Process for Considering Non-Standard Technologies at the Point of Interaction

September 2017

Version 1.3a

Company Confidential

Written and published in Sydney, Australia by Australian Payments Network Limited

Amendment Certificate

Version	Date	Author/Comments
0.4	*June 2015*	*Draft for IAF approval*
1.1	*June 2015*	*Version approved by IAF on 9 June 2015 subject to amendments included here.*
1.2	*January 2017*	*Revised to provide a single process for device review*
1.2	*February 2017*	*Include AusPayNet Management comments*
	7 March 2017	*IAF approved*
1.3	*26 June 2017*	*IAF approved inclusion of Principles for Liability Shift for pilots.*
1.3a	*September 2017*	*This document has been updated to reflect the change from APCA to AusPayNet*

Table of Contents

PART 1 INTRODUCTION

1.1 Background

The card payment system is seeing a surge in new products and services due to the rapid changes in available technology and the growing number of organisations entering the payments market. Many of these innovations fit within existing standards; however, some proposed solutions employ a different paradigm for protecting payments information.

The process for considering non-standard technologies at Point of Interaction (POI) has been established in order to:

1. allow and encourage innovation;
2. quickly address emerging technologies while limiting the potential for fraud; and

act as an industry and avoid potential inconsistencies from card schemes acting individually

1.2 Purpose of this document

This document provides a description of the process for reviewing and approving non-standard technologies at Point of Interaction (POI).

1.3 Scope

This document supports the consideration of POI 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.

A proposed POI solution / technology will be considered under this process if it would normally be required to meet any of the following Australian or global payment standards but, by nature of its design, is unable to do so:

i) PCI PTS,
ii) PCI DSS,
iii) IAC requirements for PIN Entry Devices (IAC Code Volume 3 - Acquirers Code); and
iv) EMV.
v)

Excluded from scope is any solution / technology that:

a) is not intended for use at POI,
b) is expected to be able to meet each of the standards listed above (where required) but has not yet completed the certification process; or
c) is a closed loop system.

1.4 Review of the process

The IAF will review the process for considering non-standard technologies at Point of Interaction from time to time and at least every two years.

PART 2 HIGH LEVEL PROCESS

2.1 Stages for assessing non-standard technologies at POI

The high level joint industry process for assessing non-standard technology at POI is made up of 6 stages as follows:

1. Request Phase
    a. Request for consideration of a non-standard technology by an acquirer or the IAF
2. Identification Phase
    a. Identification of existing applicable or partially applicable standards and academic research
    b. Identification of laboratories best matched for testing the non-standard technology
    c. Identification of subject matter experts
3. Technical Examination Phase
    a. Review of the device by selected laboratories
4. Assessment Phase
    a. Review of reports and assessment by an expanded ERSC, including scheme participants and subject matter experts
    b. Development of a high-level risk assessment by the expanded ERSC
    c. Development of a pass/fail/pilot decision by the expanded ERSC
5. Pilot Phase
    a. A controlled pilot with strictly defined parameters including number of devices and merchant is permitted and subject to close monitoring by the SCC.
6. Decision Phase

Development of a pass/fail decision by the expanded ERSC

2.2 Timing

The goal is to complete the Assessment within approximately 6 months from the time the Sponsor first approaches Australian Payments Network Limited (AusPayNet) Management with a request for consideration. However, the actual timing will depend largely on the complexity of the solution, the quality of documentation received from the Sponsor, the workload of the selected laboratories and the level of support from card schemes.

2.3 Request for consideration

Figure 1 below highlights the steps of the request for consideration stage:

