IAC DEVICE EVALUATION FAQ

Version 9 (Effective 1 July 2019)

This FAQ provides answers to questions regarding Australian Payments Network's physical and logical device security requirements and evaluation methodologies as specified in the IAC Code Set.

In so far as it is possible, the terminology used in this Q&A has been aligned with that used in PCI documents, however it needs to be clearly understood that the IAC process is significantly different to the PCI process.

A. GENERAL

Q1. Who is the Australian Payments Network Limited (AusPayNet)?

AusPayNet is the payment systems self-regulator which works collaboratively with members, government, regulators and other stakeholders to improve the Australian payments system through:

- enabling competition and innovation;
- promoting efficiency; and
- controlling systemic risk.

By doing this, we engender confidence in the Australian payments system and advance the common interest of our members and the interests of the Australian public.

Q2. Why is there an Australian specific device approval process?

The IAC device security standards are aligned with current Australian and/or international standards. In some cases the Australian standards are closely aligned with ISO standards, however in many cases there are material differences (see Question 26 for further detail). The Australian device approval process recognises those differences. In aligning our requirements in this manner we ensure that we are applying national and international best practice in a fair and transparent manner.

The card schemes' approval system (PCI) currently covers Point of Interaction (POI), EPPs, HSMs (otherwise referred to as SCM devices), Key Loading Devices and SPoC Solutions. In IAC, all devices involved in the initialization of Card-based transaction, i.e. Terminals, PIN handling and/or cryptographic key management are required to be tested and approved. Other significant differences include the evaluation of security-related application software, mandatory MACing of both request and response messages (PCI has no such mandates), required support of the Australian key-management protocols AS 2805.6.4, 6.2 and 6.7 and the prohibition of fixed-key, key management.

Q3. How does the PCI-Software-based PIN on COTS (SPoC) approval process work within the IAC?

The Device Approval Process, depicted in Figure 1, outlines the standard Australian device approval flow. A standard device is one which meets the device requirements set out in Volume 4 of the IAC Code Set. PCI-SCC released a standard and approval process in January 2018 for SPoC solutions. AusPayNet require that SPoC solutions must be certified by PCI. Australian specific requirements are enforced, such as privacy of communications and key management practices. The SPoC Solution approval process is outlined as part of the IAC Code Set Volume 4, Annexure G.

*Note: For purposes of clarity be aware that transactions originating from magnetic stripe data are **NOT** accepted via SPoC Solutions in Australia. Any SPoC Solution which includes magnetic stripe functionality is prohibited from implementing that functionality in Australia and any SCRP which include magnetic strip readers will **NOT** be approved.*

Q4. How are approved PCI-SPoC Solutions listed?

A PCI-SPoC Solution has four parts: The mobile (COTS) device, the secure card reader (SRCP), the PIN CVM Application and the Backend Monitoring System. The four components are listed as a single solution. Having a solution that has only an approved SCRP component does not mean that the solution is approved. All elements of a solution are evaluated in combination, not as separate components.

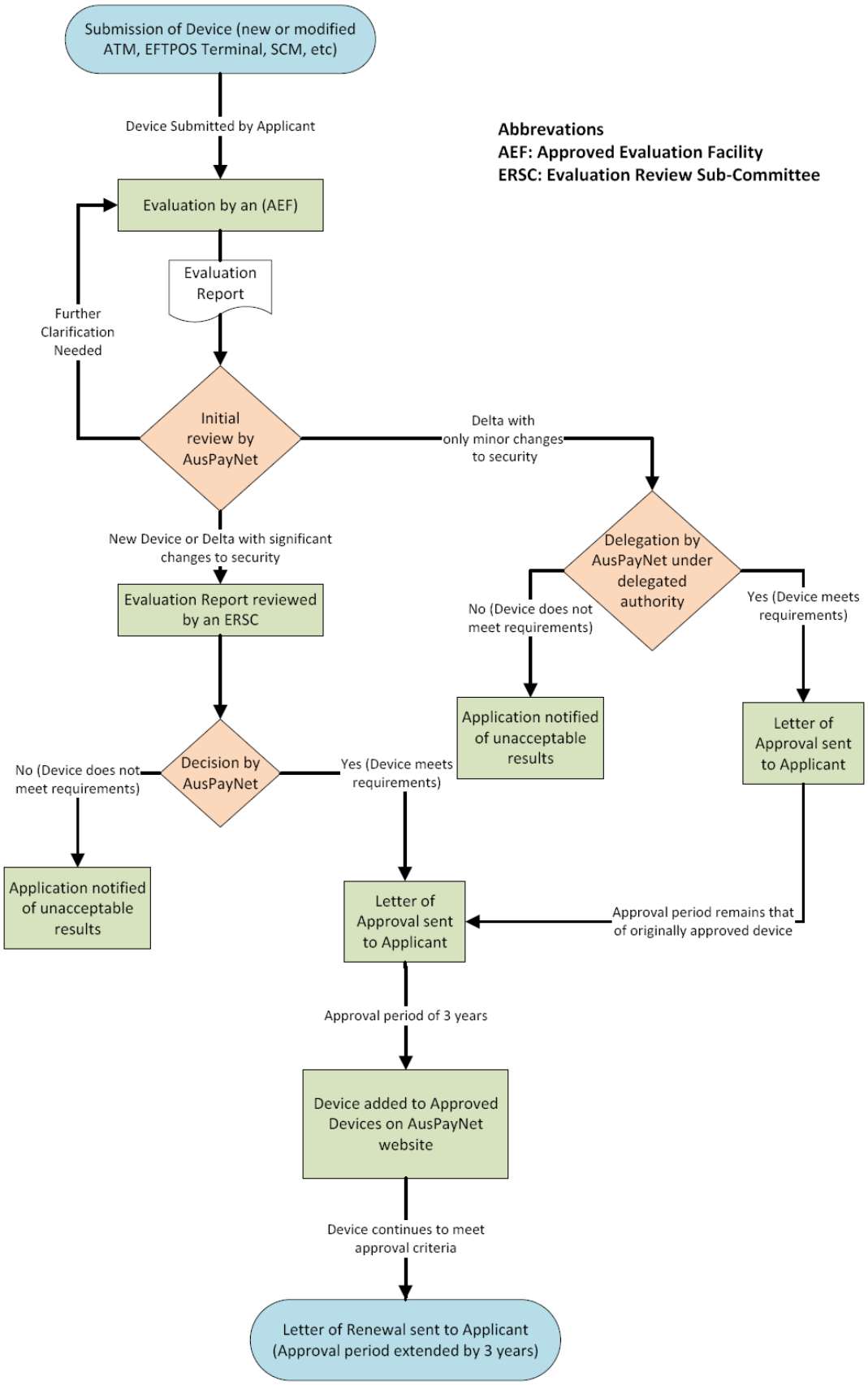
Q5. What are non-standard technologies?

