DEVICE APPROVAL PROCESS

Annexure G to IAC Code Set Volume 4

G.1 Introduction

G.1.1 Operation

This document sets out Australian Payments Network Limited's ('**the Company's**') process for device approval applications and the requirements for Device Approval Applicants and Approved Evaluation Facilities. The document operates as follows:

(a) It does not form an operative provision of the IAC Code Set.

(b) By submitting a device approval application or a delta approval application, a Device Approval Applicant agrees to comply with the applicable terms of this document.

(c) By applying to become an Approved Evaluation Facility, the evaluation facility agrees to comply with applicable terms of this document.

G.1.2 Interpretation

(a) The words defined in Part 1.3 of the IAC Code Set Volume 4 have the same meaning in this document unless a contrary intention appears.

(b) In this document, 'device approval application' and related 'device' and 'SCD' references include, when necessary and relevant, 'SPoC solution', 'SPoC solution approval application' and related 'SPoC solution' references.

G.1.3 Purpose

Part 1.1 of IAC Code Set Volume 4 states that the purpose of the IAC is to provide framework for participants in card payments in Australia to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. In the context of device approvals, that purpose includes balancing the interest of maintaining the security and integrity of Australian Card Payments with the interest of promoting innovation and competition.

G.2 Device approval criteria

The following are factors which the Company must consider in determining a device approval application under Part 3.1 of IAC Code Set Volume 4:

(a) the Evaluation Report, including the results of the testing process;

(b) the Device Security Standards in Part 2 of IAC Code Set Volume 4 as required under Part 3; and

(c) in relation to a device containing non-standard technologies, also:

(i) any criteria referenced in Schedule 1 'Process for Considering Non-Standard Technologies at the Point of Interaction' (NST Process), as updated from time to time;

(ii) any other criteria agreed upon by the Company and Device Approval Applicant.

G.3 Approved Evaluation Facilities

G.3.1 Introduction

This Part G.3 documents the process for accreditation by the Company to perform Secure Cryptographic Device (SCD) security testing. The following clauses identify the requirements a prospective Approved Evaluation Facility ("a Test Laboratory") must meet in order to qualify for accreditation by the Company for conducting device evaluations to the IAC security requirements.

G.3.2 Initiation

Test Laboratories applying for accreditation as Approved Evaluation Facilities should initiate the process by contacting the Senior Manager Operations, AusPayNet. To minimise the associated time frames, Test Laboratories should submit all required materials and evidentiary matter in a single package. Subsequent to the receipt by the Company of all prerequisite materials, a minimum of six weeks is required for processing. Where required, testing of device artefacts may result in more extended time frames.

G.3.3 Accreditation Process

(a) To gain accreditation for SCD security testing, the Test Laboratory must successfully complete the Company's Evaluation Facility accreditation process described below. The accreditation process has three components:

(i) Business Review;

(ii) Technical Review;

(iii) On-site Visit.

(b) The Company may require, at its sole discretion, that an Approved Evaluation Facility provide evidence of its continued compliance with the accreditation process requirements triennially.

(c) Once a Test Laboratory has been approved by the Company to perform SCD security testing, it will be listed on the AusPayNet website as an Approved Evaluation Facility, and it can offer its services to Device Approval Applicants. The Approved Evaluation Facility must perform testing as described in the following documents:

(i) AS 2805.14.1 Secure Cryptographic Devices, concepts, requirements and evaluation methods;

(ii) AS 2805.14.2 Secure Cryptographic Devices – Security Compliance Checklists; and

(iii) Code Set Volume 4 Part 2 – Device Security Standards

G.3.4 Business Review

The Test Laboratory must complete a business review with the Company. This review requires that the Test Laboratory meet a minimum required standard acceptable to the Company for conducting business with the highest ethical standards. The business review covers areas including, but not limited to, Due Diligence and Independence.

