP addresses.

#### **A.4 Defence against Security Events and Incidents**

Each COIN Member must implement procedures and processes that form an effective defensive response to security events and incidents and to unusual activity that may occur within the COIN infrastructure. The response should be escalated in terms of prudent management practices.

#### **A.5 Emergency Response and Fraud Detection Plan**

COIN Members must have a documented plan to deal with emergency response and fraud detection issues. The plan must identify the triggers for invoking the plan, the escalation process, key contacts and the actions that will be taken.

#### **A.6 Recording of Security Events**

Each COIN Member must accurately detect and record Security Events. Security Events must be accurately identified and reported according to the categories specified in A.3.

A Security Event must remain on record for a period of no less than one year from the date of occurrence.

## **A.7 Resolving Security Incidents**

The requirements for resolving Security Incidents are:

- (a) The resolution of any Security Incident must be done on a case-by-case basis provided the COIN Member fulfils the general obligations set out in clause A.2 above.
- (b) Security event logs must be actively monitored by each COIN Member.
- (c) Each COIN Member must develop and implement procedures which define the steps for investigating events and, where necessary, escalating an incident. Such procedures must include, but not be limited to:
  - (i) Regular follow-up of messages for security events. A COIN Member should implement automated techniques as an aid to timely incident detection and reporting and for alerting the other COIN Members about severe or persistently recurring events.
  - (ii) Guidelines for investigating Incidents and for listing causes of error messages according to event type, including a description of standard methods used for rectifying the problematic situations.
  - (iii) Escalation procedures must allow for the incremental escalation of Security Incidents from the proprietary network to affected and/or potentially affected other COIN members and the COIN Administrator, then, if necessary, to APCA.
  - (iv) Contact names, locations and phone numbers to be used in conjunction with the escalation procedures.
- (d) Security Incidents involving one or more COIN Members must be resolved by the parties involved. Security Incidents affecting a COIN Member need not be reported to other COIN Members or the COIN Administrator, provided the COIN Member fulfils the general obligations set out in clause A.2 above.

## **A.8 Logging Requirements**

Each occurrence of a Security Event must be logged.

To provide an adequate audit trail for reporting and investigating Security Events must be recorded with sufficient detail to permit an in-depth analysis of the problem and its likely affects.

For CS3 financial messages the following fields of a financial transaction at a minimum, if present in a message, must be logged by the COIN Member:

- (a) Message type;

- (b) Truncated Primary Account Number;
- (c) Transaction date and time;
- (d) Originating AIN;
- (e) Destination IIN;
- (f) Processing Code;
- (g) Transaction amount, and replacement amount, if indicated;
- (h) Response code;
- (i) Retrieval Reference Number or systems trace audit number;
- (j) Terminal ID;
- (k) Additional data (field 48);
- (l) Security control information; and
- (m) STAN.

Logged information must be kept in an access-controlled location for a minimum period of one year.

**The next page is B.1**

---

**ANNEX B COIN MEMBER CERTIFICATION CHECKLIST**

**TO:** COIN ADMINISTRATOR  
AUSTRALIAN PAYMENTS CLEARING ASSOCIATION LIMITED  
LEVEL 6, 14 MARTIN PLACE  
SYDNEY NSW 2000

**RE:** COIN CERTIFICATION

**FROM:** NAME OF APPLICANT (“Applicant”) \_\_\_\_\_

PLACE OF INCORPORATION \_\_\_\_\_

AUSTRALIAN COMPANY NUMBER /  
AUSTRALIAN BUSINESS NUMBER /  
AUSTRALIAN REGISTERED BODY NUMBER \_\_\_\_\_

REGISTERED OFFICE ADDRESS \_\_\_\_\_

NAME OF CONTACT PERSON \_\_\_\_\_

TELEPHONE NUMBER \_\_\_\_\_

FACSIMILE NUMBER \_\_\_\_\_

EMAIL ADDRESS \_\_\_\_\_

---

**Certification Objectives**

The objective of Certification is to ensure that:

- each COIN Member confirms for the benefit of each other COIN Member and APCA that it meets the technical, operational and security requirements applicable to COIN Members which are set out in Part 2 and 3 of the COIN Operating Manual as applicable;
- each COIN Member which:
  - acquires, modifies or upgrades devices, interchanges or systems, other than for remedial repairs, maintenance or routine software and hardware updates, associated with the COIN,

to that extent confirms, for the benefit of each other COIN Member and APCA, that its system or enhancements to its system (as the case may be) meet all applicable technical, operational and security requirements for COIN Members as set out in the COIN Operating Manual; and

- each COIN Member which is Certified renews its Certification at least triennially or on such other date as determined by the COIN Management Committee.

<b>REQUIRED CAPABILITIES FOR COIN MEMBERS</b>		
<b>STANDARDS</b>		
<b>Required Capabilities for COIN Member Certification</b>		<b>Applicable Sections</b>
<b>(Please complete all sections below)</b>		
B.1	Information Technology assets associated with, or connected to the COIN are protected with an appropriate security policy	Part 2.1(a)
B.2	Cryptographic Key management, where used, complies with AS 2805 part 6.1	Part 2.1(b)
B.3	Cryptographic Key sizes and algorithms protecting COIN data comply with requirements	Part 2.1(c)
B.4	Controls are in place to detect and prevent unauthorised access	Part 2.2
B.5	An incident management system is in place and complies with requirements	Part 2.3
B.6	Network separation is implemented appropriately	Part 2.6
B.7	Authentication Parameters are managed appropriately	Part 2.7
B.8	Host system requirements are met	Part 2.9

<b>OPERATING RULES</b>		
B.9	Sufficient Bandwidth is available to meet requirements	Part 3.4
B.10	Quality of Service is implemented and complies with requirements	Part 3.5
B.11	Test environment separation is maintained	Part 3.6
B.12	Security Event management system is in place and complies with requirements	Part 3.8

**REPRESENTATIONS AND UNDERTAKINGS**

By signing this Certification Checklist, the Applicant named below:

- (a) acknowledges that for the Applicant to qualify for membership of the COIN the Applicant must have obtained Certification in accordance with the COIN Regulations and Operating Manual and that this Certification Checklist is required to obtain that Certification;
- (b) warrants and represents that it satisfies the requirements applicable generally to COIN Members as set out in Part 2 and Part 3, as applicable, of the COIN Operating Manual as at the date of this Certification Checklist and that the information contained in this completed Certification Checklist is correct and accurately reflects the results of system testing against current COIN standards and including, if applicable, use of an appropriate test script supplied by APCA;
- (c) agrees that if the Applicant is granted Certification, in consideration of such Certification, to:
  - (i) immediately notify APCA if it becomes, or has become, aware that any information contained in this Certification Checklist is wrong or misleading (including without limitation because of any omission to provide relevant additional information); and
  - (ii) provide APCA with that notification full particulars of that wrong or misleading information; and

Terms used in this Checklist in a defined sense have the same meanings as in the COIN Operating Manual unless the context requires otherwise.

**SIGNED FOR AND ON BEHALF OF THE APPLICANT**

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

Name of Authorised Person	Signature of Authorised Person
Office Held	Date

**AUDITOR/RESPONSIBLE PERSON<sup>1</sup> SIGNOFF**

Amended effective date 19.12.11

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

Name of Auditor / Responsible Person	Signature of Auditor / Responsible Person
Date	

**The next page is C.1.**

<sup>1</sup> It is expected that this person would be from a separate part of the business from the other signatory, although need not be external to the company.

## **ANNEX C MEMBER CONTACT LIST**

Details of a COIN Member's operational support and Custodial contact details may be found on the APCA Extranet <https://extranet.apca.com.au/>.