Grant Thornton

PTS POI Security Requirement Change Analysis

Payments NZ Limited

June 2025

Table of contents

1 Executive Summary

Background

Background

Payments NZ is responsible for setting and overseeing the rules and standards that are central to the way payment instructions are exchanged and settled. In this role they are responsible for setting the standard for payment terminals that are approved to connect to the Consumer Electronic Clearing System (CECS) in New Zealand. In order to manage this approval, they utilise the PIN Transaction (PTS) Point of Interaction (POI) standards established by the PCI DSS Security Standards Council.

Payments NZ has engaged Grant Thornton to assist in the analysis and research of the threats and risks that the various PCI PTS POI standard changes are trying to address, to help inform their decision on what device standard should be applied in New Zealand.

Scope and Approach

Scope of Work

The scope of this engagement is:

- Conduct research on the variances between versions 3, 4, 5 and 6 of the PCI DSS PTS Standards.
- Provide a summarised analysis to Payments NZ of identified variances between versions 3, 4, 5 and 6 of the PCI DSS PTS Standards.

Disclaimer

This research has been completed based on the publicly available information. It does not constitute an assurance engagement under professional standards. Accordingly, we do not express any evaluation, opinion, or conclusion regarding PCI DSS PTS standards, nor their application by Payments NZ in the management of payment terminals. This report should not be relied upon for the purpose of demonstrating compliance with PCI DSS PTS standards.

Variance Between Versions 3 and 4

Risks and Vulnerabilities Highlighted by the Updated Requirements

Our analysis of versions 3.x and 4.x of the PTS POI Security Requirements identified that the variances between them mostly impacted the logical security requirements that devices must adhere to.

Logical security requirements concern the technical aspects and vulnerabilities of the devices. Physical security requirements (e.g., anti-tampering) remained largely unchanged.

Version 4 of the security requirements saw a complete restructure of sections related to logical security, as well as the introduction of new requirements related to cryptography, cryptographic key management, secure booting, and vendor security policy obligations. We also noted some updated physical security requirements related to tampering in transit & supply chain security.

Cryptography & Open Protocols

Version 4 saw a restructure and refresh of requirements for logical security in the ‘Open Protocols’ module of the requirements. This included amendments to requirements regarding the use of cryptography & trusted certificates, which demonstrated an increased focus on vulnerabilities arising from the use of internet protocols and system interfaces.

Vendor Policies

Version 4 introduced a requirement for vendors to develop a user-accessible security policy regarding secure use of their device, with respect to key management, device administration, functionality, and environmental requirements. Another requirement states the need for vendors to have internal policies and procedures for detecting vulnerabilities, which are effective enough to detect newly-introduced vulnerabilities as they arise.

Secure Boot & Update of Devices

Updates and additions to the ‘Core Logical Security Requirements’ section of the security requirements showed an increased focus on vulnerabilities from malicious software & updates. New requirements were introduced for authenticating software applications and updates, with another requirement amended to require that devices reinitialise memory daily as part of a measure to self-test for detecting compromises.

Supply Chain Security

Requirements for protecting devices in transit from manufacturers were updated in Version 4 to require stronger inspection procedures and tamper-evident features. This demonstrated an increased focus on securing the integrity of the device supply chain.

Variance Between Versions 4 and 5

Risks and Vulnerabilities Highlighted by the Updated Requirements

Version 5.x introduced a Secure Card Reader PIN (SCRP) approval class, and saw multiple deletions, additions, and amendments to the security requirements. Modules L & M from v4.x (manufacturing & supply chain security) became in-scope for testing by PCI laboratories.

Grant Thornton's analysis has determined that the risks and vulnerabilities addressed by these changes relate to the SCRP approval class, susceptibility of outdated firmware to emerging threats, side-channel POI compromises, manufacturing & supply chain security, and device authenticity. These are the areas which the updates placed the most emphasis on.

Aside from the above-noted modifications, the security requirements are largely similar to those of version 4.x.

New Secure Card Reader PIN (SCRP) Approval Class

The SCRP approval class is for the use of devices enabling software-based collection of PINs. Notably, an amendment was made to requirement D1 which specified higher-than-otherwise protections required from the new approval class. Requirement D1 states that SCRPs must withstand attack potentials of 26 and 13 for identification and exploitation, compared to 20 and 10 for other approval classes respectively.

Firmware Updates & the Evolving Threat Environment

Version 5 of the Security Requirements now specifies that device firmware must be updatable, allowing for new device protections to be proactively released and applied. In prior versions of the standard, this was not mandatory. This presented the risk that devices subject to emerging vulnerabilities were unable to be updated with the mitigations for new and evolving vulnerabilities.

Side Channel Attacks

Amendments made in version 5 addressed the vulnerability of side channel attacks, where information from a POI (e.g., power consumption, sounds) is used to derive sensitive information. This was through the higher attack potentials for the SCRP approval class on side channel related requirements, and amendments to clarify other requirements which aim to mitigate the risk of side channel attacks.

Device Authenticity & Supply Chain Security

The updated requirements included changes which sought to strengthen device authenticity checks. Inadequate device authenticity practices increases the risk that unauthenticated devices, potentially with malicious modifications made to them, enter the supply chain and allow for successful compromises of sensitive cardholder data.

Variance Between Versions 5 and 6

Risks and Vulnerabilities Highlighted by the Updated Requirements

Version 6.x introduced mandatory support for Elliptic Curve Cryptography (ECC) and a three-year firmware expiration requirement. It also permitted the use of magnetic stripe readers on commercial mobile devices, such as smartphones and tablets. This had previously been prohibited due to inherent security limitations of those platforms.

Grant Thornton's analysis further identified that other changes in the requirements address risks and vulnerabilities related to wireless communication channel attacks, application-layer attacks on open-platform devices, and deployment and lifecycle security.

Other than these updates, the security requirements remain largely consistent with those of version 5.x.

Mandatory support of Elliptic Curve Cryptography (ECC) in v6 chipsets

Mandating support for ECC in PCI PTS v6 enhances both security and performance by enabling faster cryptographic operations with shorter key lengths. ECC is increasingly used in EMV cards and digital wallets, and its adoption ensures that terminals remain compatible with these newer payment methods. Compared to legacy algorithms like RSA, ECC offers stronger protection against brute-force attacks and is more resilient in the face of emerging threats, including those posed by future quantum computing capabilities.