G.3.4.1 Due Diligence

Establishes the potential business relationship with the Company and its Members, the nature of services to be provided, a review of the last two years financial statements and a background check on the key executives within the organisation. The purpose of this review is to provide the Company with a clear understanding of the Test Laboratory's capabilities and business practices.

G.3.4.2 Independence

(a) The Test Laboratory must demonstrate its independence from any SCD manufacturer or vendor.

(i) The Test Laboratory must not be owned in whole or in part by any SCD manufacturer or vendor.

(ii) Evaluations will not be accepted from any Approved Evaluation Facility if the customer whose products being evaluated represent more than 10% of the facility's prior two years annual revenue.

(b) The Test Laboratory must be able to demonstrate its independence of its review. Evaluations will not be accepted from an Approved Evaluation Facility where the AEF designed the product being evaluated or was involved in its design.

G.3.5 Technical Review

The Test Laboratory must complete a due diligence technical review with the Company. This review requires that the Test Laboratory meet certain minimum technical requirements set forth by the Company. The technical review covers areas such as Laboratory Accreditation, Personnel Requirements, Equipment Requirements, Reference Library and Demonstrated Ability.

G.3.5.1 Laboratory Accreditation Checklist

(a) The Test Laboratory must complete and submit the IAC Laboratory Accreditation Checklist (Volume 4- Annexure E). This material addresses such areas as:

(i) Organisation and Management;

(ii) Quality Assurance function;

(iii) Skill sets of personnel;

(iv) Adequacy of the facilities;

(v) Appropriateness of equipment and reference materials;

(vi) Equipment and software configuration management;

(vii) Testing methodologies employed;

(viii) Records management; and

(ix) Qualities of reports issued.

(b) In addition, the Test Laboratory must specifically provide the information in clauses G.3.5.2 to G.3.5.6.

G.3.5.2 Accreditations and Certifications

(a) The Test Laboratory must provide current evidence of all accreditations claimed. These may include accreditation under the relevant national implementation of AS ISO/IEC 17025 (Criteria for the competence of testing and calibration laboratories), AS/NZS ISO 9000 (Quality management systems), AS ISO/IEC 15408 series (Common Criteria for IT security evaluations) or other similar international, national, or industry standards.

(b) The Test Laboratory must also provide evidence of sponsorship or endorsement by a recognized payment scheme engaged in the processing of PIN Transactions (either a global payment scheme or a multi-Member national debit network/network). The sponsorship or endorsement must include the testing of cryptographic devices to a prescribed set of security requirements.

G.3.5.3 Personnel Requirements

The Test Laboratory must provide a listing of personnel who will work on evaluations submitted for the Company's consideration, along with their qualifications. Qualifications should include formal and informal training, length and type of experience in doing related evaluation work. The list should include their specific role(s) in the evaluation process. This listing should be updated annually and must be made available to the Company upon request.

G.3.5.4 Equipment Requirements

The Test Laboratory must provide a listing of the relevant "standard" test equipment that is owned by the Test Laboratory, and any relevant "specialised" test equipment that is owned by the Test Laboratory or available for rent or contract service.

G.3.5.5 Reference Library

The Test Laboratory must provide a listing of reference materials that are resident at the Test Laboratory. Reference materials should include, but not be limited to, books, articles and proceedings that relate to the testing of cryptographic devices (e.g., cryptography, threats and attacks, etc.). Reference materials should also include industry standards and specifications for testing cryptographic devices (e.g., ISO and National Standards).

G.3.5.6 Demonstrated Ability

(a) The Test Laboratory must provide a test report for a cryptographic device completed by the Test Laboratory within twelve months of the application for accreditation. The test report must document the results of a security evaluation of a cryptographic device, preferably a PIN Entry Device. The test report submitted must be current, and demonstrate the Test Laboratory's ability to assess the cryptographic device against a defined set of security characteristics and assess the device's overall strengths and vulnerabilities from a physical and logical security perspective. This must be accompanied by documentation of the relevant standards and requirements that form the basis for the evaluation.