Innovation and rapid changes in technology drive the development of payment solutions that do not fit within the paradigm of traditional security standards. In this sense, conventional technologies have existing requirements and approval processes in place. When new technologies cannot be assessed against the current standards and compliance programs, then they may be deemed a non-standard technology.

Q6. What is the process for assessing non-standard technologies in the IAC?

IAC Code Set Volume 4, Annexure G, Schedule 1 outlines a process for the consideration of non-standard technologies at the point of interaction and includes an initial assessment checklist which an Acquirer must complete to initiate an evaluation. The assessment is divided into 6 stages, namely the Request, Identification, Technical Examination, Assessment, Pilot and Decision phase.

Figure 1: Device Approval Process



Q7. Which EFTPOS Terminals require approval for use within IAC?

Within IAC all services associated with the handling and management of Cardholder PINs and all cryptographic processes within financial Terminals must be performed within a device that meets the requirements of a physically secure cryptographic device as defined. These requirements are defined in ISO 13491-1 for devices employing master/session key or DUKPT key management. The checklists used by Approved Evaluation Facilities (AEFs) in evaluating devices for conformance with these security requirements are specified in AS 2805.14.2 or ISO 13491.2.

Specifically all those components of a financial Terminal that are involved in requesting, collecting and processing of Cardholder PINs and card details are required to meet the requirements of a Secure Cryptographic Device (ref clause 2.4.3 of the IAC Code Set, Volume 4).

This definition may be viewed as illustrated in Figure 2 - SCD & EFTPOS (Financial) Terminal Relationship – Type 1.

Cardholder activated EFTPOS Terminals contain (where present), the PED (keypad), display, magnetic stripe reader (MSR), Integrated Circuit Card (ICC) reader, cryptographic processor and the prompt presentment logic all of which must be contained within a container, as illustrated in figure 1, meeting the requirements of a Secure Cryptographic Device. Where the Acquirer Application has access to clear text keys used to protect either the PIN or the Transaction or controls the presentation prompts for PIN entry, it too must be assessed within the SCD container, see Figure 3 – SCD & EFTPOS (Financial) Terminal Relationship – Type 2. It is possible for a vendor to produce a device where all the components of Figure 1 are within the SCD container.

Approved Evaluation Facilities (AEFs) will evaluate devices for adherence to these requirements using the mechanisms and checklists from AS 2805.14.2. Note that this standard is identical to ISO 13491 part 2:2005.

Q8. What is a PED and what is an EFTPOS Terminal?

“PIN Entry Device” and “PED” means an optional component of a Terminal which provides for the secure entry and encryption of PINs in processing a Transaction.

“EFTPOS Terminal” means a whole approved device which provides for the secure processing and completion of a Transaction, including the secure entry and encryption of PINs when a PED is present.

For the purposes of the security evaluation the target of evaluation includes all those components associated with the collection and processing of cardholder PINs and card details. This includes where present, the PED, the magnetic stripe reader (MSR), ICC reader, display, prompt storage and presentment logic.

Q9. Which device types are included?

The IAC Rules classify financial Terminals into two broad categories, namely Electronic Funds Transfer Point of Sale (EFTPOS) Terminals and Automatic Teller Machines (ATMs). Additional device types requiring approval include Encrypting PIN Pads (EPPs), host security modules (HSMs), alternatively known as Security Control Modules (SCMs), SPoC Solutions and Key Loading and Transfer Devices (KL/TDs).

IAC device approval can only be granted to complete functioning devices; for financial Terminals this includes where present, the PED, the magnetic stripe reader, ICC reader display and any software involved in PIN security, such as PIN acceptance and handling, cryptographic processes and key management.

To assist vendors of encrypting PIN pads (EPPs), devices meeting an appropriate subset of the device security requirements from AS 2805.14.2, will be identified as such on AusPayNet's approved device list. Such listing will not remove the need to obtain device approval for any device that includes the approved EPP as a component; however, by using an already approved EPP, the amount of additional effort required to obtain device approval for the full financial Terminal may be significantly reduced.