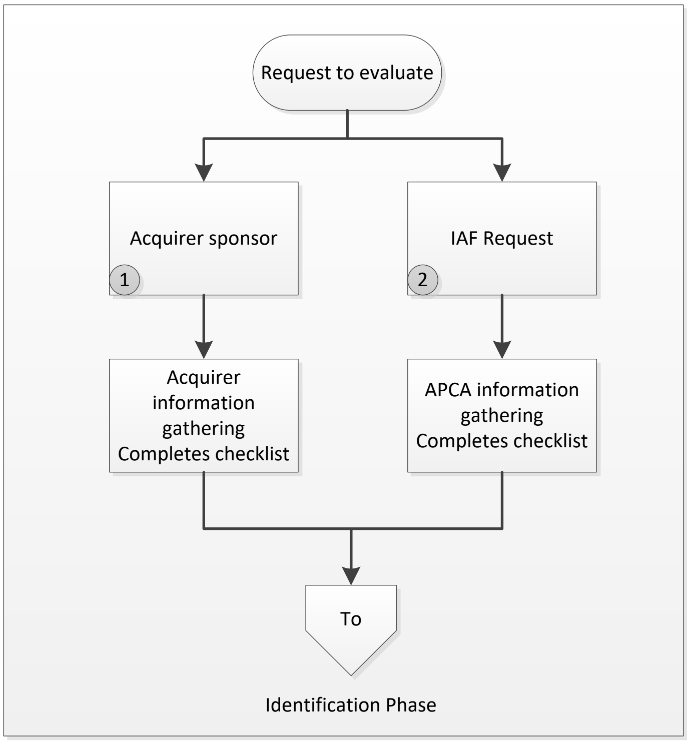
Request to evaluate
Acquirer sponsor
1
IAF Request
2
Acquirer information gathering Completes checklist
APCA information gathering Completes checklist
To
Identification Phase

Figure 1 - Request Phase

1- A request for considering a non-standard technology evaluation is made to AusPayNet by the acquirer who wishes to use the device or technology (the Sponsor)[1].

2- Alternatively, the IAF may request that a non-standard technology be considered for assessment if they believe it to be beneficial to the Australian Card Payments industry as a whole.

3- The standard checklist to be completed by the Sponsor (or AusPayNet Management if the IAF is the Sponsor) contains information about the proposed technology (Annexure A - Initial assessment checklist).

Note: As part of the initial request, the Sponsor agrees to accept the external costs associated with the device evaluation. These costs usually need to cover technical security consulting, system testing by a specialised testing company, plus travel costs for members to attend meetings.[2] If the IAF requests that a technology should be assessed, then the costs associated with the process will be covered through AusPayNet's normal budgetary process.

[1]- A primary Sponsor should be nominated if a solution has more than one acquirer.
[2]- An estimate of the expected costs will be advised to the Sponsor before any decision is made to spend the money.

The Sponsor also agrees that the Vendor is prepared to make the solution itself available to the lab for testing as part of the Industry Analysis.

2.4 Identification Phase

Figure 2 below highlights the steps of the identification phase

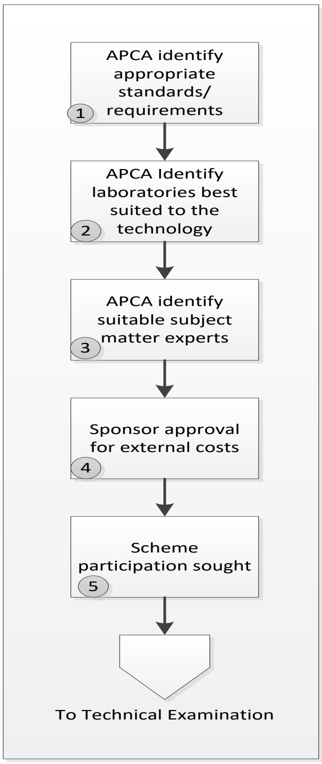
APCA identify appropriate standards/ requirements
1
APCA Identify laboratories best suited to the technology
2
APCA identify suitable subject matter experts
3
Sponsor approval for external costs
4
Scheme participation sought
5
To Technical Examination

Figure 2 - Identification Phase

1- AusPayNet Management will initially review the Initial Assessment checklist and obtain the views of the card schemes with regards to the technology under consideration. AusPayNet Management will then identify any possible existing standards including partial or draft standards or requirements applicable to the technology involved. This research must also examine the current state of academic research in the technology being considered.

2- AusPayNet Management will identify any laboratories, not necessarily approved evaluation facilities, with particular knowledge and/or skills in testing the technology involved.

3- AusPayNet Management will identify any subject matter experts willing to assist on the evaluation of the technology and estimate likely costs. Any consultants likely to be engaged must be willing to agree to the ERSC requirements for confidentiality.