(b) The Company requires that the test report be accompanied by a letter of permission signed by the applicant for the evaluation. The letter of permission must state that the applicant permits the test report to be reviewed by the Company, and kept by the Company for its records.

(c) The Company may also require the Test Laboratory to examine a test artefact (PED) with one or more features that are not in compliance with the IAC SCD Security Requirements. The Test Laboratory must discover the nonconformities, document them, and indicate which IAC SCD Security Requirements have failed due to the presence of the nonconformities. The Test Laboratory must bear the costs of this process and, in addition, compensate the Company for the costs of completing a concurrent evaluation of the same device via an Approved Evaluation Facility.

G.3.6 On Site Visit

The Company, or a third party acting on behalf of the Company, may visit the Test Laboratory. The purpose of the visit is twofold:

(a) to inspect the Test Laboratory and validate that the Test Laboratory is in compliance with the documentation provided to the Company under clauses G.3.4 and G.3.5; and

(b) to discuss security-testing issues with the Test Laboratory's staff.

G.3.7 Other Accreditations

The Company may, at its sole discretion, accept existing accreditations with other bodies, as meeting part or all of the accreditation process requirements of this Part G.3.

G.4 Process for Standard Technology Device Approvals

This part sets out the device approval process for standard technologies. Device Approval Applicants (when submitting a device approval application) and AEFs (when preparing and submitting an Evaluation Report) must also follow the requirements in Annexure C 'Device Evaluation FAQs' to the IAC Code Set Volume 4.

G.4.1 Engagement to AEF to produce Evaluation Report

(a) The AEF and Device Approval Applicant must directly enter into a contract and any necessary non-disclosure agreements for the conduct of all testing to be carried out under clause G.4.2. If a device is submitted for examination under clause G.4.2(d) such contract must authorise the disclosure of any relevant PCI Evaluation Report by the AEF to the Company.

(b) The costs and expenses incurred in securing approval for a device are the responsibility of the relevant Device Approval Applicant. The Company may levy a fee to cover its reasonable costs (if any) in supporting the evaluation of any particular device.

(c) Documents to be provided by Device Approval Applicant to AEF:

Rules and guidance for privacy shielding using the external physical environment must be provided to the Approved Evaluation Facility, for evaluation.

G.4.2 AEF review and preparation of Evaluation Report

(a) The AEF must evaluate and consider the compliance of the device with the standards at Part 2 and Part 3.1 of Code Set Volume 4.

(b) Only those checklists appropriate to the characteristics and function of the device must be evaluated. In addition to these checklists the AEF must use such additional tests as its knowledge and experience dictate.

(c) The Evaluation Report must contain:

(i) the list of all pertinent documentation used in the evaluation;

(ii) a completed list of all successful or failed tests;

(iii) the name of the Device Approval Applicant;

(iv) the name of the AEF;

(v) the date of the evaluation;

(vi) identification of the device (model name, hardware version, firmware version and application version);

(vii) completed SCD checklists;

(viii) advised deployment environment (as advised by the Applicant);

(ix) details of the examination and testing process followed in developing the report; and

(x) if the examination is conducted pursuant to clause G.4.2(d), a copy of the PCI Evaluation Report and PCI Plus Evaluation report.

(d) Where conducting a PCI Plus evaluation, the AEF must submit:

(i) a PCI Evaluation Report; and

(ii) a PCI Plus Evaluation Report, which must explicitly state whether or not the device complies with the Company's feasibility requirements set out herein;

to the Company in support of the Device Approval Applicant's application for approval of such device under the IAC Code Set.

(e) The AEF must submit a copy of the Evaluation Report and any relevant PCI Evaluation Reports (if applicable), directly to the Company.

(f) The Device Approval Applicant must arrange with the AEF consent release forms so that it has permission to release the PCI Evaluation Report to the Company.