Vendors seeking to utilise listed approved EPPs as a component of a new submission must check the EPPs deployment conditions to ensure that the EPP does not have a date listed beyond which it will no longer be accepted as a supported component in the submission for approval of a new device.

Q10. Unattended Payment Terminals

An Unattended Payment Terminal (UPT) is a financial Terminal, other than an ATM, conforming to the requirements of an SCD that is intended for deployment in an environment not under the constant oversight of the merchant.

UPTs must provide strong deterrence against penetration of their outer shell to protect the individual security related components.

A UPT is currently treated as an EFTPOS Terminal within the IAC Rules.

Q11. How are EFTPOS Terminal approvals classified?

Approval for EFTPOS Terminal types is granted under two categories, Type-1 and Type-2 depending on the level of security functionality provided by the acquirer or end-user application, as described below. The purpose of assigning these classifications is as an aid for acquirers in determining when re-approval is required as a consequence of changes to the device application. Please note, these classifications are different from the PCI classifications of POS-A and POS-B.

Type-1:

This classification is given to EFTPOS Terminal devices that have no security functionality provided by the acquirer and end-user applications. This includes the fact that the data-collection prompt presentment cannot be altered by these applications. To be granted a Type-1 classification, the device must have met all of the applicable security criteria, the end-user must be unable (by device design and construction) to modify the device's data-collection prompts, firmware and cryptographic functions, and only the manufacturer has the capability to modify the prompts and controls for PIN entry. The mechanisms and controls used to install or modify these sensitive functions and prompts must be distinct from the mechanisms used to control the modification and installation of the acquirer application. See Figure 1 of this Manual for a diagrammatic representation of a Type-1 device. Devices meeting the Type-1 specification do not require individual approval for the Acquirer application.

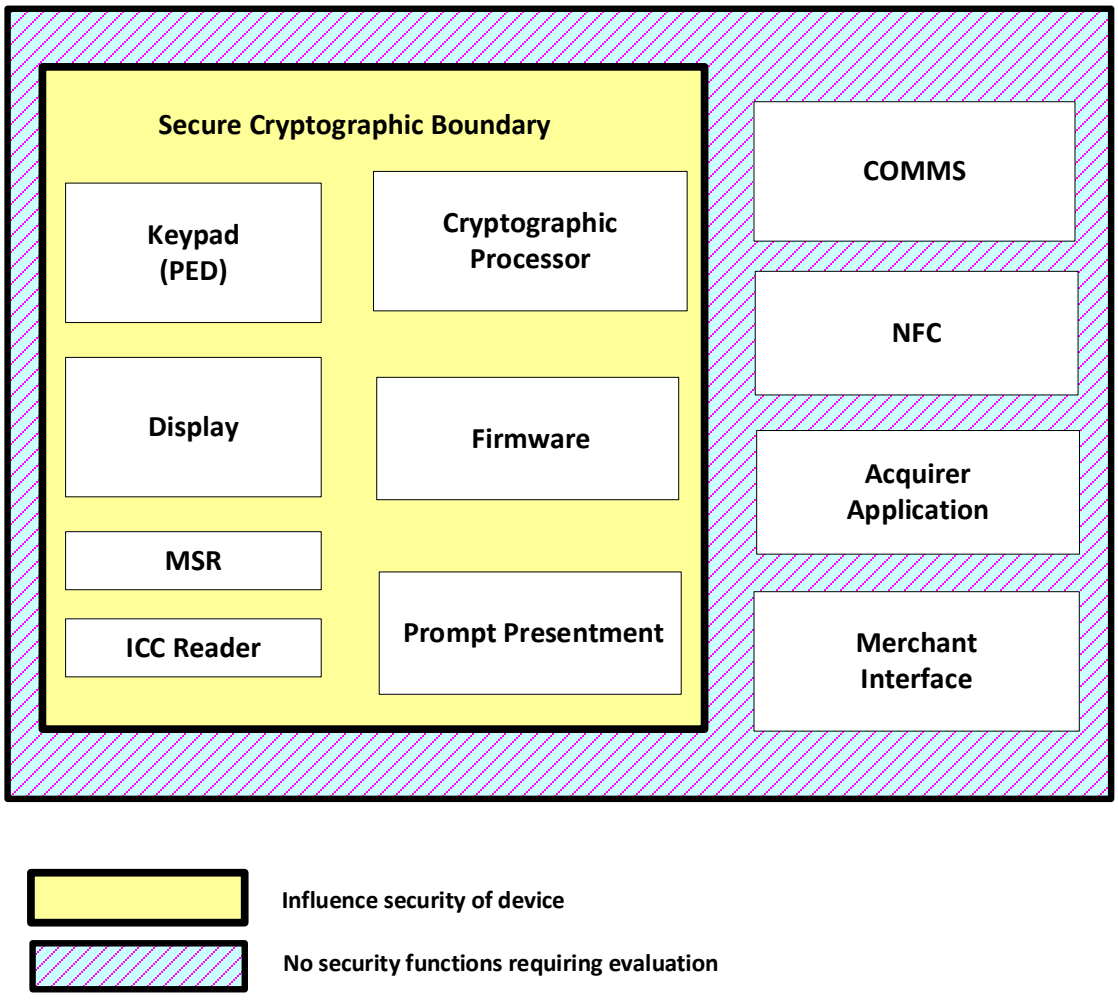


Figure 2 SCD & EFTPOS (financial)Terminal Relationship – Type 1

Type-2:

This classification is given to EFTPOS Terminal devices where, unlike for Type-1 devices, the end user application can provide some security functionality such as through having un-moderated access to the display and keyboard. This classification includes Point of Sale devices where there are multiple end user applications, including non-payment applications, which have unmodulated access to the display and keyboard. Non-payment applications must be prevented from accessing any payment application and its associated data (especially PINs and cryptographic keys).

