As amended to:
30 March 2023
Version E011

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

COMMUNITY OF INTEREST NETWORK (COIN) OPERATING MANUAL

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

COMMUNITY OF INTEREST NETWORK (COIN)

OPERATING MANUAL

The next page is 1.1

PREFACE

This initial release of the AusPayNet 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 Framework Participants and prospective Framework Participants.

Amended effective 30.03.23

Compliance with these standards and rules (as reviewed from time to time) on a uniform basis through AusPayNet will contribute to the continued integrity of all COIN-Approved Payment Systems. In particular these COIN standards and rules seek to ensure that:

Amended effective 09.05.16

- 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

Amended effective 01.01.23

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

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

(c) 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;

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

(e) words defined in the Corporations Law have, unless the contrary intention appears, the same meaning in this Manual;

(f) words defined in the COIN Regulations have, unless the contrary intention appears, the same meaning in this Manual;

(g) 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

(h) 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.

"**AusPayNet**" means Australian Payments Network Limited. Inserted effective 01.01.18

"**Authentication Parameter**" [deleted]. Deleted effective 01.01.23

"**BATNA**" or "**Best Alternative to a Negotiated Agreement**" is used to describe the default additional security controls which may apply as between Communicating COIN Framework Participants in accordance with clause 3.11 and Annex D and/or Annex E. Inserted effective 30.03.23

"**Card-related**" includes an electronic funds transfer, cash withdrawal, or balance enquiry initiated using a card, device, application or identifier issued for the purpose of effecting a payment. Amended effective 09.05.16

"**Class of Service**" or "**CoS**" is used to differentiate network traffic in order to facilitate Quality of Service (QoS). It is determined by setting specific values in the DSCP to define each Class of Service. Refer to clause 3.5. Inserted effective 01.01.17

"Communicating COIN Framework Participants" is used to describe Framework Participants who transmit Approved Traffic with each other over the COIN. Inserted effective 30.03.23

"**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. 0

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

"**Differentiated Service Code Point**" or "**DSCP**" means a field in the IP header used to determine QoS behaviour. Refer to clause 3.5. Inserted effective date 01.01.17

"**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 Framework Participant to participate to the normal and usual extent in interchange and/or clearing and settlement. Amended effective 30.03.23

"**Electronic presentment and dishonour files**" [deleted] Deleted effective 09.05.16

"**Encrypted Pre-shared Secret**" [deleted]. Deleted effective 01.01.23

"**Interchange, Interchange Agreement, Interchange Link and Interchange Line**" have the meanings given to them in the code set for the Issuers and Acquirers Community. Amended effective 09.05.16

"**ISO**" means the International Standards Organisation.

"**Plain Text Pre-shared Secret**" [deleted]. Deleted effective 01.01.23

"**Quality of Service**" or "**QoS**" means a network capability to differentiate traffic into different priorities so that appropriate levels of network resources can be applied to achieve the desired performance level. Refer to clause 3.5. Inserted effective 01.01.17

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

"**Type of Service**" or "**TOS**" means a field in the IP header that contains data such as the DSCP to enable Quality of Service (QoS) over the network. Refer to clause 3.5. Inserted effective 01.01.17

1.4 Introduction to the COIN

The COIN is a high availability, managed network used by Framework Participants for the transmission of payments-related messages and files, as well as related settlement items exchanged with the Reserve Bank. Last amended effective 30.03.23

The COIN is an optional alternative to point-to-point connectivity between Framework Participants. The requirements for Interchange Links and Interchange Lines as specified in the code set for the Issuers and Acquirers Community apply to Interchanges constructed via the COIN where applicable.

Last amended effective 30.03.23

As the COIN provides any-to-any connectivity between connecting Framework Participants, the responsibility for limiting connectivity to only COIN Framework Participants rests with all COIN Framework Participants.

Last amended effective 30.03..23

1.5 Permitted Traffic Types

The COIN is available for the transmission of all Approved Traffic, (being the electronic messages and/or files specified in the regulations, procedures or like documents for a COIN-Approved Payment System or any other traffic approved by the COIN Management Committee). A list of all COIN-Approved Payment Systems is available on the COIN Administrator's extranet. In addition, other payment or settlement related traffic may be carried if agreed bilaterally and to the extent described in the Agreement to Exchange between those Framework Participants.

Last amended effective 01.01.20

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

Amended effective 01.01.23

Clauses (a) and (b) apply to both COIN Framework Participants and the COIN Service Provider. Clause (c) applies only to COIN Framework Participants.

