IAC Device Approval - Frequently Asked Questions

Version 2.1 March 2024

Australian Payments Network Limited has published the IAC Device Approval Process to approve Devices, Solutions and Non-Standard Technology for use in Australia.

Approved Devices are listed on the Approved Devices List published on AusPayNet's website.

Set out below are a series of Frequently Asked Questions regarding AusPayNet's Device Approval Process. Additional questions may be submitted to PAG@auspaynet.com.au.

Q.1. *What are the Accepted Standards for a Device?*

Devices that comply with Accepted Standards may be registered for use in Australia. The Device Approval Process lists the Accepted Standards in (1.2. (b)(i)).

The Accepted Standards are:

1. *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Version 6+, which may be relevant to the following devices:*
    a. *Encrypting PIN pad for ATM, Vending, AFD or Kiosk (EPP).*
    b. *Secure (encrypting) card reader (SCR.*
    c. *Secure (encrypting) card reader PIN (SCRP).*
    d. *Non-PED POI device.*
    e. *Other secure components for a PIN entry device.*
2. *Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM), Version 3+, which may be relevant to the following devices:*
    a. *Hardware Security Modules (SCMs or HSMs).*
    b. *Key-Loading Devices.*
    c. *Remote Administration.*
3. *Payment Card Industry (PCI) Contactless Payments on COTS (CPoC).*
4. *Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC).*
5. *Payment Card Industry (PCI) Mobile Payments on COTS (MPoC).*

The list of Accepted Standards will be updated from time to time.

Q.2. *What is the process to Register a Device?*

If a device complies with an Accepted Standard, the Vendor, Acquirer, or Deployer may submit an Application for Registration[1] together with the Attestation of Compliance[2] to PAG@auspaynet.com.au.

[1] https://www.auspaynet.com.au/sites/default/files/2022-03/Application%20for%20Registration_DAPv2.0_.pdf

[2] PCI issued Letters of Approval (LoA) and PCI-countersigned Attestation of Validation (AoV) documents are considered Attestation of Compliance documents for this purpose of this submission.

AusPayNet will review the Application for Registration and examine the Attestation of Compliance for validity. If the Attestation of Compliance is successfully validated, AusPayNet will send to the Device Approval Applicant a Letter of Approval noting the Approval Period. The Approved Device will then be published on AusPayNet's Approved Devices List[3].

Q.3. *If a payments acceptance device does not meet an Accepted Standard, what are the approval pathways?*

Devices that do not meet an Accepted Standard are assessed through the Non-Standard Technology (NST) process for approval.

The outcome of the NST Process could be:

a. *Device registration with or without conditions.*
b. *Limited pilot approval with conditions.*
c. *Decline. Sufficient information will be included on the letter of decline to enable the applicant to understand the rationale and the technical changes or additional evidence that would be required to enable a successful resubmission.*

An Acquirer must sponsor the non-standard approval pathway, except if specifically requested and approved by the AusPayNet CEO.

Q.4. *Will expired devices not meeting an Accepted Standard be renewed?*

Where an expired device:

a. never had an Attestation of Compliance; or
b. had an Attestation of Compliance which has expired; or
c. has been grandfathered.

AusPayNet, in its sole discretion, may extend the Approval Period for a further period of three years or such other period as it (in its absolute discretion) deems appropriate.

Factors considered by AusPayNet in making a determination as to whether to extend the Approval Period, and the term of the Approval Period include but are not limited to:

a. changes in security technology.
b. changes to Approved Standards.
c. changes to the threat environment
d. newly discovered vulnerabilities
e. whether a device has been grandfathered.

If AusPayNet determines in its sole discretion not to extend the Approval Period for a device, then an IA Participant can apply to AusPayNet for an exemption from the obligation to only use approved devices. The Exemption Process is set out in Volume One Part 3 of the IAC Code Set (link). The application for exemption must include:

a. the reason for non-compliance;

[3] https://approved-devices.auspaynet.com.au/

b. a description of the risk and a risk rating for the non-compliance; and
c. an action plan to achieve compliance including the number of devices in market and the likely date when the expired device would no longer be used.

AusPayNet will review the exemption application having regard to the integrity and efficiency of the IAC and advise the IA Participant of the acceptance or rejection of the application. Any exemption granted by AusPayNet will be only for a defined period and will be required to be reviewed and renewed annually.

Q.5. *If a Device has undergone a delta assessment, how is the Registration updated?*

If the delta assessment does not affect the make, model, approval number or other details listed on the AusPayNet website, then no action is required to update the registration and AusPayNet listing.