G.4.3 Company review of device approval application

(a) The Company will review the device approval application in accordance with the device approval criteria at Part G.2 of this document.

(b) If the Company cannot determine a device approval application for reasons of incomplete or inadequate documentation, the Company will request further clarification and/or documentation from the Device Approval Applicant and/or AEF.

(c) The Company will endeavour to complete its review and issue its decision on the device approval application, within 6 weeks of receiving the Evaluation Report. Matters which can increase the time it takes the Company to issue its decision include:

(i) whether the Company has further requests for information of the Approved Evaluation Facility and/or Device Approval Applicant, and if so, the speed with which appropriate responses are provided to the Company; and

(ii) whether the device contains new technology.

(d) The Company will determine whether to approve a device in accordance with Part G.8 of this document, and if so, whether any conditions should be attached to the approval.

G.5 Process for Non-Standard Technology Device Approvals

(a) The process for non-standard technology device approvals is described in 'Process for Considering Non-Standard Technologies at the Point of Interaction' (NST Process), which is Schedule 1 to this document.

(b) The Company will review the device approval application in accordance with the device approval criteria at Part G.2 of this document.

(c) The Company will determine whether to approve a device in accordance with Part G.8 of this document.

G.6 Delta approval of an approved device

(a) Where there are proposed changes to the device software and/or minor hardware modifications to an Approved Device, the Device Approval Applicant must apply to the Company for delta approval of the Approved Device.

(b) To apply for delta approval, the Device Approval Applicant must follow the Process for Standard Technology Device Approvals in Part G.4 of this document, save that the Evaluation Report need only address the software and/or minor hardware modifications to the approved device.

(c) The Company will review the delta approval application in accordance with the device approval criteria at Part G.2 of this document.

(d) The Company will determine whether to approve a device in accordance with Part G.8 of this document, and if so, whether any conditions should be attached to the approval.

G.7 Term of Device Approval

(a) Devices will be approved by the Company for the Approval Period contained at Part 3.2(c) of IAC Code Set Volume 4, being three years from the date of the Letter of Approval.

(b) Pursuant to Part 3.2(d) of IAC Code Set Volume 4, at the conclusion of the Approval Period, the Company may, at its sole discretion, extend the Approval Period for a further period of three years or such other period as it deems appropriate, having regard to changes in security technology, applicable standards, security threats and/or other knowledge in the security industry.

(c) Device approvals may only be revoked by the Company prior to the expiry of the Approval Period in accordance with Part 3.2(e) of IAC Code Set Volume 4, being if the Company determines that the device should no longer be approved because the device:

(i) no longer meets the applicable standards; or

(ii) approval of the device has been withdrawn or revoked by any other relevant security standards body; or

(iii) the device is vulnerable to a significant security threat which did not exist or was not apparent at the time the device approval was granted.

G.8 Decisions on device approval application

(a) Approval

In accordance with Part 3.2(a) of IAC Code Set Volume 4, if the Company approves a device (including delta approvals), the Company will issue a Letter of Approval to the Device Approval Applicant. The Letter of Approval will state any conditions which are attached to the approval.

(b) Decline

In accordance with Part 3.2(b) of IAC Code Set Volume 4, if the Company declines to approve a device, the Company must notify the Device Approval Applicant in writing of the reasons for its decision, including the details of the unacceptable results.

(c) Delay

If the Company requests further information pursuant to clause G.4.3(b) of this document, and the Device Approval Applicant or AEF does not respond within two calendar months of the request, then the Company may decline the device approval application.

(d) Revocation

If the Company decides to revoke device approval prior to expiry of the Approval Period, in accordance with Part 3.2(e) of IAC Code Set Volume 4, the Company must notify the Device Approval Applicant in writing of the reasons for its decision.

(e) Re-certification

If the Company requires the re-certification of a device in accordance with Part 3.2(g) of IAC Code Set Volume 4, the Company must notify the Device Approval Applicant in writing of the reasons for its decision.

