IAC Security Audit – Frequently Asked Questions

Version 2.1 (Effective 1 March 2025)

This FAQ provides answers to questions regarding Compliance to the AusPayNet IAC Code Set and IAC Annual Security Audits. Terminology used in the FAQ are aligned with PCI PIN, PTS POI and PTS HSM, however clear differentiations should be understood in both the process and requirements.

A. General FAQ

A.1. Who can signoff an Annual Security Audit as an "auditor"?

The IAC Regulations or IAC Code Set does not define the term "auditor" used in Volume 1 of the IAC Code Set. AusPayNet considers the use of the term "auditor" in the context of the Annual Security Audits to be a person, internal or external, authorised by the Participant to carry out an independent review of the Annual Security Audit checklists. This person must have suitable knowledge and expertise in IT security and auditing procedures. There are no requirements that this person, authorised by the Participant, be a registered auditor or part of an internal compliance, risk or auditing division.

It is up to the Acquirer or Issuer to decide who is appropriately qualified to sign the Auditor Signoff.

A.2. Can an auditor be involved in the collection of evidence and coordination of technical teams?

No, the auditor sign-off must be independent of the preparation of the annual security audit.

A.3. Who can sign on an Annual Security Audit as a "business signoff"?

Business signoff of the annual security audit would normally be expected to be by a senior business manager responsible for the component of the business under audit.

A.4. What is the process that an auditor role participant should follow?

The following Six steps are a suggested audit process an auditor many utilise:

1. Obtain the completed relevant checklist from the IA Participant.
2. Select a representative sample of questions from the checklist, which should include questions that indicate both:
    a. non-compliance, and
    b. compliance with the IAC Code Set.
3. Perform a walk-through of each of the selected questions with the relevant staff, focusing on how they have assured themselves that the responses to the checklist are complete and accurate.
4. Where non-compliance is noted on a checklist, ensure that the IAC Participant have an adequate and timely action plan in place, including:
    a. remedial actions which will ensure future compliance to the Code Set;
    b. realistic and proper resolution time frames; and
    c. there exists a distributed responsibility of tasks.
5. Raise all concerns with the IA Participant and achieve satisfactory resolution/agreement.
6. The auditor should continually be asking the relevant staff as to:
    a. how they ensure compliance with the IAC Code Set; and

b. to provide evidence which demonstrates that their compliance control/monitoring procedures are operating effectively.

A.5. What is the audit obligation of IAC participants?

All IA Participants must complete an Annual Security Audit (as set out in the IAC Code Set Volume 1 Annexure A, once every calendar year. IA Participants must give AusPayNet prior written notice of the date by which they will complete their Annual Security Audit. The IAC Participant and external auditor must sign the audit once completed.

Failure to comply with IAC Code Set Volume 1 clause 3.2 requirement to submit an Annual Security Audit once every calendar year, six months after the end of that calendar year (by 30 June) is a breach of a Threshold Requirement.

Under the Regulations for the Issuers and Acquirers Community (IAC), the Issuers and Acquirers Forum (IAF) may designate specific requirements of the IAC Code Set as Threshold Requirements for compliance by IA Participants. The IAF has power under the IAC Regulations to impose fines on IA Participants for non-compliance with the Threshold Requirements, and to refer non-compliance to a Sanctions Tribunal.

A.6. What Third Party Providers are in scope for the audit obligations of IAC participants?

The IAC Code Set, Volume 1, Section 3.2.2 describes a third-party provider as an organisation that supplies services to a Participant which may or may not be directly connected to Interchange, that provides payment-related services, directly or indirectly, to an IAC participant and/or stores, processes or transmits payment-related data.

This payment data includes:

- Cardholder Data
- PIN Data
- Key material

A.7. If an IAC Participant has an existing AusPayNet exemption request, is the participant required to resubmit the exemption for the next audit?

Resubmission of exemption requests undergoing correction within the granted period is not required. The member must provide an update on the existing exemptions and exemption that is about to expire. Members must also supply an update on the progress of remediation, in accordance with project plans submitted to AusPayNet.

A.8. What are the key rotation intervals for Key Encryption Keys (KEK) and Session keys used in Interchange Links?

IAC Code Set Volume 4, Section 4.5.2 (b): "*Key Encrypting Keys must be changed at the request of the Interchange partner, or, as a minimum, once every two years" and "Session Keys must be changed, as a minimum, once every 2048 Transactions or once an hour, whichever occurs first"*

A.9. What is the difference between Interchange Links and Interchange Lines?

"Interchange Line" means the physical (including wireless) communications infrastructure that provides the medium over which Interchange Activity is supported. An Interchange Line contains, at a minimum, one Interchange Link.