Firmware Expiration

The introduction of a three-year expiration period for POI v6 firmware ensures that devices remain aligned with current security expectations and are periodically reassessed in the context of evolving threats. By limiting the lifespan of approved firmware, the standard helps prevent prolonged use of outdated or vulnerable code that may not reflect new attack vectors or mitigation techniques.

Allow the inclusion of MSRs in SCRPs for use in SPoC solutions

The allowance for including magnetic stripe readers (MSRs) in Secure Card Readers for PIN (SCRPs) used in SPoC (Software-based PIN Entry on COTS (Commercial Off-The-Shelf)) solutions addresses the practical need for merchants to support fallback transactions where chip or contactless methods are unavailable. While MSRs were previously excluded due to their inherent security limitations, this change recognises that, with appropriate controls, magstripe acceptance can be supported without compromising the integrity of SPoC architectures. Strict requirements for data encryption, interface separation, and secure handling ensure that the inclusion of MSRs does not expose cardholder data or weaken the overall security posture.

Evolving Focus on Vulnerabilities

The shift in vulnerabilities addressed by the changes in Versions 4, 5, and 6

These vulnerabilities, and others addressed by the security requirements, are detailed in Section 5

Version 3 to 4

The risks and vulnerabilities focussed on by the new and amended requirements in 4.x were across the below 4 areas:

Communication & Protocol-Level Attacks

- Man-in-the-middle attacks.
- Replay attacks on transaction data.
- Cryptographic key exposure/misuse.
- Network-based key brute-force attacks.

Malicious Software & Firmware

- Unauthorised firmware installation.
- Firmware rollback attacks.

Physical Security & Device Interface Protection

- Debug Port Exploitation (JTAG/UART).
- Tamper grid bypass (drilling/probing).

Supply Chain Compromises

- Unsecured device shipment & deployment.
- Inadequate repair/maintenance security.

Version 4 to 5

The main update in Version 5 was the requirement that firmware on devices is updatable. Other amendments addressed side channel attacks and device authenticity. The vulnerabilities we noted as being addressed by these changes are:

Secure Firmware Updates & Lifecycle Integrity

- Emerging threats: Vulnerabilities that are unknown as of today, but could pose a threat to new & existing devices as they arise (vulnerability management program).
- Firmware rollback attacks.
- Unauthorised firmware installation.

Side-Channel & Fault Injection Resilience

- Side channel attacks.
- Fault injection attacks.

Device Authenticity & Supply Chain Security

- Inadequate repair/maintenance security.
- Unsecured device shipment & deployment.

Version 5 to 6

Version 6 introduced a 3-yearly expiry cycle for device firmware. This built on firmware-related requirement updates in version 5.x. Overall, the vulnerabilities that this version sought to address are:

Wireless Attacks

- Man-in-the-middle attacks over unsecured Bluetooth/Wi-Fi.
- Exploitation of unauthenticated wireless links.

Application-Layer Exploits

- Attacks from rogue or poorly isolated apps, or through shared resources on open platform devices.

Deployment & Lifecycle Tampering

- Device impersonation during merchant installation.
- Insecure repair/refurbishment.

Cryptographic Weaknesses

- Inability to process ECC-based cards and wallets.
- Increased exposure to brute-force and downgrade attacks using outdated RSA.

Summary of Analysis

Themes & opportunities identified across the version updates

This analysis of the variances in versions 3 to 6 of the PTS POI Security Requirements sought to identify the threats and risks that each update addressed. From this, we have identified a clear shift in focus toward firmware and supply chain risks.

Comparative to legacy devices, modern day payment terminals are better equipped to defend against physical security risks such as tampering, card skimming devices, and side channel attacks. This was evident through newer versions of the security requirements, which left physical security requirements largely unchanged.

Rather, updates to the requirements centered on the technical functionality of payment terminals. Key changes across the latest versions included version 5.x's requirement for device firmware to be updatable and version 6.x's 3-yearly firmware expiration cycle. These changes demonstrate that securing device firmware against emerging threats to be a key focus of the newer requirements.

Analysis of the vulnerabilities addressed by the version changes supports this theory, with a number of vulnerabilities identified being exploits of a terminal's firmware and logical functionality.

New and amended requirements for supply chain security were also present across the version updates. While physical security requirements address the risks of device tampering for devices already in use, updated requirements have sought to address the risk that devices are compromised ahead of entering the market.

Overall, phasing in devices compliant under versions 5.x and 6.x will better protect the New Zealand network of payment devices against firmware and supply chain related risks.

Payments NZ's quicker cadence of sunset dates comparative to other markets is understood to be necessary for enforcing the adoption of modern & more secure payment terminals. Where other markets with later sunset dates tend to pivot to newer devices at a similar cadence to New Zealand through the nature of their supply chain, such as Australia's bank-influenced device supply chain's device rollout cycle, New Zealand's switch to newer payment terminals comes through more stringent regulation.

It is however important to consider the security advantage version 6.x devices have through the 3-yearly re-assessment of device firmware. Coupled with the version 5.x-introduced requirement for firmware updatability, these devices are better placed to remain resilient against emerging threats over time comparative to earlier device versions, which tended to be static in nature.

We recommend that Payments NZ take into consideration the improved firmware security of version 5.x and 6.x devices when determining their respective sunset dates.