G.9 Review

(a) The Device Approval Applicant may request review of a Company decision issued in accordance with Part G.8 of this document.

(b) Any request for review must be made to the Company, in writing, within 30 days of the Company's notification to the Device Approval Applicant. The request must properly detail the reasons for the requested review, including by reference to the Company's reasons for its decision.

(c) The Company must review and respond in writing to the request for review within a reasonable time depending upon the subject matter of the review request. If, following the review, the Company approves a device, the Part G.8 of this document will apply.

SCHEDULE 1 PROCESS FOR CONSIDERING NON-STANDARD TECHNOLOGIES AT THE POINT OF INTERACTION

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 the device security standards in Part 2 of IAC Code Set Volume 4; 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

3. 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.

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

1.1 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 AusPayNet

    b) Development of a high level risk assessment by AusPayNet

    c) Development of a pass/fail/pilot decision by AusPayNet

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 Company.

6. Decision Phase

   a) Development of a pass/fail decision by AusPayNet.

1.2 Timing

The goal is to complete the Assessment within approximately 6 months from the time the Device Approval Applicant first approaches 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 Device Approval Applicant, the workload of the selected laboratories and the level of support from card schemes.

1.3 Request for consideration

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

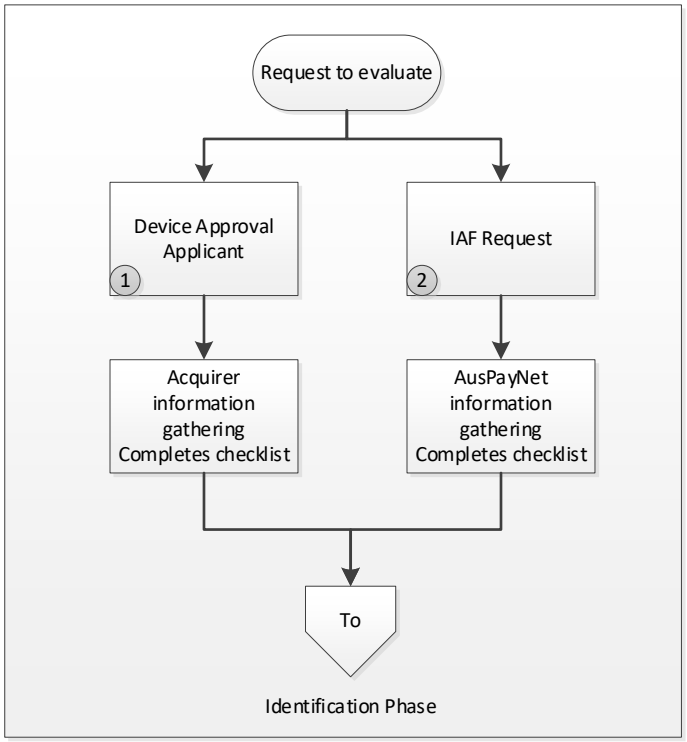

Figure 1 – Request Phase

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 Device Approval Applicant)[1].

[1]- A primary Device Approval Applicant should be nominated if a solution has more than one acquirer.

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 Device Approval Applicant (or AusPayNet if the IAF is the Device Approval Applicant) contains information about the proposed technology (Annexure A - Initial assessment checklist).

Note: As part of the initial request, the Device Approval Applicant 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.

The Device Approval Applicant must ensure that the Vendor is prepared to make the solution itself available to the lab for testing as part of the industry analysis.