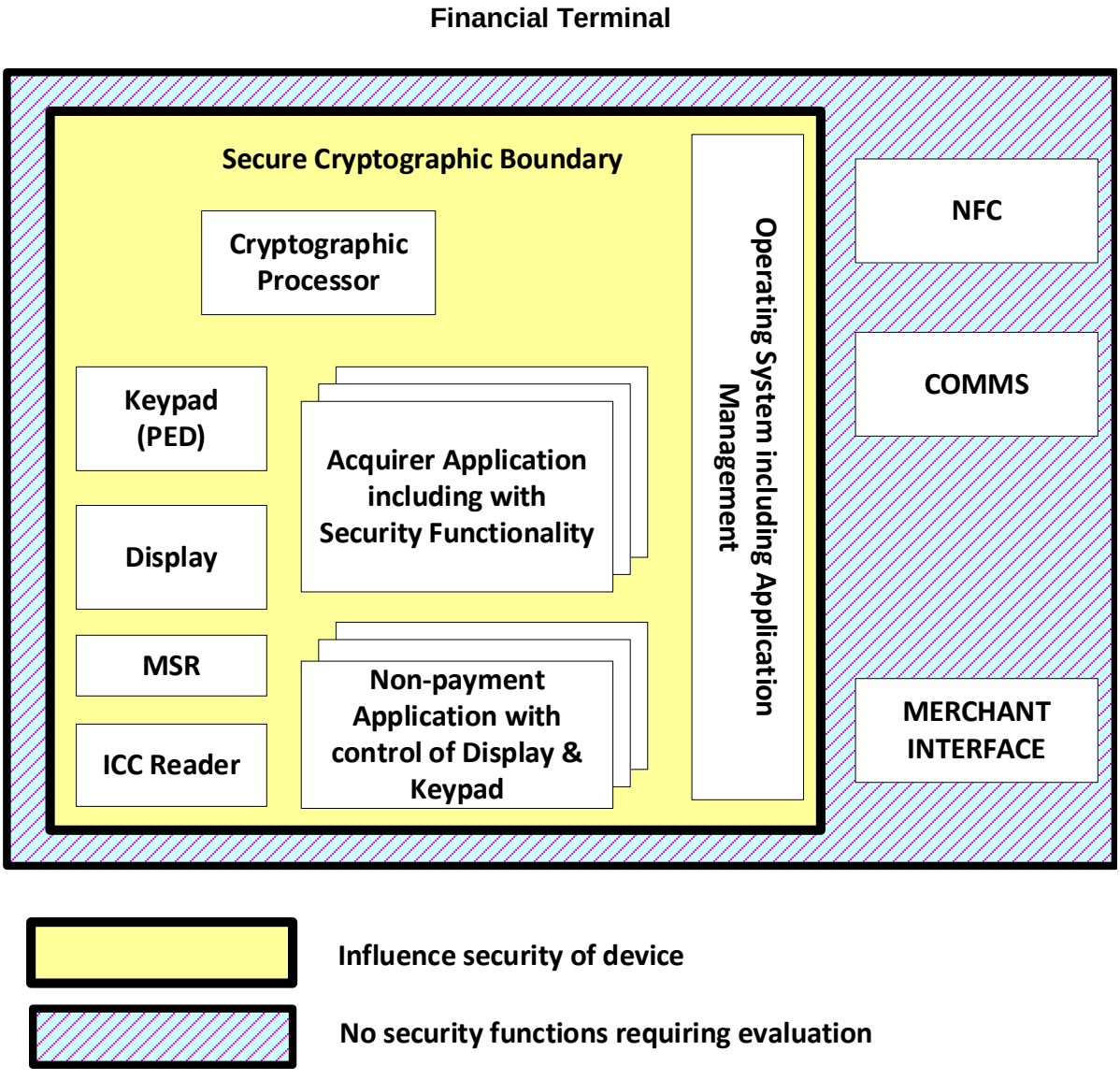


Figure 3: SCD & EFTPOS (Financial) Terminal Relationship – Type 2

To be granted a Type-2 classification, the device must have met all of the applicable security criteria and the manufacturer must be capable of shipping the device with mechanisms in place for controlling the display and its use. These mechanisms can be employed to unlock the device, using proper cryptographically controlled processes, to allow the Acquirer to update the prompts. The Acquirer application would typically have un-moderated access to the device's display, keyboard and prompts. As prompt presentment is part of the Acquirer application, devices meeting the Type-2 specifications require individual approval for each different Acquirer application to be deployed. Updates to approved Acquirer applications will only require further approval as described in Question 9 below.

Additionally, where the device is capable of running multiple applications, including non-payment applications, the manufacturer must be capable of shipping the device with cryptographic mechanisms in place for controlling the deployment of all applications running on the device.

Non-payment applications must be subject to a cryptographic mechanism which authenticates and authorises each application before each execution on the device. The details of these mechanisms must be addressed in the device evaluation report.

Non-payment applications require individual evaluation and authorisation by the Acquirer, or a party explicitly trusted by the Acquirer, for each application to be deployed or updated.

Q12. Can the EFTPOS Terminal hardware be approved for use without an application?