Amended effective 30.03.23

(a) Information Security Policy

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

Amended effective 30.03.23

(b) Cryptographic Key Management – General

All cryptographic key management practices shall conform to ISO 11568 all parts.

Amended effective 01.01.23

(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

Amended effective 30.03.23

All COIN Framework Participants, including any third parties engaged by a COIN Framework Participant 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

Amended effective 30.03.23

Framework Participants 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 Framework Participants must provide an incident report to the COIN Administrator if there is an unplanned outage of more than 30 minutes which affects a COIN Framework Participant'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.

Amended effective 30.03.23

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

2.4 Framework Participant Change Window

Amended effective 30.03.23

Unless bilaterally agreed otherwise, and subject to any overarching AusPayNet clearing system rules: Changes which may impact a COIN 'Framework Participant's production connectivity to the COIN and associated Framework Participant infrastructure for Card-related 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.

Last amended effective 30.03.23

Changes which may impact a COIN Framework Participant's production connectivity to the COIN and associated Framework Participant 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.

Amended effective 30.03.23

When seeking bilateral agreement to schedule any COIN infrastructure changes that impact upon other COIN Framework Participants in any way, a COIN Framework Participant is encouraged to give as much notice as possible to other COIN Framework Participants and cooperate fully in finding mutually acceptable dates.

Amended effective 30.03.23

2.5 Framework Participant Change Freeze

Amended effective 30.03.23

No changes, alterations or additions, other than emergency remedial repair, shall be made to a COIN Framework Participant'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 Framework Participants.

2.6 Network

Amended effective 01.01.23

Amended effective 30.03.23

The COIN Service Provider will provide distinct, IPSec protected Virtual Private Network connections that will be used between two Communicating COIN Framework Participants.

The minimum IPSec VPN specifications that will be used include:

(a) the system will be configured to use Encapsulating Security Payload, authentication must be at a minimum HMAC-SHA-2;

(b) data encryption will be AES with a minimum key length of 256 bits;

(c) the data stream will be fully encrypted with the exception of communication headers;

(d) certificates will be used;

(e) key management if used, must comply with AS ISO 11568 all parts;

(f) VPN tunnel termination points will be on the COIN Service Provider's equipment within the COIN Framework Participant's or their trusted agent's facilities;

Amended effective 30.03.23

(g) the minimum Diffie-Hellman MODP group size is 1536-bits; and

(h) IPSec Security Association lifetimes will not exceed 24 hours.

2.7 Management Requirements of Authentication Parameters [Deleted]

Deleted effective 01.01.23

2.8 Email Exchange of Authentication Parameters [Deleted]

Deleted effective 01.01.23

2.9 Host System Requirements

Last amended effective date 30.03.23

As the COIN will be used by some COIN Framework Participants for the transportation of identifying and authenticating data (such as 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 Framework Participant's host environment;

Amended effective 30.03.23

(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 Framework Participant's environment that provide internal or external access;

Amended effective 30.03.23

(c) COIN Framework Participants 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; Amended effective 30.03.23

(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 Framework Participants have a responsibility to each other and to AusPayNet as a whole, to co-operate in resolving any processing difficulty including during a Contingency. Amended effective 30.03.23

To the extent that such co-operation does not adversely affect its own processing environment, a COIN Framework Participant receiving a request for assistance may not unreasonably withhold such assistance. Amended effective 30.03.23

The next page is 3.1

3 COIN FRAMEWORK PARTICIPANT OPERATING RULES

Amended effective 30.03.23

3.1 Redundant connections

Each COIN Framework Participant must maintain two distinct connections to the COIN network. The COIN Service Provider, will at a minimum, supply redundant, carrier diverse circuits and equipment for each of these connections. Sufficient redundancy must be provided to ensure that no single point-of-failure exists within the network components under each Framework Participant's control. An active-active configuration is preferred for Framework Participants with large clearing volumes (i.e., greater than 5% in any Approved Clearing System).

Last Amended effective 30.03.23

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

All COIN connections, regardless of whether they are inactive, redundant or backup connections, must be tested and verified annually to prove that they function correctly (i.e. end to end acknowledged traffic between Framework Participant's Hosts, e.g. Telnet Test). Connections that are regularly used for normal production processing (e.g. in an active-active configuration) do not require any additional verification.

Last amended effective 30.03.23

3.2 Connectivity Options [Deleted]

Deleted effective 01.01.23

3.3 Availability and Support

Amended effective 01.01.23

A COIN Framework Participant'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.

Amended effective 30.03.23

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 real time transaction messages does not exceed 1 second.

Amended effective 09.05.16

Each COIN Framework Participants 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.