1.4 Identification Phase

Figure 2 below highlights the steps of the identification phase

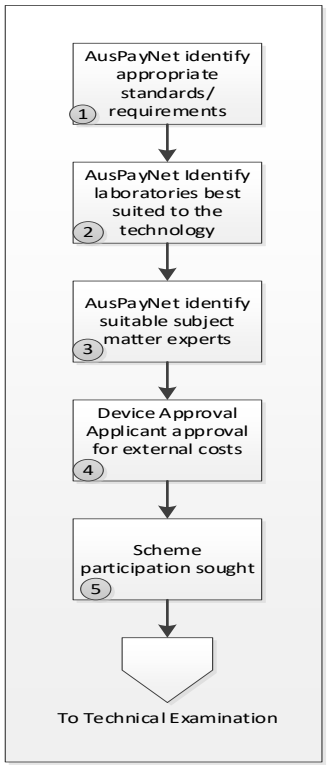

Figure 2 – Identification Phase

[2]- An estimate of the expected costs will be advised to the Device Approval Applicant before any decision is made to spend the money.

1. AusPayNet will initially review the Initial assessment checklist and obtain the views of the card schemes with regards to the technology under consideration. AusPayNet 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 will identify any laboratories, not necessarily Approved Evaluation Facilities, with particular knowledge and/or skills in testing the technology involved.

3. AusPayNet will identify any subject matter experts willing to assist in the evaluation of the technology and estimate likely costs. Any consultants likely to be engaged must be willing to agree to AusPayNet's confidentiality requirements and any applicable terms of reference.

4. AusPayNet will advise the Device Approval Applicant of the selected laboratory (more than one laboratory is possible) and the likely estimate of external costs and obtain the Device Approval Applicant's agreement to bear those costs.

5. Having gained the Device Approval Applicant's approval for bearing the costs involved, AusPayNet may approach the card schemes requesting nominations for experts to attend and assist in the evaluation of the technology.

Prior to completing the Identification Phase, AusPayNet will ensure that appropriate contractual arrangements are 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 Device Approval Applicant/Vendor and any Subject Matter Experts.

1.5 Technical Examination Phase

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

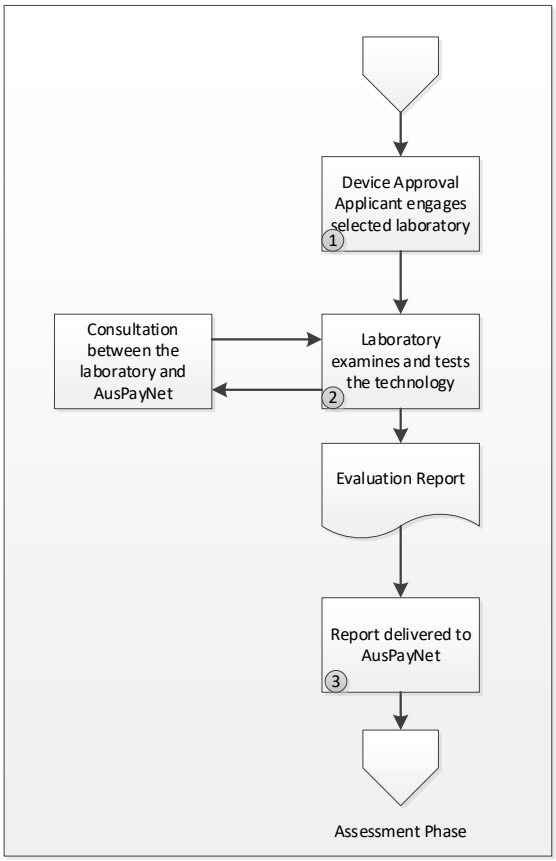

Figure 3 – Technical Examination

1. The Device Approval Applicant or vendor will engage the identified laboratory or laboratories if so required by AusPayNet and arrange for a review with the output report to be provided to AusPayNet. This engagement should permit an ongoing dialogue between the laboratory and AusPayNet 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 card schemes may also choose to do their own testing in addition to the industry testing.

3. The laboratory will provide the report to AusPayNet and the Device Approval Applicant/Vendor if required by AusPayNet:

    a) Card schemes may carry out their own testing/analysis and provide AusPayNet with any additional risks that they consider as relevant for the device or technology under consideration.