Only a complete functioning Terminal can be approved for deployment under the IAC Code Set. If an application is required to perform transactions, then an application must be part of the approved Terminal. The Terminal will be identified on the Approved Device Lists by hardware, firmware and application identifiers.

EFTPOS Terminals achieving a type 1 classification do not require re-approval if deployed with other Acquirer applications than that listed. Type 2 EFTPOS Terminal devices require re-evaluation (delta evaluation) and approval for each unique instance of the Acquirer application.

Q13. Component Approval

Where a device consists of a number of components, each individually meeting the requirements for a secure cryptographic device, and intended for use where the inter-connections between the components provide the necessary level of either physical and/or logical protection, then such devices may be individually evaluated and listed in the approved device lists.

Irrespective of whether all individual components making up a financial Terminal are themselves approved, an evaluation-report and approval of the complete device is still necessary before deployment within IAC. Such a final evaluation need not re-examine approved components.

Where the individual components of a device host public keys or PIN-security related cryptographic keys, and/or key components and residues, then the device component must be evaluated against those values of “Not Feasible” (clause 2.3.1 of the IAC Code Set, Volume 4) required protecting for attacks against keys as well as the device component specific requirements.

Q14. Can a device's hardware be approved separately?

Hardware only evaluations can be accommodated and devices so approved will be listed, suitably annotated in the approved device lists. However, only fully approved, complete devices can be deployed within IAC. As complex interactions can occur between the hardware and software, an evaluation report covering the entire device (hardware and software) will be required before full approval is given.

Q15. Do changes to the Acquirer application require re-approval?

For type 1 EFTPOS Terminals, no change to the Acquirer application can affect the security components so re-approval is not required.

For type 2 EFTPOS Terminals, any changes to the device’s cryptographic processes, PIN handling (including cardholder prompts relating to security data collection), and cryptographic key management will require re-evaluation and re-approval. The evaluation may not need to be a complete review but go only to the changes and any consequential effects (i.e., a delta evaluation). The determination, as to the areas impacted by a change, is the responsibility of the Acquiring Member supported by advice from the equipment vendor. It is a requirement of IAC that only devices meeting the IAC security requirements be deployed within the system.

New non-payment applications or updates to existing non-payment applications are required to be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer, and must be authenticated by the same cryptographic mechanism that was part of the device approval.

All **ATM payment applications** other than those identified as approved payment applications on the AusPayNet approved devices list are required to be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer, and must be authenticated by the same cryptographic mechanism that was part of the original device approval. AusPayNet approval of an ATM payment application is applicable to only the specific device with which it is listed, that is approved ATM payment applications are not transferable to other ATM types and/or models.

ATM certification includes the requirement that a payment application be approved for use prior to deployment. If an Acquirer wishes to deploy an ATM payment application not listed as approved for that ATM model on the Approved Devices List then that application must be evaluated and authorised by the Acquirer, or a party explicitly trusted by the Acquirer by the same cryptographic mechanism that was part of the original device approval, prior to being deployed.

Additionally, any update or modifications to the payment application must also be re-evaluated and authorised prior to deployment. AusPayNet approval of an ATM payment application applies to only the specific device with which it is listed, that is approved ATM payment applications are not transferable to other ATM types and models.

Q16. Do changes to the device's hardware require re-approval?

Any changes to a device's physical characteristics that impact on its security features including protection mechanisms, PIN handling (including prompt presentment relating to security data collection), cryptographic processing and cryptographic key storage require re-examination and re-approval. The determination, as to the areas impacted by a change, is the responsibility of the Acquiring Member supported by advice from the equipment vendor. It is a requirement of IAC that only devices meeting the IAC security requirements be deployed within the system.

Q17. How strong must tamper evidence be?

Because merchants and cardholders are not trained to identify tamper-evidence and it is not expected that there will be frequent inspections by qualified inspectors, any tamper-evidence must be very effective. The typical uninformed cardholder and merchant must recognise that the device has been tampered with. This means damage that is ambiguous or can be hidden, or the use of tamper-evident seals are not sufficient. No device can be approved relying solely on tamper evidence for protection, (ISO 9564-1)

Q18. When is an "N/A" response to a requirement acceptable?

An "N/A" response is acceptable in three cases: first, if compliance is achieved by meeting another requirement option, such as meeting B2, but not B18; second, if the characteristics governed by the requirement are absent in the EFTPOS Terminal, (such as requirement B4 if the EFTPOS Terminal does not emit any audible tones); and last where a requirement relates to device management tasks which are the responsibility of the Acquirer. The evaluation laboratory must verify that all responses are appropriate.

Q19. What is required to adequately identify a device?

EFTPOS Terminals submitted for testing must be properly identified so that AusPayNet Members can be certain of acquiring a Terminal that has been approved by AusPayNet. The EFTPOS Terminal Identifier is used by AusPayNet to denote all relevant information, consisting of the: Make (manufacturer), Model Name, Hardware Identifier and Version, Firmware Identifier and Version, and, if applicable, Application Identifier and Version. In order to ensure that the EFTPOS Terminal has been approved, Acquiring Members are advised to purchase and deploy only those Terminal models with the information that matches exactly the designations given in the components of the EFTPOS Terminal Identifier. (This is subject to the qualifications described in Question 12 and Question 13.)

For self-certification purposes, the Acquirer's auditor must be able to confirm the device identification. This necessitates the use of tamper-proof labels and/or device functionality capable of displaying the relevant data for examination and confirmation.