"Interchange Link" means the logical link between an Acquirer and an Issuer which facilitates Interchange Activity between them. Interchange Links are supported physically by an Interchange Line, and are either direct between an Acquirer and Issuer or indirect via a third party intermediary.

A.10. Is it acceptable to use a KEK hierarchy, up to three levels, to facilitate key rotation?

The term 'KEK' is commonly used within AS2805 and the IAC Code Set to refer to a key encrypting key used to exchange session keys (including the PIN encryption key, MAC send key etc). With this definition, only the second-lowest layer in the key hierarchy will include KEKs. KEKs may be loaded encrypted under a parent key, thereby adding additional levels to the hierarchy. There is no prescribed limit to the number of levels in the key hierarchy.

For Interchange Links, there are several methods detailed in IAC Code Set Volume 4, Section 4.6, for introducing a KEK, namely:

- AS 2805.6.6 method;
- Native RSA key method;
- KTK method;
- KEK Component method.

Key management must comply with the requirements set out in the IAC Code Set Volume 4, Section 4.5.2.

For Interchange Lines, Key Management practices are outlined in the IAC Code Set Volume 4, Section 4.7.

A.11. Key management often relies upon manual key handling processes, including key ceremonies and storage of key components. Requirements in A.1.3, A.2.3 and A.3.3 apply to key management processes and require auditors to confirm such processes are being followed. What evidence needs to be shown to an auditor to confirm manual key handling processes are being followed?

It is impossible to list all possible scenarios where manual key handling processes are used. A few common examples are shown below

- Where keys are loaded into a HSM via components, then the auditor shall observe an actual or demonstration key ceremony. Consistent with test requirement 7-1.c from PCI PIN v3.1.
- Where plaintext components rely upon tamper-evident packages, the auditor shall be provided with a sample package to confirm the tamper-evident and anti-observation protections.
- Where keys are manually exchanged between organizations, then the auditor shall be shown completed logs, consistent with PCI PIN 7.2.c

A.12. Clause 3.1 from Code Set Vol 1 requires IA participants to ensure devices used in Interchange are approved for use within the IAC. How is the approval status of a specific device determined?

A device is approved for use within the IAC if it meets one of the following conditions and is not listed on the Revoked Devices List on the AusPayNet website:

1. Listed by an Approved Standard Entity as an approved device under an Accepted Standard (e.g. PCI PTS, PCI MPoC, NIST CMVP).
2. Listed by an Approved Standard Entity as an expired device under an Accepted Standard, has not passed its Sunset Date and was purchased prior to the Expiry Date.

3. Listed on the AusPayNet Approved Devices List on the AusPayNet website.
4. Listed on the AusPayNet Expired Devices List on the AusPayNet website, has not passed its Sunset Date and was purchased prior to the Expiry Date.
5. Pilot approved device with a letter of pilot approval issued by AusPayNet to the acquirer.

Conditions included as part of a device approval may be listed on the website and must be validated.

A.13. Can devices purchased during the Sunset Period be deployed and used in the IAC?

No, only devices purchased during the Approval Period can be deployed and used in the Sunset Period.

A.14. Why is a device previously registered and listed on the AusPayNet Approved Devices Page no longer visible?

Under the new Device Approval Process effective January 2025 all approval listings which are duplicates of an Approved Standards Entity listing have been removed from the AusPayNet Approved Devices List. Refer to the list managed by the Approved Standards Entity.

A.15. HSMs approved under PCI PTS HSM may include a global setting (commonly called PCI mode) where all HSM functionality complies with PCI requirements. Does compliance with the IAC Code Set require the HSM to operate in PCI mode?

No, the Code Set requires only that cryptographic operations used for IAC payments comply with the Code Set.

The use of PCI mode is encouraged, however is not required for compliance of AusPayNet requirements. If PCI mode is disabled, other HSM security options, including the option(s) enforcing minimum key length(s), shall be appropriately configured in compliance with all applicable requirements of the IAC Code Set.

A.16. Listings for PCI approved HSMs include the hardware, firmware and application (if applicable) version identifiers for the approved product. Must the hardware, firmware and application (if applicable) version numbers from the listing exactly match the deployed HSMs?

Hardware version must match the PCI listing. Firmware and application versions shall match the PCI listing, except when the difference is introduced by 'non-PCI mode' supported on certain HSMs. HSMs in non-PCI mode must be configured securely in compliance with all applicable requirements of the IAC Code Set. The assessor shall validate all other HSM security options being appropriately configured and examine other supporting evidence (e.g. key cryptograms demonstrating key lengths).

A.17. Does the IAC Code Set require AS2805.2 or AS2805.12 conformant message structure for card-present transactions?