2 Version 4 Updates Analysis

Summary of Changes

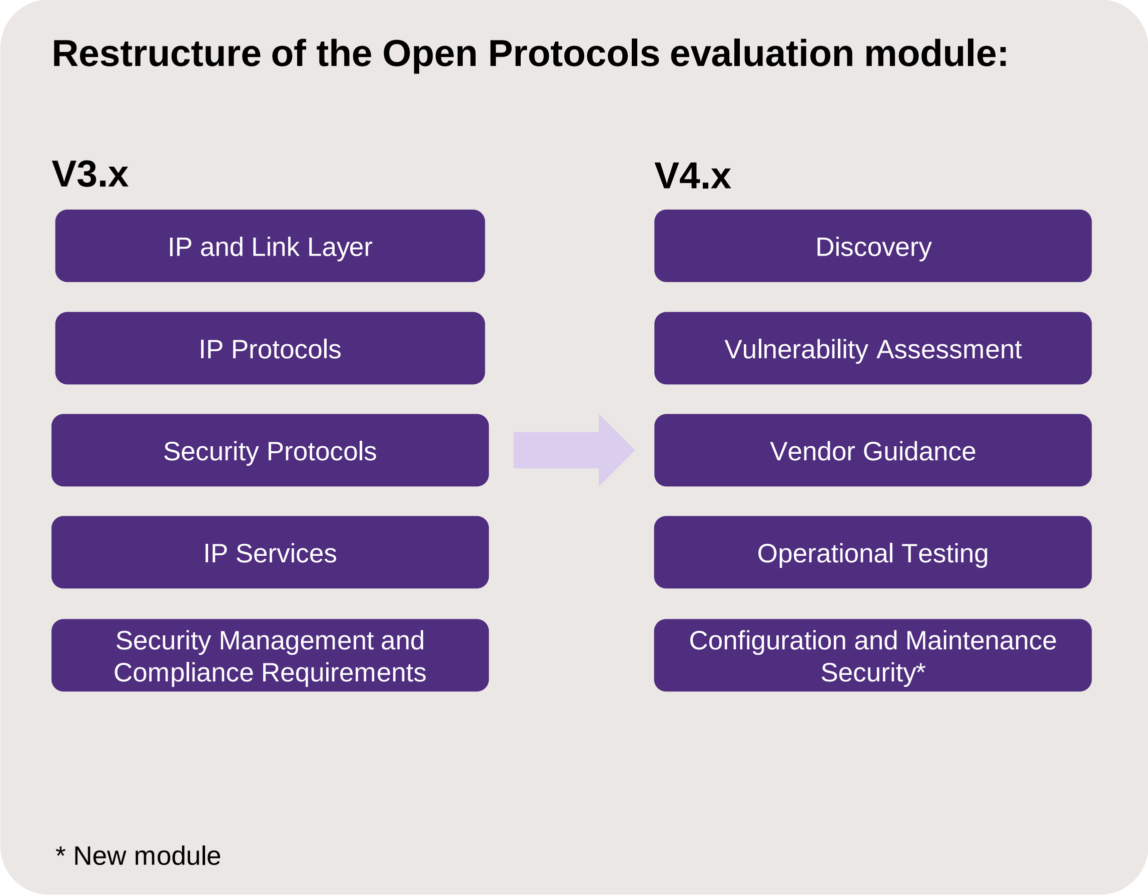
Risks and Vulnerabilities Addressed by Version 4 of the PTS POI Security Requirements

Changes made to Version 4 of the PTS POI Security Requirements demonstrated an increased focus on risks and vulnerabilities arising from the logical operations of payment terminals.

This is through the changes made to the Core Logical Security Requirements, and the full restructure of the Open Protocols module. Key themes of these changed requirements are authentication, confidential information management, and cryptography.

The ‘Derived Testing Requirements’ for Version 4 of the security requirements also demonstrated more stringent testing procedures which payment terminals are required to meet.

The following slides detail our analysis of newly introduced and amended requirements as to what risks and vulnerabilities these changes sought to address.



Restructure of the Open Protocols evaluation module:

V3.x

- IP and Link Layer
- IP Protocols
- Security Protocols
- IP Services
- Security Management and Compliance Requirements

V4.x

- Discovery
- Vulnerability Assessment
- Vendor Guidance
- Operational Testing
- Configuration and Maintenance Security*

* New module

Version 4 New Requirements

Risks and Vulnerabilities Addressed by New Requirements

Module & Sub Module	ID	Requirement Description	Associated Risks & Vulnerabilities
Core Requirements – Core Logical Security Requirements	B4.1	The firmware must support the authentication of applications loaded onto the terminal consistent with B4[1]. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.	The addition of requirement B4.1 specifically requires that software applications and their associated updates are cryptographically authenticated. This addresses the risk of malicious software being installed onto a payment terminal. Under this requirement, if software and associated software updates cannot be authenticated, then the device is to reject and delete it[1].
	B4.2	The vendor must provide a defined and documented process containing specific details on how any signing mechanisms must be implemented. This must include any “turnkey” systems required for compliance with the management of display prompts, or any mechanisms used for authenticating any application code. This must ensure: • The signing process is performed under dual control. • All executable files are signed. • Software is only signed using a secure cryptographic device provided by the terminal vendor.	Requirement B4.2 addresses vulnerabilities arising from unauthenticated software through the requirement for vendors to document processes which ensure the signing of executable files and that secure signing practices are followed. Unauthenticated software introduces risks that a payment terminal is compromised by malware. This is because inadequate authentication of software introduces the risk that malicious software is loaded onto a payment terminal.

[1] B4 states “If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.”

Version 4 New Requirements

Risks and Vulnerabilities Addressed by New Requirements

Module & Sub Module	ID	Requirement Description	Associated Risks & Vulnerabilities
Core Requirements – Core Logical Security Requirements	B20	A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions - i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.	The introduction of requirement B20 addresses the risk that misuse of a payment terminal by an end user exposes it to a security breach. Each of the responsibilities mentioned in B20 is a source of risk to a payment terminal if it is not managed in a secure fashion. For example, cryptographic keys play an important role in encryption, signing, and secure communication for payment terminals. Mismanagement of keys exposes a terminal to vulnerabilities such as replay attacks and man-in-the-middle attacks. These attacks have the potential to compromise sensitive cardholder data.
Open Protocols – Vulnerability Assessment	G1	The device vendor has internal policies and procedures that ensure that the vendor maintains an effective process for detecting vulnerabilities that may exist within their device. This process is expected to be robust enough to include all interfaces defined in requirement F1[1]. This process must be effective enough to detect vulnerabilities which may have not been publicly known during the last vulnerability assessment.	Requirement G1 was amended in the restructuring of the Open Protocols module to include new security requirements. Specifically, requirement G1 now mandates that vendors have vulnerability detection procedures which detect new vulnerabilities, i.e., those not already known at the time of a prior vulnerability assessment. This clause does not address any one vulnerability, but rather, seeks to ensure that vulnerability management practices remain fit for purpose in addressing evolving security threats to payment terminals.

[1] F1 states “All public domain protocols and interfaces available on the device are clearly identified in the Open Protocols Module – Protocol Declaration Form. All protocols and interfaces available on the device are accurately identified by the device vendor. The vendor has a complete and comprehensive understanding of how all protocols and interfaces present on the device interact..”