Example of an EFTPOS Terminal Identifier (four components):

Terminal Manufacturer:	Acme
Terminal Model Name:	PIN Pad 600
Hardware Identifier & Version:	600-NN-421-000-AB
Firmware Identifier & version:	NOS-FW ver. 1.01
Application Identifier & Version:	AusPayNet 4.53

Hardware Identifier

The Hardware Identifier represents the specific Hardware component set used in the approved EFTPOS Terminal. The fields that make up the Hardware identifier may consist of a combination of fixed and variable alphanumeric characters. A lower case "x" is used by AusPayNet to designate all variable fields. The "x" represents fields in the Hardware identifier that the vendor can change at any time to denote a different EFTPOS Terminal configuration, such as country usage code, customer code, language, device colour. The AEF has assessed the "x" field(s) as to not impact EFTPOS Terminal's security requirements or the device's approval. To ensure that the EFTPOS Terminal has been approved, Acquiring Members are advised to purchase and deploy only those EFTPOS Terminals with the Hardware Identifier whose fixed alphanumeric characters match exactly the Hardware identifier depicted on the Approval List or the vendor's approval letter from AusPayNet. (This is subject to the qualifications described in Question 13.)

Examples on the use of Hardware Identifier:

Listed Hardware Identifier	Comments
NN-421-000-AB	Hardware identifier NN-421-000-AB of the Device Identifier does not employ the use of the variable "x." Hence, the EFTPOS Terminal being deployed must match the Hardware identifier exactly in order for the device to be considered an approved EFTPOS Terminal (Hardware component).
NN-4x1-0x0-Ax	Hardware identifier NN-4x1-0x0-Ax of the Device Identifier does employ the use of the variable "x." Hence, the EFTPOS Terminal being deployed must match the Hardware Identifier exactly in only those position(s) where there is no "x."
Vendor Hardware Identifier	**Comments**
NN-421-090-AC	If the Approved Device List lists NN-421-000-AB as the Hardware identifier in the Device Identifier, then the EFTPOS Terminal with the Hardware identifier NN-421-090-AC cannot be considered an approved device (Hardware component). However, if the IAC List of Approved Devices lists NN-4x1-0x0-Ax as the Hardware Identifier in the PED Identifier, then the Terminal with Hardware Identifier NN-421-090-AC can be considered an approved Terminal (Hardware component)
NN-421-090-YC	If the Approved Device List lists NN-4x1-0x0-Ax as the Hardware identifier in the Device Identifier, then the EFTPOS Terminal with the Hardware identifier NN-421-090-YC cannot be considered an approved Terminal (Hardware component).

The EFTPOS Terminal Identifier will be included in the approval letter and on the IAC List of Approved Devices. If an identical EFTPOS PED is used across a family of devices, vendors are cautioned against using a Hardware Version Number that may restrict approval only to that EFTPOS Terminal model.

Q20. What is classified as firmware?

For the purposes of the security evaluation, all EFTPOS Terminal software that is fixed and unchangeable across differing Acquirer payment applications is considered firmware.

This includes boot loaders, operating systems and in most cases cryptographic libraries. As noted in Question 8, the controls over the loading and/or modification of Firmware must be distinct from those used to control end-user application loading. Where cryptographic controls are employed the mechanism must be such as to ensure that only the equipment manufacturer has the ability to authorize and implement firmware changes. Firmware must be fully identified by name/number and version information. Changes in firmware that impact the security of a device require re-examination and separate approval.

AEF's should particularly note that this definition is not the same as that used in the PCI approval process, which classifies, as firmware any code within a device that provides security protections needed to comply with the PCI PTS device security requirements or can impact compliance to those security requirements, including code necessary to meet PCI PTS Core, OP or SRED security requirements.

Q21. Which Message Authentication Methods are acceptable?

The only acceptable methods of MAC generation are those contained within AS 2805.4, which currently consists of two parts. Part 4.1 addresses methods using a block cipher and part 4.2 addresses methods using hash functions. It is important to note that only one block cipher algorithm, MAC algorithm 1, is specified consisting of a full triple-DES encryption of the message. MAC algorithm 2, commonly known as the ANSI Retail MAC as specified in ANSI X9.19, may only be used when the entire process, including the key decomposition, is executed within the confines of a Secure Cryptographic Device from which no intermediate results are ever released. Approved Evaluation Facilities should monitor activity within Standards Australia for changes in this area.

Q22. Which Terminal key management schemes are acceptable?

Terminal key-management schemes acceptable to IAC are those specified in the sub-parts of AS 2805.6, namely transaction key management conformant to AS 2805.6.2 or master/session key management conformant to AS 2805.6.4. or Derived Unique Key Per Transaction key management conformant to AS 2805.6.7.

Importantly, fixed key is not currently acceptable for use with IAC. Approved Evaluation Facilities should monitor activity within AusPayNet for changes in this area. However individual acquirers may request specific permission to use other key-management schemes (e.g., ATMs) from the IAC Management Committee. Question 20 provides further guidance on the requirements for the approval of a Terminal key management scheme.

Q23. Terminal Key Management approval requirements

IAC requires that all key-management comply with AS 2805.6.1 (similar to ISO 11568-1). Additionally, for Terminals, it requires master/session or transaction key-management that complies with one of the Australian standards AS 2805 parts 6.2, 6.4 or 6.7, or alternatively with other approved mechanisms. IAC also provides for the approval of other key-management mechanisms.

The following minimum requirements will be used by AusPayNet in evaluating the suitability of Terminal key-management mechanisms. These are in addition to the key-management principles contained in the various parts of ISO 11568.