1.6 Assessment Phase

Figure 4 below highlights the steps of the assessment phase:

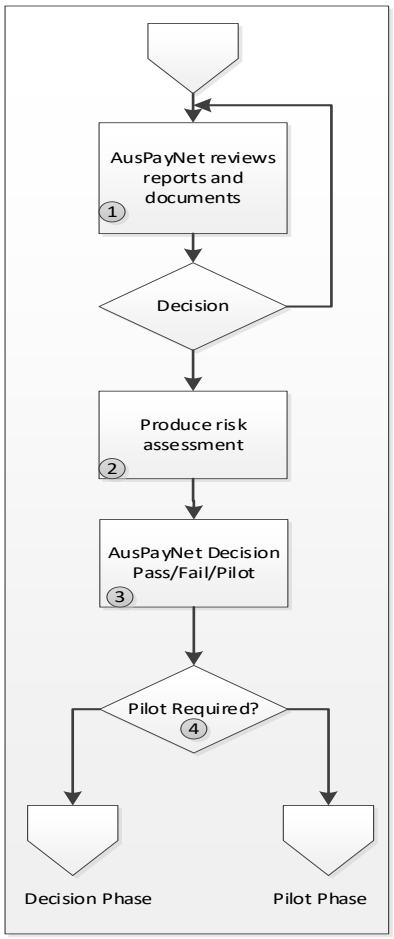

Figure 4 – Assessment phase

1. AusPayNet convenes a meeting, which includes 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 may occur if more information is required.

2. AusPayNet produces a high level risk assessment of the device.

    a) In order to facilitate the risk assessment, the Device Approval Applicant/Vendor should provide to AusPayNet any available technical documentation and/or results from previous testing, including relevant testing carried out by the card schemes in Australia or internationally.

b) In the risk assessment, AusPayNet 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. AusPayNet will determine whether:

- to approve the device or decline to approve the device in accordance with Part 8 of the Device Approval Process; or
- a Pilot Phase is required and determined appropriate criteria.

1.7 Pilot Phase

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

1. All agreed criteria are applicable to the Device Approval Applicant, not the Vendor;
2. The Device Approval Applicant should report on performance against criteria at a pre-determined frequency;
3. Anything that AusPayNet 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 AusPayNet 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. By undertaking the Pilot Phase, the Device Approval Applicant accepts the liability shift stated in 'Principles for Liability Shift' in Annexure B to this Schedule; and

[4] Such criteria (including success criteria) would be agreed with the Device Approval Applicant and card schemes. Annexure B of this Schedule 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

7. The Device Approval Applicant 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 Device Approval Applicant collects the data and provides it to AusPayNet in line with the agreed criteria. Card schemes receive the data in relation to their pre-determined individual criteria from the Device Approval Applicant directly.

The data provided by the Device Approval Applicant is assessed by AusPayNet Management against the pre-defined criteria.

If significant issues are identified during the course of the pilot it can be shut down prior to completion by the Device Approval Applicant, the Vendor or AusPayNet.

1.8 Decision Phase

Following any Pilot Phase, AusPayNet will:

- 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; and

- approve or decline to approve the device, in accordance with Part 8 of the Device Approval Process.

PART 3 ANNEXURES

ANNEXURE A INITIAL ASSESSMENT CHECKLIST

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

1- Date of submission: …../……/…..

2- Name of the Device Approval Applicant (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 Device Approval Applicant 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 Device Approval Applicant deems relevant:
.....
.....

ANNEXURE B HIGH LEVEL CRITERIA FOR PILOT

Once AusPayNet 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 Device Approval Applicant 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 Device Approval Applicant and AusPayNet to track during the course and at the completion of the pilot.

Note: the card schemes may separately impose their own requirements to the Device Approval Applicant.

Principles for Liability Shift

- A Device Approval Applicant 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 Device Approval Applicant'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 Device Approval Applicant 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).