Version 4 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Core Requirements – Core Logical Security Requirements	B1	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.	Added the final sentence "The device must reinitialize memory at least every 24 hours."	The addition of the requirement to reinitialise memory daily ensures that the device's self-test for integrity and authenticity is run daily. Rather than directly addressing any one vulnerability, this requirement acts as a fail-safe in the event that a device is successfully compromised.
Open Protocols - Vendor Guidance	H2	The device has guidance that describes the default configuration for each protocol and services for each interface that is available on the device. Each interface and protocol on the device should default to secure settings. If the interface has the ability to be configurable to non-secure settings, vendor guidance should strongly recommend against configuring to non-secure settings.	This requirement now states the need for vendor guidance regarding default configurations of protocols and services.	Amendments made to requirement H2 demonstrate an increased focus on vulnerabilities arising from the use of internet protocols. Example vulnerabilities that this requirement addresses are: • Man-in-the-middle attacks. • Network-based brute force attacks. • Replay attacks. The amendment to H2 seeks to prevent devices from being configured insecurely by end users. Insecure device configurations expose the device to greater risk of a compromise through the above-listed vulnerabilities.

Version 4 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Open Protocols - Operational Testing	I1	The device has all the security protocols that are available on the device clearly identified in the Open Protocols Module – Protocol Declaration Form. The device vendor provides documentation that describes the implementation and use of the security protocols that are available on the device.	Requirement I1 now requires that vendors provide documentation regarding the implementation & use of security protocols.	As with other amendments made within the open protocols module, the update to requirement I1 continues a theme of requiring vendor documentation related to device security. The documentation now required by I1 is to inform end users of the device's security protocols. Rather than addressing any one vulnerability, this instead acts as a step to better inform device users of security configurations.
Open Protocols - Operational Testing	I4	The device uses a declared security protocol to authenticate the server. a) Server authentication utilizes key sizes appropriate for the algorithm(s) in question. b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. c) The device is able to verify the validity of the public keys it receives. d) The device is able to verify the authenticity of the public keys it receives. e) The device's trusted root certificate store shall contain only public key certificates from trusted CA's or else self-signed certificates verified by the acquirer.	List item e) now requires that certificates stored on devices are from trusted certificate authorities, or are certificates verified by an acquirer.	Requirement I4 addresses the risk that a device connects to a malicious or otherwise unauthorised server. This would expose the device to network-based vulnerabilities and allow for the disclosure of sensitive cardholder information if successfully executed. While the requirement was present in version 3 of the security requirements, the addition of list item e) demonstrates an increased focus on this vulnerability for the next generation of devices.

Version 4 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Device Management Security Requirements – Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment	M1	The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. Where this is not possible, the POI is shipped from the manufacturer’s facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.	Although version 3 of the standard included provisions for tampering in transit, the updated standard now includes the additional physical security measures of further tamper-evident features and customer inspection procedures.	The amendments to requirement M1 address the vulnerability of a supply chain compromise. The additional requirement within M1 for providing customers with the means to assess the authenticity and integrity of a POI act as a mitigation against a supply chain compromise, such as a POI being substituted with a malicious POI, or a POI being tampered with to allow the compromise of cardholder data (e.g., card skimming).

3 Version 5 Updates Analysis

Summary of Changes

Risks and Vulnerabilities Addressed by Version 5 of the PTS POI Security Requirements

Updates to the PTS POI Security Requirements identified in Version 5.x saw the introduction of a new approval class[1], the removal of 2 requirements, the addition of 2 requirements, and 5 notable amendments to pre-existing requirements.

Overall, the level of change was smaller than that of the prior version.

The updates to the security requirements addressed a key issue with prior standards, which was that firmware for devices was not required to be updatable.

The implication of this was that some devices could not process firmware updates that mitigated emerging vulnerabilities.

Another new requirement mandated tokenisation for the operation of SCRPs[1]. This is a means of protecting cardholder data from disclosure through network-based attacks.

Requirements L & M, which relate to manufacturing and supply chain security, also became in-scope for testing by PCI laboratories. In v4.x, these requirements were in place with an attestation-style approach to testing, to which the outcome did not influence final device approvals.

Other changes to the security requirements were minor adjustments which addressed device physical security, supply chain security, methods of device authentication, and a more stringent attack potential that SCRPs must be able to defend against for a requirement related to side channel attacks.

[1] SCRP: Secure Card Reader PIN, a newly introduced approval class. https://blog.pcisecuritystandards.org/new-pci-software-pin-entry-on-cots-standard

Version 5 New Requirements

Risks and Vulnerabilities Addressed by New Requirements

Module & Sub Module	ID	Requirement Description	Associated Risks & Vulnerabilities
Core Requirements - Core Logical Security Requirements & Secure Reading and Exchange of Data (SRED) - Account Data Protection *This new requirement is duplicated.*	B4 & K12	The device must support firmware updates. The device must cryptographically authenticate the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	The introduction of this requirement addresses the risk that devices cannot process updates and therefore are unable to protect against emerging threats and vulnerabilities using the latest mitigations. Under prior versions of the standard, it was not required for devices to support firmware updates. Overall, this change does not address any one vulnerability. Rather, it ensures that devices are designed such that devices can support updates which defend against emerging vulnerabilities as they arise.
Secure Reading and Exchange of Data (SRED) - Account Data Protection	K24	Secure enablement tokens are required from the SPoC[1] monitor system for operation of the SCRP[2].	Secure enablement tokens refers to a practice of using tokens to represent cardholder data & hence protect it from being disclosed. This new requirement mandates that where an SPoC monitor utilises an SCRP for pin entry, tokenisation must be used. This change addresses the risk that sensitive cardholder data, such as PAN (primary account number), is captured though network-based attacks which aim to capture sensitive data. An example of this is a man-in-the-middle attack.

[1] SPoC: Software-based PIN Entry on COTS (commercial off the shelf) devices

[2] SCRP: Secure Card Reader PIN, a newly introduced approval class

Version 5 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Core Requirements - Core Physical Security Requirements	A1	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader. Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario.	Minor changes. A requirement for attack times to require a minimum of 10 hours to succeed was removed. A requirement regarding the consideration of front and rear casings was introduced.	While physical security requirements remained largely unchanged in this version of the security requirements, the amendment made to requirement A1 addresses a physical security risk that a device's casing are replaced as part of a wider attempt at tampering with the device. Replacing the casings on a device could form part of a side channel attack, through the possibility that an attacker replaces casings in order to make modifications to the device to collect information to use in a side channel attack (e.g., power consumption monitoring). This demonstrates a minor change in requirements to better address the risk of tampering and side channel attacks.