(a) Minimum symmetric key size and algorithm:

(i) PIN encipherment must use DEA-3 with either a 128 or 192-bit key length (clause 4.4.2 of the IAC Code Set, Volume 4).

(ii) Message Authentication must be achieved by using either of the MAC algorithms from AS 2805.4.1 using a 128-bit key length (clause 4.5.1(f) of the IAC Code Set, Volume 4).

(iii) Message encipherment must use DEA-3 with either a 128 or 192-bit key length (clause 4.4.2 of the IAC Code Set, Volume 4).

(b) Minimum asymmetric key size and algorithms

(i) Only DEA-2 is approved for use within IAC.

(ii) In accordance with clause 4.2.2 of the IAC Code Set, Volume 4, the minimum size for DEA-2 keys is 2048-bits. This key-size requirement may be waived for EMV compliant Terminals, where the requirements of EMV must apply.

(c) Key encipherment

A key used to protect other keys must offer the equivalent or greater cryptographic strength to the key it is protecting.

(d) Message encipherment

As message encipherment, conformant to AS 2805.9, is required for EFTPOS Terminals after January 2009, the key-management mechanism must provide for a data-protection key.

(e) Message Authentication

Bi-directional message authentication is mandatory using an approved MAC algorithm from AS 2805.4.1.

(f) Session key backtracking

Any session based key-management scheme must be designed to make backtracking of key enciphering keys as difficult as exhaustive key determination.

(g) Master key roll-over

A mechanism for updating the top-level symmetric key should be provided where a unique key per transaction mechanism is not used. This mechanism needs to ensure that the requirement for the non-disclosure of future keys is met.

(h) Session key roll-over

A mechanism that provides for the regular updating of session keys is required.

(i) Key separation

Either variants or key-tags are acceptable mechanisms for providing key-separation. It is preferable that distinct keys be used for each direction of communications.

(j) Remote Terminal initialization (if supported)

The IAC requirements for remote Terminal initialization are those in AS 2805.6.5.2 (symmetric) and AS 2805.6.5.3 (asymmetric) and ANSI X9.24 Part 2 (asymmetric). Other mechanisms may be approved, provided the basic principles of AS 2805.6.5.1 are met.

As ATM's do not typically support either of the approved Terminal key managed mechanisms, evaluation reports covering ATM devices should contain full details of the device's key-management including initialization and key-change to enable its evaluation.

Q24. What support is required for privacy of communications?

For EFTPOS Terminals, the AEF is required to confirm that the device can support data encryption in line with the requirements of AS 2805.9. The management of the key(s) used for data encryption must comply with AS 2805.6.1.

All application level data elements, including but not limited to fields P-45 (Track 1 data) and P-35 (Track 2 data), as defined in AS 2805.2, must be protected except those fields necessary to indicate the origin of the transaction and information required to correctly reconstruct the message. The latter may include the data required to derive the privacy key.

Where the EFTPOS Terminal relies upon DUKPT for the management of keys for Privacy of Communications the device must conform to AS 2805.6.7 including the normative appendix, Appendix C.

Q25. How should device evaluation reports be formatted?

The exact layout of evaluation reports is not particularly important; the device that is the subject of the report should be clearly and fully identified in the opening sections of the report. In particular, complete identification of the physical device and all firmware and software is required. Revision levels of all components should be clearly revealed.

The contents of the report must include:

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

(b) A completed list of all successful or failed tests;

(c) For failed tests, any compensating factors that mitigate the severity and/or impact of the non-compliance;

(d) The name of the sponsor;

(e) The name of the AEF;

(f) The date of the evaluation;

(g) Identification of the device (e.g., manufacturers name, model, revision, software version etc.);

(h) Completed SCD checklists;

(i) Advised deployment environment (as advised by the Sponsor);

(j) Details of the examination and testing process followed in developing the report, and

(k) An indication as to how the device meets the specification of "not-feasible" defined in clause 2.3.1 of The IAC Code Set, Volume 4. Evidence should be given into the derivation of the cost and time calculations.

Q26. What is the relationship between Australian and ISO standards?

For the purposes of an IAC evaluation, Australian standards take precedence over ISO or other national standards bodies or PCI-SSC. This is particularly important when working with Australian Standards that are clones of ISO standards. Examples include AS 2805.14 the text of which is identical to ISO 13491:2005. In these cases, as referenced standards are not necessarily functionally equivalent, references within the body of the standard to other ISO standards should be replaced with the Australian standard equivalent. For example all references to ISO 11568 should be replaced with AS 2805.6, similarly ISO 9807 is replaced with AS 2805.4. It should not be assumed that all algorithms, process and procedures appearing in ISO standards have equivalents within Australian standards. It should also not be assumed that the Australian standard is a replica of the latest version of an ISO standard as some significant delay can occur before a revision is adopted.

Q27. What mode of operation, other than Output Feedback Mode (OFB) are allowed to use as part of message encipherment in AS 2805.9?

Both OFB and CBC mode of operation as specified in AS 2804 5.2 is allowed for message encipherment in AS 2805.9.

Q28. Does Key Loading Devices which are compliant with PCI-PTS HSM V3 satisfy the IAC Code Set Requirements?

Yes, based on a gap analysis conducted by AusPayNet in 2016, the PCI-PTS HSM V3 requirements satisfy the IAC Code Set requirements for KLD's.

Q29. Who may authorise non-payment applications on devices?

Acquirers are responsible for evaluating non-payment applications, and are required to maintain a register for the Annual Acquirer Audit as per Volume 1 – Acquirer Audit Part 1 (1.2(e)).