Amended effective 30.03.23

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 09.05.16

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 Framework Participant 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-related real time traffic occupying intermediate positions.

Amended effective 30.03.23

Amended effective 09.05.16

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-related 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 19.12.11

3.6 Separation of test environments

COIN Framework Participants 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 Framework Participant.)

Amended effective 30.03.23

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 28.07.10

3.7 IP Addressing and Network Address Translation

Amended effective 01.01.23

The COIN Service Provider will utilise Network Address Translation across the COIN to avoid IP Address clashing between COIN Framework Participants. Applications utilising the COIN must be NAT aware.

Amended effective 30.03.23

3.8 Security Event Management

Amended effective 30.03.23

Each COIN Framework Participant 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.

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

Framework Participants 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 Framework Participant must immediately notify any other Framework Participant, the COIN Administrator and AusPayNet's Risk and Compliance Manager of any security event where another Framework Participant may be at risk.

Framework Participants 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

Amended effective 30.03.23

Where in the reasonable opinion of a COIN Framework Participant 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

Amended effective 01.07.15

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 as required.

(a) Requirement for Certification

Each COIN Framework Participant 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 Optional Additional Encryption

Inserted effective 30.03.23

Additional encryption between two Communicating COIN Framework Participants is permitted where one or both Communicating COIN Framework Participants require it. If only one party from a pair of Communicating COIN Framework Participants requires additional encryption measures to be implemented, the other party is obliged to negotiate and attempt to agree upon the additional encryption measures to be implemented.

Note: While the implementation of application-level encryption between two Communicating COIN Framework Participants would maximise the benefits of the TNS COIN network design, this is not a requirement and Communicating COIN Framework Participants are able to reach an agreement which meets their respective needs.

(a) Financial Transactions BATNA

Where additional encryption is required for transmission of financial transactions data over the COIN, and bilateral agreement cannot be reached between two Communicating COIN Framework Participants, both parties will be required to implement VPN tunnels as defined in Annex D below.

(b) File Transfer Protocol BATNA

Where additional encryption is required for transmission of files over the COIN and that bilateral agreement cannot be reached between two Communicating COIN Framework Participants, both parties will be required to use Connect: Direct Secure Plus as defined in Annex E below.

Where Connect Direct is used, it is recommended that compression is turned on for all outbound traffic.

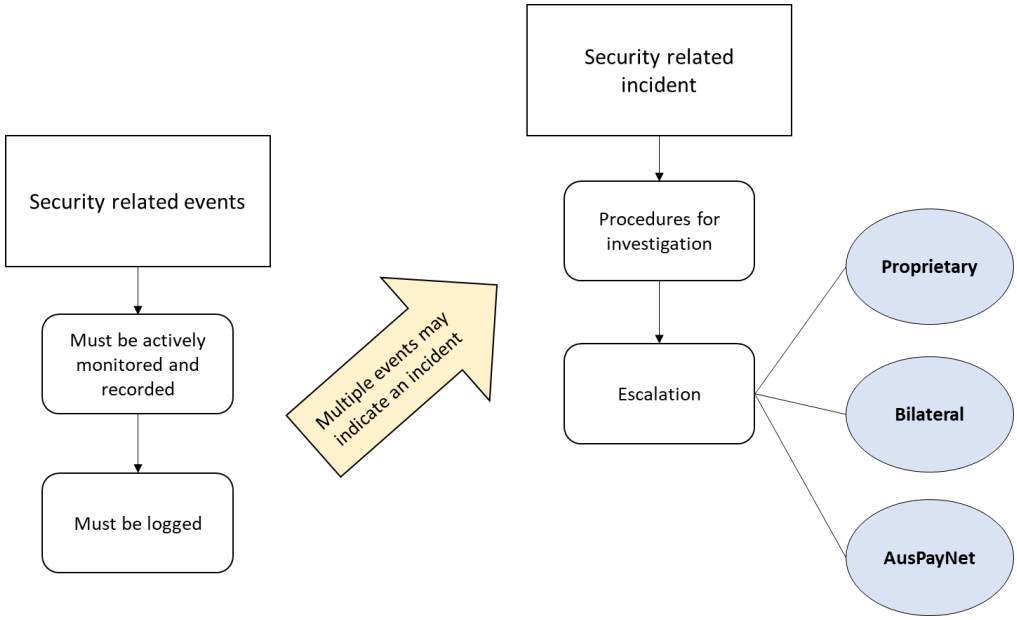
The next page is A.1

ANNEX A SECURITY EVENTS, LOGGING, ESCALATION AND CONTINGENCY

A.1 Introduction

Framework Participants 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.