Version 5 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Core Requirements - Offline PIN Security Requirements	D1	It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, nor is it possible for both an IC card and any other foreign object to reside within the card insertion slot. SCRPs shall require an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation.	Added the final statement regarding SCRPs, which specifies a higher threshold for identification and exploitation attack potentials.	The higher attack potential specified for SCRPs indicates that SCRPs are considered to be more susceptible than other approval classes to modifications for the purposes of capturing sensitive cardholder data. For example, a side-channel attack may seek to modify a device to aid with disclosing sensitive information.
Open Protocols - Vendor Guidance	H3	The device has guidance for key management describing how keys and certificates must be used. a) The key-management guidance is at the disposal of internal users and/or of application developers, system integrators, and end- users of the device. b) Key-management security guidance describes the properties of all keys and certificates that can be used by the device. c) Key-management security guidance describes the responsibilities of the device vendor, application developers, system integrators, and end-users of the device. d) Key-management security guidance ensures secure use of keys and certificates, including certificate status (e.g., revoked), secure download, and roll-over of keys.	Added the requirement in item d) that guidance addresses certificate status, secure downloads, and the roll-over of keys.	Version 4 of the security requirements included a stronger focus on security of devices through secure key management practices & the use of certificates. It also required that vendors better document guidance for the secure use of devices. This theme has continued in version 5 of the standard, with H3 being updated to specify the need for guidance on the secure use of keys, certificates, and downloads. This addresses the risk that poor device key and certificate management exposes the POI to a network based exploit such as a man-in-the-middle attack.

Version 5 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Device Management - During Manufacturing	L6	If the device will be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the device during manufacturing, this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device. Secret information is installed under dual control to ensure that it is not disclosed during installation, or the device may use an authenticated public-key method. Authentication by secret information will become mandatory in POI v6.	The requirement now allows the use of a public key authentication method.	The change to this requirement isn't strictly addressing any one vulnerability, but rather it allows an additional method of device authentication. This demonstrates an increased focus on device authenticity. It is noted that in version 6, the requirement of authenticating with secret information will be (is) mandatory.
Device Management - Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment	M1	The POI should be protected from unauthorized modification with tamper-detection security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time—such as the use of serialized tamper-evident packing for all devices with no tamper detection, in conjunction with thorough physical inspection (possibly including sampling of HW internals) upon reception. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement. In the absence of defined agreements stipulating otherwise, the POI vendor remains responsible.	Minor changes. Added clarifications regarding protecting the device from unauthorised modifications using tamper detection, and that vendors are ultimately responsible for compliance unless agreed otherwise.	This requirement has been strengthened to better address the risk of tampering within the supply chain. This is through the additional clarifications regarding tamper detection, and vendor responsibility for ensuring compliance with this supply chain security requirement. Grant Thornton notes this requirement was also strengthened in the change from version 3 to 4 to address the risk of a supply chain compromise.

Modules L & M

Newly-Tested Manufacturing & Supply Chain Security Requirements

Requirements in Modules L (During Manufacturing) & M (Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment) have previously been applied through an attestation-style approach.

This meant vendors needed to confirm through forms that their devices were meeting the requirements. Any non-compliance noted would require corrective action, but would not impact a device's final approval.

Under Version 5, the PCI Council has now required that PCI laboratories test these requirements.

Module L: During Manufacturing

Module L contains 8 security requirements applicable to the manufacturing process of devices.

This module addresses the risk that a device undergoes unauthorised modifications, either physically or to the device's firmware, prior to entering the supply chain.

This module addresses this risk through requirements such as secure storage of device firmware, tamper-evident packaging, and secure repair processes.

Module M: Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment

Module M contains 8 security requirements applicable to the security of devices in the supply chain.

The main vulnerability that this section addresses is tampering within the supply chain.

This could occur through unauthorised modifications to a device, or the substitution of a device with a malicious or otherwise unauthorised counterpart.

4 Version 6 Updates Analysis

Summary of Changes

Risks and Vulnerabilities Addressed by Version 6 of the PTS POI Security Requirements

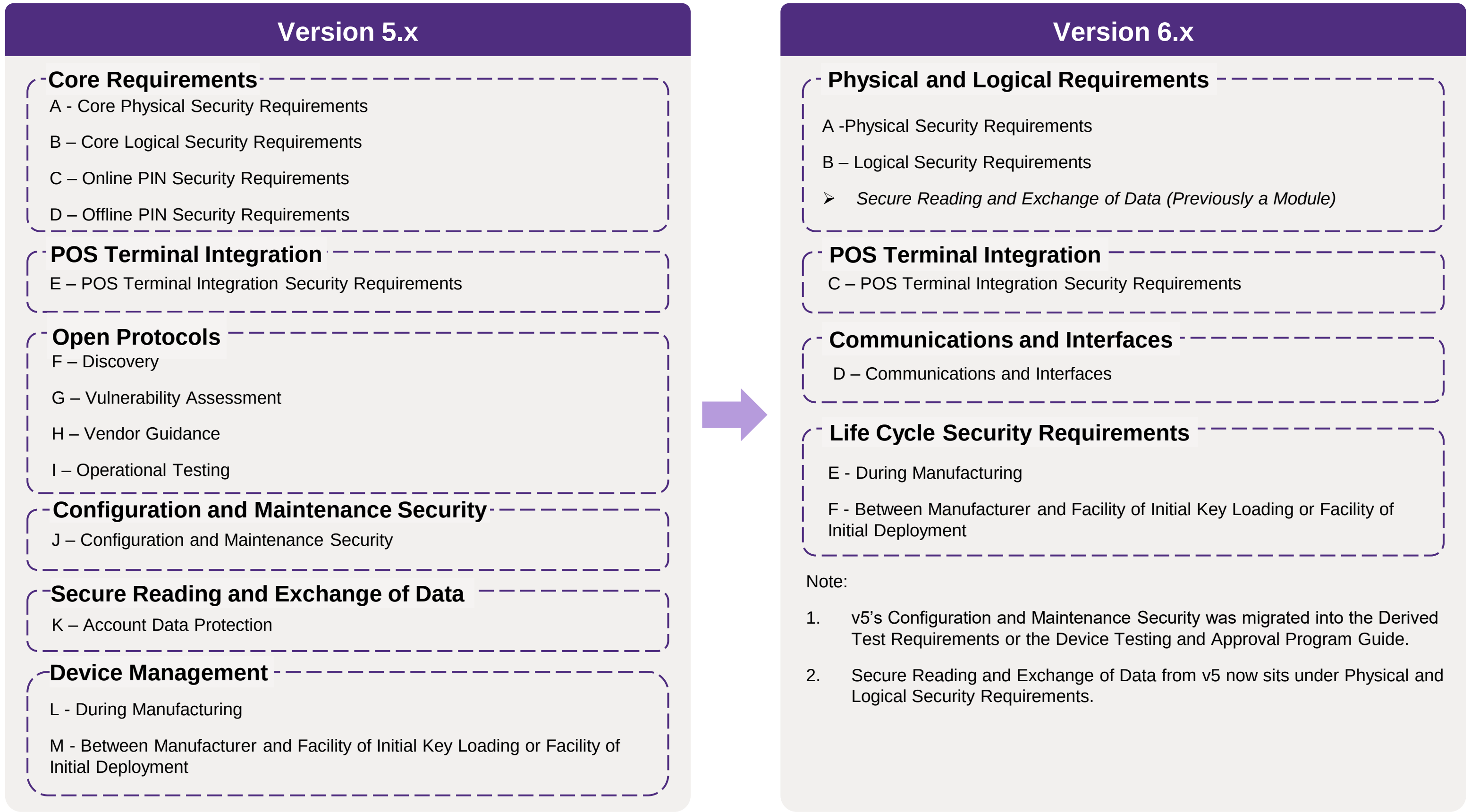
Changes to Version 6 of the PTS POI Security Requirements introduced a number of new features, including:

- Updates to the module structure, along with a reorganisation and renumbering of requirements.
- POI v6 chipsets must provide support for ECC (Elliptic Curve Cryptography) – a stronger cryptography to resist quantum risks.
- POI v6 firmware expires three years from the approval date but cannot expire after the device's overall approval expiration.

Version 6 introduced 2 new, 2 removed and 8 amended requirements.

The following slides detail our analysis of newly introduced and amended requirements as to what risks and vulnerabilities these changes sought to address.

Restructuring of the Security Requirement Modules:



Version 5.x

Core Requirements
A - Core Physical Security Requirements
B – Core Logical Security Requirements
C – Online PIN Security Requirements
D – Offline PIN Security Requirements

POS Terminal Integration
E – POS Terminal Integration Security Requirements

Open Protocols
F – Discovery
G – Vulnerability Assessment
H – Vendor Guidance
I – Operational Testing

Configuration and Maintenance Security
J – Configuration and Maintenance Security

Secure Reading and Exchange of Data
K – Account Data Protection

Device Management
L - During Manufacturing
M - Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment

Version 6.x

Physical and Logical Requirements
A -Physical Security Requirements
B – Logical Security Requirements
➢ *Secure Reading and Exchange of Data (Previously a Module)*

POS Terminal Integration
C – POS Terminal Integration Security Requirements

Communications and Interfaces
D – Communications and Interfaces

Life Cycle Security Requirements
E - During Manufacturing
F - Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment

Note:

1. v5's Configuration and Maintenance Security was migrated into the Derived Test Requirements or the Device Testing and Approval Program Guide.
2. Secure Reading and Exchange of Data from v5 now sits under Physical and Logical Security Requirements.

Version 6 New Requirements

Risks and Vulnerabilities Addressed by New Requirements

Module & Sub Module	ID	Requirement Description	Associated Risks & Vulnerabilities
Physical and Logical Requirements B – Logical Security Requirements	B16.1	If the device supports software with lesser security requirements or that is not developed by the vendor - e.g., applications - it must enforce segregation at least between different software security domains.	The introduction of this requirement addresses the risk that applications with lesser security requirements, or those developed outside of the device vendor's control, could interfere with or compromise sensitive payment functions. Without strict segregation of software domains, a lower-trust application could access payment data, disrupt secure operations, or introduce vulnerabilities through unintended interactions. By mandating isolation between different application domains, the requirement significantly reduces the likelihood of memory scraping, privilege escalation, or malicious application injection attacks that could otherwise lead to cardholder data compromise or full device takeover. This requirement is particularly critical for open platform POI devices, where multiple applications coexist on a single system (e.g., Android POS terminals).
Communications and Interfaces D – Communications and Interfaces	D14	Wireless communication interfaces which do not have specific security requirements, or have not met those requirements as listed, must be physically or cryptographically isolated. *Note: Where the security requirements in D12 and/or D13 for Bluetooth or Wi-Fi are not met, D14 must be met.*	The introduction of this requirement addresses the risk that insecure or unapproved wireless communication channels could be exploited to intercept sensitive data, inject fraudulent transactions, or compromise device integrity. By mandating that any wireless interfaces which do not meet defined security requirements must be either physically disabled or cryptographically isolated, the standard significantly reduces the attack surface exposed by embedded wireless technologies such as Bluetooth or Wi-Fi. This isolation prevents unauthorised wireless access paths from being leveraged to compromise payment security functions.

Version 6 Amended Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Requirement Description	Update	Associated Risks & Vulnerabilities
Physical and Logical Requirements B – Logical Security Requirements	B16.2	The vendor must provide clear security guidance consistent with D2 and B4 to all application developers to ensure: • That it is not possible for applications to be influenced by logical anomalies which could result in clear-text data being outputted while the terminal is in encrypting mode. • That account data is not retained any longer, or used more often, than strictly necessary. • That SRED functions, where provided, are correctly implemented.	Added the requirement in item 3) that security guidance for application developers must specify that SRED functions, where provided, are correctly implemented.	The introduction of this additional item addresses the risk that Secure Reading and Exchange of Data (SRED) functions - critical for the protection of sensitive cardholder data during capture - might be incorrectly implemented, partially bypassed, or inconsistently applied within devices. By explicitly requiring that SRED functionality, where provided, must be correctly and fully implemented, the standard ensures that cardholder data is immediately encrypted upon capture and remains protected throughout its lifecycle within the device. This reduces the risk of memory scraping attacks, cleartext data exposure, and unauthorised interception of payment information.
Physical and Logical Requirements B – Logical Security Requirements	B26	Secure enablement tokens are required from the attestation and monitoring system for the SCRP to accept and/or process payments.	Modified wording to address both SPoC (Software-based PIN Entry on Commercial off-the-shelf (COTS) Devices) and MPoC (Mobile Payments on COTS) and to clarify the enablement token impact.	The updated requirement tightens control over payment operations specifically, requiring devices to cryptographically prove integrity before accepting or processing cardholder data, while allowing limited non-payment operations to continue if enablement tokens are missing.