If the delta assessment affects the details listed on the AusPayNet website, then the applicant must complete and submit a new Application for Registration and the delta Attestation of Compliance to PAG@auspaynet.com.au. AusPayNet will validate the Application for Registration and AoC and send to the Device Approval Applicant a new Letter of Approval, and update the registration on AusPayNet's Approved Devices List.

Q.6. *How are Payment Applications for PTS Approved Devices assessed?*

AusPayNet does not require independent assessment of payment applications executing on approved PTS devices. It is the responsibility of the Acquirer to ensure that the payment application is free of security vulnerabilities or other security weaknesses. Devices running multiple applications including non-payment applications must protect the payment application and its associated data from any interference or corruption caused by any other data or other application.

Q.7. *How are Payment Applications for PIN on COTS solutions assessed?*

Payment Applications are an important part of the approved solution and require security review and approval. Payment applications handle plaintext PIN and/or plaintext PAN, either directly through code developed by the app creator or indirectly by embedding a third-party SDK.

Review of a Payment Applications which embeds a previously approved SDK will focus on the interface to the SDK and secure coding practices of the payment application developer. This approach reduces the review workload and is consistent with MPoC Module 2.

Non-payment applications executing on the same COTS platform as payment applications do not require AusPayNet or Acquirer review.

Q.8. *How does the Device Approval Process assess and renew ATM Devices?*

AusPayNet does not assess whole ATM Devices under the Device Approval Process introduced in Jan 2022. Only the EPP component of the ATM is required to be approved by an Approved Standards Entity. If the

EPP meets an applicable Accepted Standard[4] then the Device Approval Applicant can submit a request to register the EPP as an Approved Device.

If an existing ATM device approval is nearing the end of its Approval Period:

a. where the EPP of the ATM device is approved by an Approved Standards Entity, the Device Approval Applicant can submit to AusPayNet an Application for Registration (link) together with the Attestation of Compliance for the EPP. AusPayNet will validate the Attestation of Compliance and register the EPP as an Approved Device. The period of approval will align with the expiry period under the Attestation of Compliance. The EPP name and details will be published on the Approved Devices List;
b. where the EPP of the ATM device is not approved by an Approved Standards Entity, AusPayNet will determine, in its sole discretion, whether to extend the Approval Period for a further period of three years or such other period as it (in its absolute discretion) deems appropriate. If AusPayNet determines not to extend the Approval Period for the ATM device, an IAC Issuer or Acquirer can apply to AusPayNet for an exemption from the obligation to only use approved devices, as detailed in FAQ 4 above.

Card readers in an ATM should be an approved device type from an Approved Standards Entity.

Q.9. *Major card brands have been requiring independent lab evaluations against brand specific requirements as part of their T2P or ToP pilot programs. Must these lab evaluation reports be provided to AusPayNet for a non-standard technology assessment of a COTS with PIN solution?*

Non-standard technology assessments require detailed design documentation and other information which enables an understanding of the risk level of the solution to be determined. Lab evaluation reports are a useful and valuable source for this information and should be provided if possible. If lab evaluation reports to card brand requirements are not provided, then equivalent information must be provided in other documentation.

Q.10. *Non-Standard Technologies may utilize backend systems which process plaintext PINs or PIN related keys. Must evidence of PIN security compliance be included in the submission for a non-standard technology approval?*

Yes, any backend solution components with PIN security related impact are required to be assessed against PCI PIN or the AusPayNet Annual Security Audit and have evidence of compliance provided for review by AusPayNet.

[4] As of July 2023, the only applicable Accepted Standard for EPPs is PCI PTS. New devices must be compliant with PCI PTS 6.0 or higher.

Q.11. ***Can SDKs be assessed under the non-standard technology process?***

Yes, an SDK can be assessed and listed. An SDK is typically classified as a component because it does not implement all security controls required for the approval class. Component approvals will include conditions stating that additional approvals are needed for any solution integrating the component.

Q.12. ***IAC Code Set Vol 1 – Annexure A Annual Security Audits requires all Non-Standard Technologies to be approved by the Company (AusPayNet). Is using an approved SDK sufficient to meet this part of the annual audit?***

No, an SDK is a component of an acceptance solution and will include a condition requiring an additional approval/s for the application, backend monitoring and attestation system, transaction processing backend or other components not covered under the SDK approval. The annual security audit requires the complete solution or complete device to be approved.

Q.13. Can all Android platforms be used as part of Non-Standard Technology solution?

No, an Android platform must use Android 9.0 or newer. Use of the hardware-backed keystore present on Android 9+ compatible mobile devices (https://source.android.com/docs/compatibility/overview) is strongly recommended.