No, other messaging formats are acceptable. The security and cryptography principles described in the Code Set shall be met, regardless of the messaging format used.

A.18. Does TLS encryption address the privacy of communications requirement?

There are two answers depending upon the type of communication link

For Terminal to Acquirer links using TCP/IP, Clause 3.2.4 in Code Set Vol 3 requires transport level message encipherment in addition to end-to-end financial message encipherment. TCP/IP Terminals therefore require TLS (or equivalent transport layer encryption) plus a second layer of encryption (e.g. AS2805.9 privacy encryption) to meet the Code Set obligations.

During Interchange, IAC Code Set Vol 3, Clause 2.4.9 specifically allows privacy of communications to be met with transport level data encryption, subject to a series of conditions. Where the combination of TLS design, key management practices and configuration settings addresses all applicable conditions, then TLS can be used to comply with Clause 2.4.4 – Privacy of Communication (for IAC Interchange Lines).

A.19. Can JSON Web Encryption (JWE) be used as a replacement for AS2805.9 compliant encryption for the privacy protection of payment messages used by TCP/IP terminals?

Yes, JWE can be classified as a type of point-to-point communications technique as defined in AS2805.9. The two layers of cryptographic protection required by Code Set Vol 3, 3.2.4 for TCP/IP terminals can be addressed by using TLS together with JWE. Not all options within JWE comply with Code Set requirements. For example, PBES2 password based key derivation systems do not typically meet the privacy requirements and cannot be used in an IAC compliant system.

A.20. Can JWE be used as the primary protection for session keys during transmission?

The code set includes the following requirements applicable to session key distribution

- Session keys are to be encrypted using the CBC mode of operation
- All PIN and MAC cryptographic functions (including encryption and decryption of session keys) must be performed within an approved device.
- A key (including KEK and session key) is used only for a single designated purpose

If a system using JWE to transport session keys can be shown to meet all applicable Code Set requirements, then it may be used for session key exchange.

A.21. AS2805.2 messages are known to comply with applicable IAC Code Set requirements. How is compliance of non-AS2805.2 messaging formats assessed?

Acquirers and Issuers are responsible for ensuring communications of card payment messages follow IAC Code Set requirements. The annual audit shall consider whether the communications mechanism in use complies with all applicable IAC Code Set requirements.

Code implementing payment messages is commonly included in the application layer, executing on either a payment terminal or a host server. This code is outside the scope of the device approval program therefore using an approved device provides no guarantee on whether the messaging format complies with IAC rules.

A.22. Can RESTful APIs be used for PIN transmission?

Code Set Vol 3, clause 2.3.1 requires plaintext PINs and related plaintext key material to be handled exclusively within approved devices. TLS and RESTful APIs are commonly handled by general purpose computers which are not approved devices and are therefore not suitable for handling of plaintext PIN material.

A PIN may only be transmitted as an encrypted PIN block output from an approved device. Clause 2.2 (e) requires online PIN blocks to comply with ISO 9564-1, excluding Format 1 and 2 but there is no restriction on the mechanism for transfer of encrypted PIN blocks.

A RESTful API may be used to transfer an encrypted PIN block but not a plaintext PIN block or plaintext PIN data.

B. Issuer Audit FAQ

B.1. Is PIN change within an Issuer owned environment in scope?

Yes, PIN change within an Issuer's environment is in scope as compliance with ISO 9564-1 is mandatory for all PIN related activities (see clause 2.1 of Volume 2).

B.2. Are issuing PIN activities outside of Interchange in scope of the IAC annual audit?

Yes, section A.3 of the annual audit applies to all issuing services associated with the management of PINs and the associated cryptographic practices. An example of these PIN activities is card personalisation for cardholder's PIN performed by a card manufacturer.

B.3. Is the use of Approved Devices required for issuing PIN activities outside of Interchange?

Branch terminal does not require to be an Approved Device. However, it is recommended to follow the device guidelines outlined in the IAC Code Set Volume 2, clause 3.6.1.

SCM used outside of Interchange functions, such as PIN change or PIN selection, must be an Approved Device as per requirement set out in IAC Code Set Volume 2, clause 2.2. The minimum Accepted Standards are NIST 140-2 or NIST 140-3 level 3 for these SCMs.

B.4. Are on-us transactions and cash deposits via a cash/coin counting machine to the cardholder's cheque or savings account in scope for the audit?

All "on-us" non-PIN transactions which are not routed via Interchange Links are not in scope for the audit.

Any cash/coin counting machines that have PIN entry functionality must be a secure cryptographic device in conformance with ISO 9564.1 but does not require AusPayNet/IAC approval. Note that the PIN must be encrypted when transmitted from the cash/coin counting machine. SCMs used for handling plaintext PIN values or PIN-related cryptographic keys must be approved as per Vol 2, Clause 2.2.