Q30. Do the PCI-PTS HSM V3 satisfy the IAC Code Set Requirements for quiring?

The PCI+ approach for HSM is to certify compliance with Clause 2.4.10 of Volume 4 of the IAC Code Set which defines the limited set of functions allowable on an AusPayNet Approved HSM plus any specific IAC Code requirements, such as the ability to disable support of single DES and Format 1 PIN Blocks.

B. LOGICAL SECURITY CHARACTERISTICS

Q31. Is source code evaluation necessary?

To form a true opinion as to compliance with the logical security requirements it is necessary that all source code associated with security, cryptographic key-management and PIN handling including all display output (e.g., prompts) be reviewed by an AEF. This includes the acquirer application to the extent that the acquirer application and/or payment application hosted by the ATM controller, participates in security related functions including message authentication.

Exception is available for low level code such as boot loaders and operating systems where those systems are not providing security related functionality. See Question 25.

Q32. What is acceptable practice regarding the use of diagnostic features in source code?

The AS 2805.14.2 security characteristics A16, A18 and A21 impose requirements that ensure the absence of diagnostic and test features within the EFTPOS Terminal application that could be misused to reveal sensitive information. It is highly preferable that source code provided to an AEF for evaluation is free from such functions.

However, where the removal of the diagnostic code from the source code would impose significant difficulty for the manufacturer, then the presence of such code during an AEF evaluation is acceptable provided that:

(a) all such code is conditionally compiled to ensure diagnostic features are not included in versions of the application used in production;

(b) when debug features are enabled there is an unambiguous display of that fact that would be clearly evident to a cardholder or other user of that device; and

(c) the manufacturer/software developer must impose auditable quality control processes covering the compilation and release of production level application code.

Q33. Are vendor assertions acceptable in evaluating logical security?

In the event that the inspection of a source code relating to logical security by an Approved Evaluation Facility (AEF) is not practical, any vendor assertions:

(a) are acceptable but only for low level firmware such as boot loaders and operating systems; and

(b) must be accompanied by sufficient evidence to fully satisfy the AEF as to the veracity of assertions and must include:

(i) sufficient documentation, including design specifications, Application Program Interfaces (APIs), etc., to confirm the assertion;

(ii) evidence of the vendor's internal security review processes, and

(iii) evidence of the vendor's quality assurance programs and processes; and

(c) must be confirmed through full evaluation testing of affected, external APIs.

C. DEVICE MANAGEMENT REQUIREMENTS A40 THROUGH A43 : (AS2805.14.2)

Q34. How are these requirements to be evaluated?

It is sufficient for an AEF to obtain vendor assertions on these requirements and for the AEF to reasonably satisfy themselves that the evidence provided provides a high likelihood that the Manufacturer is capable of and does meet these device management requirements. Such vendor assertions must be accompanied by sufficient evidence to fully satisfy the AEF as to the veracity of those assertions and must be accompanied by evidence of the vendor's quality control processes and programs.

D. DEVICE MANAGEMENT REQUIREMENTS A44 THROUGH A52

Q35. Are these requirements to be evaluated?

No, these requirements are an Acquirer responsibility and are the subject of other processes within IAC. The correct response to these questions in a device evaluation report is Not Applicable.

E. DEVICE MANAGEMENT REQUIREMENTS B23 THROUGH B26 (CLAUSE B3)

Q36. Are these requirements to be evaluated?

No, these requirements are an Acquirer responsibility and are the subject of other processes within IAC. The correct response to these requirements is Not Applicable.

F. PERMISSIBLE DEVIATIONS

Q37. Must a PED include a privacy shield?

Yes, under normal circumstances, in accordance with the relevant clauses of AS 2805.14.2, the device must provide a means to deter the visual observation of PIN values as they are being entered by the cardholder. As an alternative, it is permissible for a device to rely on the external physical environment in which it is to be installed to provide such protection.

Such an alternative is only permissible where the manufacturer supplies rules and guidance as to how the visual observation is to be deterred by the installation environment of the PED. These rules must be evaluated along with the device during the approval process and subsequently provided to all purchasers and prospective purchasers.

These rules and instructions provided by the manufacturer must clearly state that the acquirer must meet the implementation criteria. These rules must be binding for any acquirers placing the PED into service.

Q30. Which PIN Block formats are permitted for PEDs and SCMs use within IAC?

Clause 2.7 of the IAC Code Set, Volume 4, requires that PEDs may use any PIN Block format as defined in ISO9564.1:2017, except format 1 and that format 3 is preferred. Therefore a device must support more than ISO PIN Block format 1 in order to be approved for use within IAC.

Q31. May an Approved Evaluation Facility rely on the FIPS 140-2 certification when evaluating a Secure Cryptographic Module for use in a KIF?

Yes, only where the device in question has been deployed prior to 1 January 2012 and where the device is no longer produced or supported by the original device vendor (i.e. it is past “end-of-life” for production). The FIPS 140-2 certification, the device’s security policy and the content of the original FIPS test report, which must be made available by the vendor, may be used by the AEF to inform the findings for the security requirements as required by clause 3.1 of the IAC Manual, Volume 4: Device Requirements and Cryptographic Management.

The evaluation report must clearly show the origin of the data considered in the report, whether it is generated from tests or observations performed by the AEF or whether it is sourced from the FIPS 140-2 documentation. The AEF shall confirm that data sourced from a FIPS 140-2 report is fit for purpose when drawing conclusions as to the result for each security characteristic of the device.