Amended effective 30.03.23



A.2 Responding to Security Incidents

COIN Framework Participants 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 Framework Participant must immediately notify any other COIN Framework Participant, the COIN Service Provider, the COIN Administrator and AusPayNet's Risk and Compliance Manager of any Security Incident where another Framework Participant may be at risk.

Last Amended effective 30.03.23

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 Framework Participant may constitute a threat or likely threat to the COIN infrastructure. Amended effective 30.03.23

(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 Framework Participant 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. Amended effective 30.03.23

A.5 Emergency Response and Fraud Detection Plan

COIN Framework Participants 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. Amended effective 30.03.23

A.6 Recording of Security Events

Each COIN Framework Participant must accurately detect and record Security Events. Security Events must be accurately identified and reported according to the categories specified in A.3. Amended effective 30.03.23

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 Framework Participants fulfils the general obligations set out in clause A.2 above. Amended effective 30.03.23

(b) Security event logs must be actively monitored by each COIN Framework Participant. Amended effective 30.03.23

(c) Each COIN Framework Participant 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: Amended effective 30.03.23

(i) Regular follow-up of messages for security events. A COIN Framework Participant should implement automated techniques as an aid to timely incident detection and reporting and for alerting the other COIN Framework Participants about severe or persistently recurring events. Amended effective 30.03.23

(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 Framework Participants and the COIN Administrator, then, if necessary, to AusPayNet. Amended effective 30.03.23

(iv) Contact names, locations and phone numbers to be used in conjunction with the escalation procedures.

(d) Security Incidents involving one or more COIN Framework Participants must be
resolved by the parties involved. Security Incidents affecting a COIN Framework Participant need not be reported to other COIN Framework Participants or the COIN Administrator, provided the COIN Framework Participant fulfils the general obligations set out in clause A.2 above. Amended effective 30.03.23

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 Card-related financial messages the following fields of a financial transaction at a minimum, if present in a message, must be logged by the COIN Framework Participant:

Last Amended effective 30.03.23

(a) Message type;

(b) Truncated Primary Account Number;

(c) Transaction date and time;

(d) Originating AIIN;

(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 FRAMEWORK PARTICIPANT CERTIFICATION CHECKLIST

TO: COIN ADMINISTRATOR
AUSTRALIAN PAYMENTS NETWORK LIMITED ("**AusPayNet**")
LEVEL 23, TOWER 3, INTERNATIONAL TOWERS,
300 BARANGAROO AVENUE
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 Framework Participant confirms for the benefit of each other COIN Framework Participant and AusPayNet that it meets the technical, operational and security requirements applicable to COIN Framework Participants which are set out in Part 2 and 3 of the COIN Operating Manual as applicable;

- each COIN Framework Participant 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 Framework Participant and AusPayNet, that its system or enhancements to its system (as the case may be) meet all applicable technical, operational and security requirements for COIN Framework Participants as set out in the COIN Operating Manual; and

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

REQUIRED CAPABILITIES FOR COIN FRAMEWORK PARTICIPANTS

STANDARDS

Required Capabilities for COIN Framework Participant Certification *(Please complete all sections below)*	**Applicable Clause**

B.1 A comprehensive security policy exists and is in use for all Information Technology assets associated with, or connected to the COIN. — 2.1(a)

Yes	No	N/A

If N/A response: Reason ----------

B.2 Procedures exist and are in use that ensure all cryptographic key management complies with ISO 11568:2023 — 2.1(b)

Yes	No	N/A

If N/A response: Reason ----------

B.3 Procedures and policy governing cryptographic key sizes and algorithms protecting COIN data exist, are in use and comply with COIN requirements — 2.1(c)

Yes	No	N/A

If N/A response: Reason ----------

B.4 Procedures exist[1] and are used to detect and prevent unauthorised access — 2.2

Yes	No	N/A

If N/A response: Reason ----------

B.5 Policies and procedures[1] for an incident management system exist and comply with COIN requirements — 2.3

Yes	No	N/A

If N/A response: Reason ----------

B.6 The design of the Framework Participant's COIN network meets the COIN network separation requirements. — 3.6

Yes	No	N/A

If N/A response: Reason ----------

B.7 [Deleted] — Deleted effective 01.01.23

B.8 The design and management of any host system used for the carriage and/or processing of COIN traffic meets COIN requirements. 2.9