B.5. Does the scope of an annual audit include PINs used as a form of customer identification?

The IAC code set applies to all usage of PIN for both acquirer and issuer functions. The applicable questions in the AusPayNet Annual Security Audit should be applied for all usages of PIN, including those cases not directly associated with payment transactions, e.g. PIN Change.

B.6. Does this Audit include internal PIN-related key management and PIN related activities?

The IAC Code Set Volume 2, clause 2.1, requires Issuers to be compliant to ISO 9564.1. Unless specifically exempted by the Code Set, this includes all PIN related activities.

ISO 9564.1 requires compliance to ISO 11568 all parts (key management). Therefore, key management in respect of the annual audit includes all PIN key related activities including establishment, issuance, verification, selection, replacement and change.

B.7. Requirement A.3.1(f) states 'All parties to the interchange…maintain procedures and practices to prevent the unauthorised disclosure of Cardholder Data...'. Does the reference to interchange indicate the requirement _*only*_ applies to activities directly involving interchange (payment processing, settlement, disputes, etc.)?

No, the requirement applies to all cardholder security related activities for all parties connected to the interchange.

B.8. The Code Set, Vol 1, Part 2.1.1, requires all Devices (including NSTs and payment acceptance solutions) used in Interchange to have been approved by the Company. Can non-approved Devices be used for non-interchange purposes?

Yes, unless prohibited by a different requirement.

As an example, IAC Code Set Vol 2, Clause 2.2, requires SCMs handling or managing plaintext PINs and/or related keys to be Approved. This includes SCMs not involved in interchange.

Devices used for issuer functionality related to PIN over open networks (e.g. cardholder selected PIN change via a banking app) are not connected to interchange, and therefore do not require approved devices. Alternative requirements apply as detailed in IAC Code Set Vol 2, Part 3.

B.9. Do mobile banking apps with PIN change functionality need to comply with requirements in A.3.4 – General Security Control for PIN Usage over Open Networks?

Yes, PIN change via a mobile banking app is classified as Issuer functionality and the internet is a type of Open Network. The app, supporting backend systems and relevant procedures must comply with requirements in Annex A.3.4.

C. Acquirer Audit FAQ

C.1. Does the IAC Code Set Volume 3, clause 2.4.5 Privacy of Communications apply to ATM transactions?

No, this requirement applies only to EFTPOS terminals.

C.2. When a cardholder performs a 'balance inquiry' can the ATM store the PIN in secure memory, to be used for subsequent transactions?

EMV transactions currently allow this, and more specific requirements of the Code Set Volume 6, Annexure G.4.11 & G.4.12 noting that this is in contravention of PCI requirements.

C.3. Would on-us transactions that are not sent over an open network apply to AusPayNet Audit requirements?

No audit requirements will apply, however, there are a general IAC requirement for Issuers to comply with ISO 9564-1 : **Basic principles and requirements for PINs in card-based systems**

C.4. What is the scope of PAN security as required by the issuer audit?

The Issuer audit must consider PANs in the following situations:

1. Interchange links, where PANs must be encrypted as per A.3.1(h)
2. Systems handling PIN over open networks as per A.3.4

PAN can be excluded from the scope of the annual audit for issuer systems not listed above.

C.5. Requirement A.1.1(a) asks for a list of deployed EFTPOS terminals, SCRs and EPPs. The definition of terminal was changed in 2018 from a PIN entry device to any device used to accept card payment transactions. SCRs and other terminals without PED deployed prior to changes to the Code Set introduced do not need to be approved devices. Is it necessary to list such SCRs when completing the annual acquirer audit?

Yes, all card acceptance terminals connected to the payments network need to be listed as part of the annual audit. Where a device is exempted from being an approved device, a note should be added to the audit report under requirement 1.1(o) confirming the devices were deployed prior to the rule changes in 2018.

C.6. Clause 2.2(f) from Code Set Vol 3 requires ATM payments applications released after 2021 to have been reviewed by the Acquirer or a trusted third party and to have been shown to contain no security vulnerabilities or other security weaknesses. What types of evidence are sufficient to address this requirement?

The purpose of this requirement is to have an assessor review the ATM software. The requirement does not prescribe specific review techniques or evidence collection. A list of known acceptable techniques are listed below:

- A signoff form from the Acquirer confirming the ATM software has been reviewed and that no security issues were found.
- A penetration test performed by an independent assessor which did not find any significant security issues.
- A report showing evaluation of the software against an industry standard security program, for example PCI Secure Software Standard.
- Details of the software developer's security practices including the results of their security testing.

Other techniques offering equivalent assurance may also be considered acceptable.