4- AusPayNet Management will advise the sponsor of the selected laboratory (more than one laboratory is possible) and the likely estimate of external costs and obtain the sponsors agreement to bear those costs.

5- Having gained the sponsor's approval for bearing the costs involved, AusPayNet Management will approach the schemes requesting nominations for experts to attend and assist in the evaluation of the technology.

Prior to completing the Identification phase, contractual arrangements need to be put in place, including:

a. Consent from the Vendor to authorise AusPayNet to access documents / personnel / premises as required by the scope of the assessment; and

b. A confidentiality undertaking between AusPayNet and the Sponsor / Vendor and any Subject Matter Experts.

2.5 Technical Examination Phase

Figure 3 below highlights the steps of the technical examination phase:

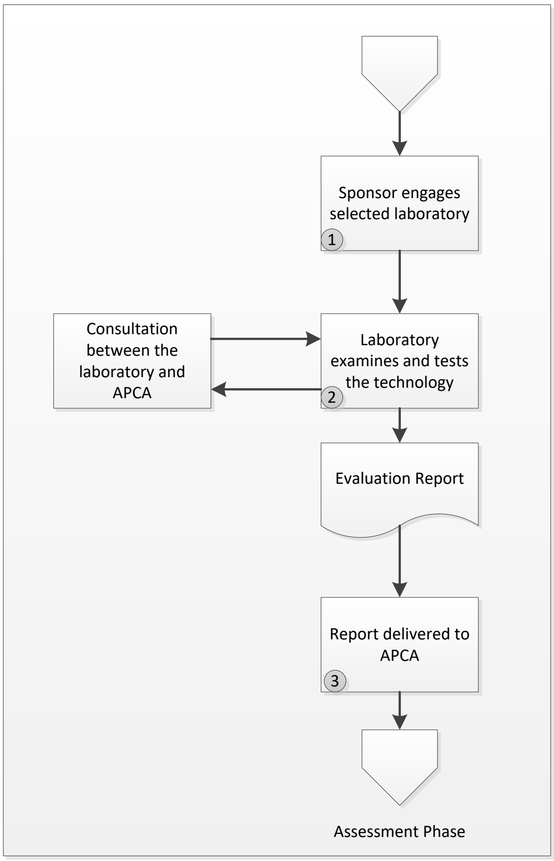
Sponsor engages selected laboratory
1
Consultation between the laboratory and APCA
Laboratory examines and tests the technology
2
Evaluation Report
Report delivered to APCA
3
Assessment Phase

Figure 3 - Technical Examination

1. – The sponsor or vendor will engage the identified laboratory or laboratories if so advised and arrange for a review with the output report to be provided to AusPayNet. This engagement should permit that an ongoing dialogue between the laboratory and AusPayNet Management to ensure that desired outcomes are met.

2. The laboratory will examine and test the device against standards and requirements as advised by AusPayNet and its own knowledge and skill set.

    a. The lab carries out the technical review / penetration testing[3] for any identified risks and writes a draft report including:

        i. Highlighting the risks and the effectiveness of any relevant mitigation measures in place; and

        ii. Areas of uncertainty and why they are not able to provide a clear statement.

3. The laboratory will provide the report to AusPayNet and the sponsor/vendor if required.

[3]- The card schemes may also choose to do their own testing in addition to the industry testing.

a. Card schemes may carry out their own testing / analysis and provide the ERSC with any additional risks that they consider as relevant for the solution under consideration

2.6 Assessment Phase

Figure 4 below highlights the steps of the assessment phase:

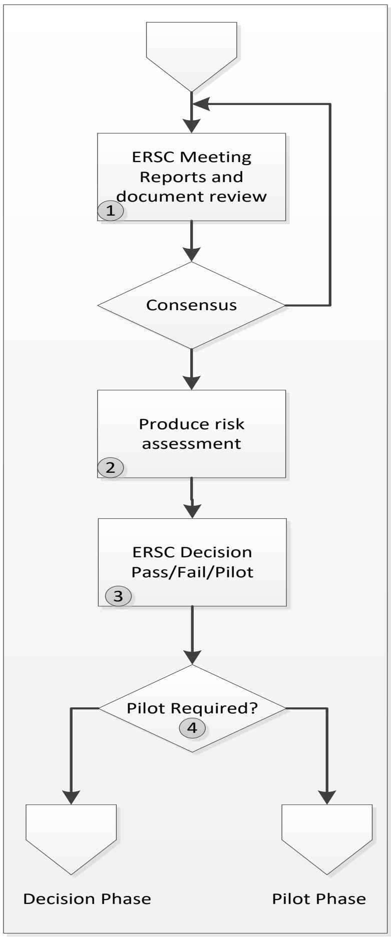

Figure 4 - Assessment phase

1. AusPayNet convenes a meeting of the expanded ERSC including nominated experts from the schemes and the attendance of any nominated subject matter experts to review the laboratory's findings and other relevant documentation. A maximum of three meetings of the ERSC may occur if more information is required; if consensus cannot be reached, the non-consensus ERSC process (in the ERSC TOR) will be adopted.

2. The ERSC produces a high level risk assessment of the device.

   a. In order to facilitate the Risk Analysis, the Sponsor / Vendor should provide any available technical documentation and / or results from previous testing, including relevant testing carried out by the card schemes in Australia or internationally to the ERSC.

   b. The Risk Analysis will:

      - Assess the solution against the current standards to confirm and potentially identify which requirements of the current standards are not met;

- Identify potential threats and risks to the payment system arising from the gaps to the current standards;
- Assess the controls applied by the Vendor against these potential threats and risks to the payment system;
- Assess the residual threats and risks to the payment system based on the combination of the potential threats and risks identified and the controls applied.

3. The ERSC produces a pass/fail decision in conjunction with the risk assessment.
4. The ERSC decide if a Pilot Phase is required and determine appropriate criteria.

2.7 Pilot Phase

If a pilot is recommended by the ERSC, it can be run in line with pre-determined criteria[4] and the following assumptions:

1. All agreed criteria are applicable to the Sponsor, not the solution provider,
2. The Sponsor should report on performance against criteria at a pre-determined frequency,
3. Anything that the ERSC considers as having an impact on the suitability of the new technology whilst the pilot is running will be part of the considerations when running and assessing a pilot,
4. The criteria may be amended by the ERSC during the course of the pilot, although this should be a rare occurrence,
5. Card schemes may withdraw from a pilot at any time at their own discretion if it is deemed that the pilot will create a liability or risk to their issuers, their brands or network,
6. The Sponsor shall accept all liability and / or costs arising from the use of the solution and the pilot, which includes, but is not limited to, all chargebacks or losses that may arise from fraud or the data integrity of the solution; and
7. The Sponsor has the financial reserves to withstand the magnitude of liability described above.

Note it is acknowledged that a pilot, in and of itself, cannot be used to test whether a solution is secure.

During the course of the pilot, the Sponsor collects the data and provides it to AusPayNet Management in line with the agreed criteria. AusPayNet Management then reports to the ERSC on the performance of the pilot. Card schemes receive the data in relation to their pre-determined individual criteria from the Sponsor directly.

The data provided by the Sponsor is assessed by AusPayNet Management against the pre-defined criteria as determined by the ERSC.

If significant issues are identified during the course of the pilot it can be shut down prior to completion by the Sponsor, the Vendor or the ERSC.

2.8 Decision Phase

[4] Such criteria (including success criteria) would be agreed with the Sponsor and card schemes. Annexure B contains high level criteria for a pilot. The criteria for the pilot shall be strong enough to provide comfort to the industry that the technology is acceptable

This phase returns to the normal ERSC process, AusPayNet reconvene the ERSC meeting who review whether the criteria for the pilot have been met within the timeframe, and determine if the technology is suitable for broader rollout, and if a phased or full rollout is appropriate, thus passing or failing the device accordingly. Using standard ERSC processes AusPayNet Management will notify the

sponsor of the outcome of the approval process and if approved add the device to the list of approved devices.