Yes	No	N/A

If N/A response: Reason

OPERATING RULES

B.9 All COIN connections, regardless of whether they are inactive, redundant or backup connections, have been tested and verified at least annually to prove that they function correctly (i.e. end to end acknowledged traffic between Framework Participant's Hosts, e.g. Telnet test)). Connections that are regularly used for normal production processing (e.g. in an active-active configuration) do not require any additional verification. 3.1

Yes	No	N/A

If N/A response: Reason

B.10 Procedures exist and are followed to monitor COIN communications traffic and ensure that sufficient bandwidth is available to meet COIN requirements. 3.4

Yes	No	N/A

If N/A response: Reason

B.11 The design and implementation of the Framework Participant's COIN network provides Quality of Service features that comply with COIN requirements. 3.5

Yes	No	N/A

If N/A response: Reason

B.12 A separate test environment between institutions exists over the COIN and its design ensures that the COIN separation requirements are met. 3.6

Yes	No	N/A

If N/A response: Reason

B.13 Policy and procedures[1] exist and are in use for a security event management system that it complies with COIN requirements. 3.8

Yes	No	N/A

If N/A response: Reason

TRIENNIAL PSS EXCHANGES (EXISTING FRAMEWORK PARTICIPANTS ONLY)

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 Framework Participants 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 AusPayNet;

(c) agrees that if the Applicant is granted Certification, in consideration of such Certification, to:

(i) immediately notify AusPayNet 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 AusPayNet 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[1] 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.

[1] 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 FRAMEWORK PARTICIPANT CONTACT LIST

Details of a COIN Framework Participant's operational support and Custodial contact details may be found on the AusPayNet Extranet https://extranet.auspaynet.com.au/.

ANNEX D BATNA FOR FINANCIAL TRANSACTIONS: FRAMEWORK PARTICIPANT-TO-FRAMEWORK PARTICIPANT VPN TUNNELS

Note:

- This Annexure only applies when Communicating COIN Framework Participants invoke it as the best alternative to a negotiated agreement (BATNA), to implement VPN tunnels over and above the requirements of the COIN.

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 Framework Participant'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 Framework Participant's security policy;

h) the minimum Diffie-Hellman MODP group size is 1536-bits;

i) IPSec Security Association lifetimes must not exceed 24 hours; and

j) IKE, if used, must be configured to only use main mode, specifically aggressive mode must NOT be used.

ANNEX E BATNA FOR FILE TRANSFER: CONNECT:DIRECT SECURE PLUS

CONFIGURING THE APPLICATION

Note: cipher suite references refer to specific cipher suites or their direct equivalent.

1. SSL or TLS option must be set to TLS, and the system must be configured to use TLS1.2 at a minimum.

2. The list of supported cipher suites MUST include TLS_RSA_WITH_AES_256_GCM_SHA384 within the Sterling product in use at each organisation.

3. The following cipher suite settings are acceptable for use in preference to RSA_WITH_AES_256_GCM_SHA384 where both participants agree and are able to generate the required certificates.
    a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

4. Cipher suites must NOT be enabled that:
    a. Permit use of AES_128
    b. Permit use of CBC cipher mode
    c. Permit use of DES, 3DES or DES40
    d. Permit use of Null ciphers
    e. Permit use of hash algorithms weaker than SHA256 such as SHA or MD5
    f. Permit use of RC4 cipher
    g. Permit use of ‘export’ strength ciphers

CERTIFICATE REQUIREMENTS

5. RSA-based certificates must have a minimum key size of 2048 bits.

6. In certificates, a Diffie-Hellman key length setting of 2048 bits or higher is preferred, with 1024 bits to be accepted only where platform limitations prevent use of the higher setting.

7. If Elliptic Curve (EC) cryptography is used, the minimum EC key length should be secp256r1. secp384r1 is also acceptable and preferred.

8. TLS certificates must be signed with a SHA2, SHA256 or SHA384 hash or better

9. The option to verify certificate common names (CN) must be enabled and configured with the correct CNs.
    a. How does this get implemented? Differs from component to component. Any doco on server certificates?

10. Certificates must be signed by a public certificate authority (CA). Participants must notify counterparts of their preferred certifying authority. Each participant is responsible for acquiring the relevant CA certificates and maintaining current, valid CA certificate versions in their own trust stores.

11. Certificates other than the CA certificates (i.e. server and client certificates) must have a maximum lifespan of approximately one year. Each Framework Participant is responsible for the life cycle of their own certificates. Each Framework Participant should have a mechanism in place to track the expiry date(s), and to renew the certificate(s) well in advance of expiry.

ENFORCING USAGE

12. Usage must be configured to
    a. ensure data confidentiality and
    b. require mutual authentication.