Version 6 Minor Changes to Requirements

Risks and Vulnerabilities Addressed by Amended Requirements

Module & Sub Module	ID	Update	Associated Risks & Vulnerabilities
Physical and Logical Requirements A – Physical Security Requirements	A1 / A2	Split requirement A1 into two separate requirements: 1) Tamper-Detection Mechanisms 2) Protection of Sensitive Keypad Inputs	This minor change does not address any new risk or vulnerability.
Physical and Logical Requirements A – Physical Security Requirements	A6 / A7	Split requirement A6 into two separate requirements: 1) Invasive Attacks for Cryptographic Keys 2) Non-invasive Attacks for Cryptographic Keys	This minor change does not address any new risk or vulnerability.
Physical and Logical Requirements B – Logical Security Requirements	B3	Combined B5 / A10 into a single requirement. A10: If PIN entry is accompanied by audible tones, the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit. B5: The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.	This minor change does not address any new risk or vulnerability.
Communications and Interfaces D – Communications and Interfaces	D12 / D13	Reference to D14 as alternate: D12: If Bluetooth is used, D14 may alternatively be used. D13: If Wi-Fi is used, D14 may alternatively be used.	This minor change does not address any new risk or vulnerability.

5 Vulnerabilities in Detail

Vulnerabilities in Detail

This section provides a summary of each vulnerability identified from the upgrades within Versions 4, 5 and 6 of the PTS POI Security Requirements.

The key themes of risks and vulnerabilities across the two updates were:

Version 3 to 4:

1. Communication & Protocol-Level Attacks
2. Malicious Software & Firmware.
3. Physical Security & Device Interface Protection.
4. Supply Chain Compromises.

Version 4 to 5:

1. Firmware Updatability.
2. Side-Channel & Fault Injection Resilience.
3. Device Authenticity & Supply Chain Security.

Version 5 to 6:

1. Wireless Attacks.
2. Application-Layer Exploits.
3. Deployment & Lifecycle Tampering.
4. Cryptographic Weaknesses.

Specific vulnerabilities that fall under these key themes have been analysed further for their potential impacts on payment security.

In total, we identified 32 main vulnerabilities which versions 3 to 6 of the PTS POI Security Requirements addressed.

Vulnerability descriptions and impacts, alongside detail of how the Security Requirements have changed to address these vulnerabilities over time are explored on the following slides.

Stagnant Firmware (No Ongoing Revalidation)

Secure Firmware Updates & Lifecycle Integrity

Description

Devices continue to operate indefinitely with old firmware, even after new vulnerabilities emerge or mitigations are developed. Without enforced expiration, outdated devices may remain in use long after security assumptions are no longer valid.

Impact

Persistent exposure to known vulnerabilities; firmware cannot be assumed secure after long periods.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Not Addressed

Version 5.x: Not Addressed

Version 6.x: Addressed

Current Risk Level

v4.x/5.x devices operating on unvalidated firmware beyond three years face high risk of exploitation through known vulnerabilities. Without revalidation, there is no assurance they remain secure against evolving threats.

Detail

Prior to v6.0, PCI PTS POI standards did not enforce expiration or revalidation of device firmware. While vendors were encouraged to patch vulnerabilities and release updates, there was no guarantee that firmware in the field was still being supported or had been evaluated against newer threats. Devices could remain operational indefinitely with unpatched bugs, expired cryptographic keys, or implementation flaws that were no longer acceptable under newer testing regimes. Attackers have historically exploited these gaps by targeting devices with known firmware versions and weaknesses.

PCI PTS v6.0 introduces a maximum three-year validity period for firmware approvals, forcing manufacturers to either revalidate their firmware or retire it from compliance listings. This change introduces an essential feedback loop between evolving threat intelligence and the certified security posture of deployed devices, closing a critical window that often led to real-world compromise of outdated terminals.

Real-World Example

2017 malware cases in Europe exploited five-year-old firmware with known weaknesses that were never patched.

Device Cloning/Impersonation (Deployment Authentication)

Supply Chain Compromises

Description

Weak or missing authentication during deployment and installation may allow attackers to replace legitimate devices with rogue or cloned ones.

Impact

Cardholder data theft, PIN harvesting, fraudulent transactions if a cloned device is deployed.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Not Addressed

Version 5.x: Not Addressed

Version 6.x: Addressed

Current Risk Level

Without secure deployment authentication, cloned or rogue devices can be introduced during installation, risking cardholder data theft. The impact could range from isolated incidents to mass compromise if systemic weaknesses exist.

Detail

In earlier versions of the standard (v4.x and v5.x), there were limited technical or procedural controls to prevent rogue devices from being introduced during shipment, staging, or merchant deployment. Physical tampering or cloning of devices could occur between the factory and the point of installation without robust detection or authentication mechanisms in place. This vulnerability was particularly critical in environments where merchant staff or field technicians had broad installation privileges and lacked methods to verify device authenticity.

Version 6.0 introduced stricter controls for the deployment chain, including secure pairing and registration processes, and v6.1 further enforced cryptographic authentication for wireless onboarding, making it significantly harder to impersonate devices. These measures reduce the risk of cloned or rogue terminals capturing PINs or PANs while masquerading as legitimate devices.

Real-World Example

2006 UK case where POS terminals were intercepted in transit and replaced with skimming devices.

Unsecured Wireless Communications

Communication & Protocol-Level Attacks

Description

Devices with wireless interfaces (e.g., Wi-Fi, Bluetooth) that do not require mutual authentication or strong encryption are exposed to remote attacks.

Impact

Remote hijacking, skimming, or manipulation of payment data via wireless channels.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Partially Addressed

Version 5.x: Partially Addressed

Version 6.x: Addressed

Current Risk Level

Devices with unsecured Bluetooth or Wi-Fi remain vulnerable to remote hijacking, transaction injection, and credential theft, particularly in public or semi-controlled environments. Moderate risk in v4/v5 deployments where wireless functionality is often enabled for ease of use, but lacks hardening.

Detail

Earlier PCI PTS versions placed only minimal focus on the risks posed by embedded wireless communication modules like Bluetooth and Wi-Fi. Many POI devices included these interfaces for service, telemetry, or peripheral connection without enforcing strong authentication or encryption. In such cases, attackers could exploit wireless channels to inject transactions, capture sensitive data, or interfere with device operation - particularly when Bluetooth pairing was left open or unprotected.

v6.1 introduced Requirement D14, which mandates mutual authentication and strong encryption for all wireless communications before the interface is allowed to participate in any sensitive process.