ANNEXURES

ANNEXURE A INITIAL ASSESSMENT CHECKLIST

The initial assessment checklist should be completed by the Sponsor to request consideration for a non-standard technology at Point of Interaction and provided to AusPayNet Management in line with the process for consideration document.

1.	Date of submission: …../……/…..
2.	Name of the Sponsor (acquirer)
3.	Name of the Vendor (technology provider)
4.	Name of the non-standard technology for consideration
5.	Software / hardware / firmware version numbers
6.	Provide details around the current and expected use of the technology
7.	Level of support from card schemes and names of contacts in Australia:
8.	Information on markets where it is already running, for how long and the experience so far:
9.	Incremental and economic benefits the solution delivers to stakeholders that existing solutions don't:
10.	Description of the non-standard technology, including details around the equipment used, the security process and procedures used to manage the equipment and information about the system architecture where applicable
11.	What is required for merchants and/or other issuers and acquirer to adopt the solution?
12.	Other technology that is relied upon to support the solution (e.g. mobile phone):
13.	List (non-exhaustive) of standards that devices would be expected to be assessed against:
14.	Details of the gap between the existing standard requirements and the new technology (why doesn't it comply with existing standard?)
15.	Perceived risks of the non-standard technology and how can they be mitigated (impact on payment ecosystem):
16.	How the sponsor intends to mitigate the risks
17.	Evidence of any relevant certifications already obtained, failed or in progress
18.	Provide details of any previous independent testing that may have already been carried out:
19.	Provide information (if available) on whether any process is already underway internationally or within Australia to establish new relevant standards
20.	If a pilot is proposed, details of any existing plans for pilot including merchant base, numbers and target date for initiating the pilot
21.	Any additional comments to be considered that the Sponsor deems relevant:

ANNEXURE B HIGH LEVEL CRITERIA FOR PILOT

Once the ERSC has agreed that the technology under consideration is appropriate for pilot, it will meet with the card schemes and agree on the industry criteria for pilot. It is important that the criteria for pilot are strong enough to provide comfort to the industry that the technology is acceptable for launch on the Australian market at the end of the pilot. This is because the expectation would be that if all the criteria for pilot are met within the timeframe, then the next step will be a phased or full rollout (depending on the size of the pilot).

Criteria for pilot include:

- Length of pilot (including tentative start and end dates)
- Pilot phases
- Frequency and content of reporting
- Restriction to specific states and/or concentration requirements
- Transaction types
- Eligible merchants (include anticipated number)
- Eligible devices
- Eligible cards
- Minimum number of transactions that need to be going through to consider that the technology was sufficiently tested
- % of active users that continue to use the solution throughout the pilot
- Industry mix of merchants
- Compliance and fraud limits
- Communication (or no communication) to merchants and card holders about the risks of the technology they are piloting
- Broader communication plan for before, during and after the pilot is being run.
- Merchant training
- Fraud rate
- Surveys to users (merchant and card holders) on how comfortable they are in using the solution
- Social media response
- Any additional security testing to be done whilst the pilot is running
- Progress through relevant standards bodies or similar
- The Sponsor has the financial reserves to withstand the magnitude of liability inherent to the risk of running the pilot

Each of the criteria will be assigned a success measure for the Sponsor and the ERSC to track during the course and at the completion of the pilot.

Note: the card schemes may separately impose their own requirements to the Sponsor.

Principles for Liability Shift

- A Sponsor is responsible for card losses incurred by an Issuer, where such losses arise from the compromise of PIN and/or card data caused by the Sponsor’s use of a non-standard POI technology in an approved IAC pilot during the pilot and for 2 years after the conclusion of the pilot.
- The definition of losses will be limited to chargebacks and chargeback fees associated with fraudulent use of PIN and/or card data, and costs associated with re-issuing Cards.
- Upon an Issuer identifying that the PIN and/or card data associated with the cards of two or more Issuers have been compromised at a pilot device (or group of pilot devices), the Issuer must immediately advise the Sponsor of the pilot and AusPayNet in writing.

- The standard of proof for all matters related to the pilot shall be on the balance of probabilities.
- Parties to any cost dispute shall attempt to resolve it by negotiating in good faith bilaterally prior to seeking to use AusPaynet's dispute resolution process (to be developed).