Q.14. ***PCI MPoC includes requirements which may be relevant to a Non-Standard Technology. Will Non-Standard Technologies which are not compliant with one or more MPoC requirements result in an automatically declined submission?***

No, AusPayNet uses a risk-based approach to non-standard technology assessments. Compliance gaps between a submitted solution and an Approved Standard will add to the risks considered during the non-standard technology assessment but does not automatically mean a solution is unacceptable.

Q.15. ***What PIN block formats are acceptable for use by a Non-Standard Technology?***

Consistent with PCI MPoC, ISO 9564 Format 4 must be used for transport of PINs between non-standard POI technologies and the introduction to interchange.

Q.16. ***Can 3-key TDEA be used for cryptographic protection of PINs or account data between POI and initial interchange (terminal to node) in a Non-Standard Technology?***

No, AES is the only symmetric algorithm allowed for use by the POI in a non-standard technology.

Q.17. ***A fundamental security principle from PCI SPoC (Guidance, TR B3) was that PIN is kept separated from account data? Does the Non-Standard Technology program require that PIN and PAN are never present in volatile memory at the same time?***

No, creation of an ISO 9564 Format 4 PIN block requires the presence of the plaintext PIN and plaintext real(funding) or tokenized PAN for formation of the PIN block. The real PAN may be used in the creation of PIN blocks providing all temporary buffers are erased immediately after encryption of the PIN block. Tokenized PANs must be cryptographically bound to the plaintext real(funding) PAN. Buffers must be in volatile memory. The operating system must prevent other applications executing on the platform from accessing the buffers and the system shall include remote monitoring to detect modifications to the operating system.

Q.18. ***PCI MPoC has a requirement that plaintext secret and private key material present in the Rich Execution Environment is unique per transaction. Does the same requirement apply to non-standard technologies under the SRA process?***

Yes, general purpose memory on COTS devices has limited protection and can only be used for temporary storage of one-time use data for the shortest possible duration and must be securely overwritten when erased.

Q.19. ***What is the scope of a non-standard technology assessment?***

The scope of a non-standard technology assessment includes all components which impact the security of sensitive payment data, including PINs, PANs and the cryptographic keys used to protect PINs and PANs.

For devices which include hardware based anti-tampering features, the scope includes the hardware and software executing on the device. Scoping for such devices will be performed consistent with PCI PTS.

For solutions which rely upon remote security services, such as attestation and monitoring systems, the scope includes the payment acceptance device, remote service and any relevant operational processes. Scoping for such solutions will be consistent with PCI MPoC.

Non-standard technologies which do not fit into either of the above categories will be scoped during the AusPayNet assessment process and communicated to the applicant.

Evidence (lab reports, design details etc.) provided for the assessment is required to cover all components within the defined scope.

Q.20. ***What technical documentation should be submitted with an NST application of a complete solution?***

To aid in its analysis and speed up the evaluation process, AusPayNet requires NST applications to be accompanied by clear professional descriptions of:

- The overall technical architecture including both POI and backend components.

- A key table listing all stored and ephemeral keys. For each key, its origin, creation method, storage and usage locations, fully defined cryptographic usage mechanisms[5], and key lifetimes must be listed.
- Solution management, key management and transaction data flows between the POI and solution backend components, preferably in the form of, or augmented by, ladder diagrams.
- Key management and transaction data flows between solution backend components including HSMs, and for payment solution backend processing components interfaces to acquirers.
- Backend automated risk management monitoring and velocity controls.

Note that laboratory reports, especially those targeting card brand requirements, often assume access to the above information and do not present sufficient of the information therein for AusPayNet to arrive at a risk determination.

Q.21. *MPoC supports three different approval types – MPoC Solutions, MPoC Software and MPoC A&M Services. Can all three types be registered under the AusPayNet Device Approval Program?*

Yes. MPoC Solutions are complete solutions which can be unconditionally listed. MPoC Software (including SDKs) and MPoC A&M Services are reusable components which can be used as part of a complete MPoC Solution. Conditions will be added to the listing of MPoC Software and MPoC A&M Services detailing the additional assessment required for an MPoC Solution utilizing these components.

A common design is to have an SDK (e.g. an Android aar file) and A&M software (e.g. containerized app ready for cloud deployment) submitted for assessment as MPoC Software. Once approved and listed, solutions can reference these components during the assessment of the overall solution. The final application (apk) used by the merchant would be included in the overall solution listing, together with a reference to the underlying SDK and A&M software listing.

[5] For example, it is insufficient and incorrect to state that something is encrypted with an RSA or ECC public key: the precise mode of operation must be explained including padding or chaining rules, and where public keys are used to transport or agree symmetric keys which are then used to form cryptograms or in other calculations, the precise modes of use for those symmetric keys.