This shift recognises the growing trend of attacks leveraging wireless vectors and ensures that only trusted and verified wireless endpoints can interact with payment devices.

Real-World Example

2017 "BlueBorne" vulnerability[1] allowed attackers to compromise Bluetooth stacks across millions of devices, including POS terminals.

[1] BlueBorne vulnerability description: https://en.wikipedia.org/wiki/BlueBorne_(security_vulnerability)

Application Isolation Failure in Open Platform Devices

Communication & Protocol-Level Attacks

Description

POI devices using Android or Linux-based systems allow third-party apps to run, potentially exposing payment functions to poorly coded or malicious software.

Impact

Application-layer attacks, data leakage, bypass of encryption or user interface controls.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Not Addressed

Version 5.x: Partially Addressed

Version 6.x: Addressed

Current Risk Level

Open platform devices lacking strong app segregation are highly exposed to memory scraping, privilege escalation, and internal data leakage through rogue or poorly coded apps. Moderate risk for v4/v5 open platform devices, especially if apps are added or updated post-deployment without revalidation.

Detail

Open platform POI devices, such as those running Android or Linux, introduced a powerful but risky architecture where third-party or merchant-developed applications could coexist with core payment functions. In v4.x and v5.x, there were some controls around application signing and code validation, but these were often insufficient to prevent poorly coded, vulnerable, or even malicious apps from accessing sensitive components or weakening the device's secure environment. Attackers could exploit shared memory spaces, lack of process isolation, or insufficient runtime permissions to bypass encryption, leak data, or alter transaction logic. In v6.0 and further clarified in v6.2 (especially via Requirements B16.1 and B16.2), the standard introduces a robust framework for software domain segregation, secure APIs, and enforcement of SRED functions across all application contexts. This ensures that even in multi-app environments, no untrusted software can undermine core payment security.

Lack of ECC Support

Secure Firmware Updates & Lifecycle Integrity

Description

Devices that support only RSA-based cryptography may not be able to process cards or mobile wallets that require Elliptic Curve Cryptography (ECC). ECC provides equivalent or greater security with shorter key lengths and better performance, especially for resource-constrained devices.

Impact

Inability to process certain EMV cards; weaker cryptographic strength over time; possible downgrade attacks.

Security Requirement Versions

Version 3.x: N/A

Version 4.x: N/A

Version 5.x: N/A

Version 6.x: Addressed

Current Risk Level

Devices without ECC support can still process most EMV cards and mobile wallets today, as RSA fallback remains widely available to maintain compatibility. However, relying solely on RSA results in weaker cryptographic security, increased processing overhead, and reduced resilience against emerging threats, including potential quantum computing risks. Over time, as ECC adoption grows and fallback paths are eventually phased out, RSA-only devices may face interoperability issues or forced replacements. The immediate risk is not transaction failure, but continued exposure to older cryptographic methods that may become vulnerable faster than devices are retired.

Detail

In v4.x and v5.x, payment devices could be certified without support for Elliptic Curve Cryptography (ECC), relying solely on RSA-based mechanisms. However, RSA requires longer keys for equivalent security and is significantly less efficient, particularly in constrained hardware environments like mobile or handheld POS terminals.

The global EMV ecosystem is steadily shifting to ECC-based cryptographic operations due to ECC’s superior performance and its robustness against brute-force attacks. More importantly, some EMV cards and mobile wallets now use ECC-only certificates, which cannot be verified on RSA-only devices. Without ECC, these cards may be rejected or fallback to insecure magstripe processing, introducing fraud risks and causing interoperability failures. v6.0 mandates ECC support for all IC interfaces, closing a critical futureproofing gap and aligning with long-term cryptographic migration plans, including those driven by emerging quantum computing threats.

Inadequate Repair/Maintenance Security

Supply Chain Compromises

Description

The process for repairing or refurbishing devices being conducted insecurely (e.g., swapping a broken part or resetting a tamper after service in an insecure manner).

Impact

An attacker could pose as a service technician or exploit the repair process to disable tamper sensors or insert malicious components, then return the device to service. Alternatively, after legitimate repairs, the device might not be properly resealed or tested, leaving it vulnerable.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Not Addressed

Version 5.x: Partially Addressed

Version 6.x: Addressed

Current Risk Level

Version 4.x devices remain exposed to the risk that inadequate or insecure maintenance procedures may compromise their security. Since the v4.x standard does not include explicit requirements for post-repair validation or secure servicing processes, the integrity of a device following maintenance largely depends on the security practices voluntarily implemented by vendors and users. It is noted that actual risk is likely minimal where entities operate secure maintenance processes as enforced by the latest versions.

Detail

This area was formally addressed starting in versions 5.x. Earlier versions did not lay out requirements for post-repair validation. Version 6.2 introduces requirement E9 (vendors must have controls over repairs at all authorised facilities). This includes strict procedures for resetting tamper mechanisms (so that the device is just as secure after a repair) and mandatory inspection/testing after any repair to ensure no unauthorised modification was made during the process. For example, if the device's circuit board is replaced, it must be re-tested to determine whether all security features (tamper switches, encryption keys, etc.) function correctly and no new debug ports or code have been introduced. Under v5.x, the Device Management requirements implied some of the above items (PCI may have provided guidance to check devices after service, possibly in vendor questionnaires), but they were not explicit Security Requirement line items until v6.

Real-World Example

Service-Tech Impersonation (2008)[1] – In Ireland, criminals pretended to be POS repair technicians and installed Bluetooth skimmers inside PIN pads. Because there were no strict controls or post-repair validation at the time, the attack went unnoticed until fraud occurred. This type of incident illustrates why formal repair security procedures (added in v6) became necessary.

[1] Service-Tech Impersonation: https://murdoch.is/papers/ieeesp09tamper.pdf

Inadequate Vulnerability Disclosure & Response

Other Risks and Vulnerabilities

Description

No formal channel for reporting and distributing information about vulnerabilities in the device.

Impact

If a security researcher or user finds a flaw in a POI device, a lack of disclosure procedures could delay fixes or leave stakeholders uninformed. Similarly, without defined response, mitigation might not reach the field in time.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Partially Addressed

Version 5.x: Partially Addressed

Version 6.x: Addressed

Current Risk Level

Devices approved under versions 4.x and 5.x are more likely to be breached through a newly-discovered vulnerability. This is because inadequate vulnerability disclosures could result in slower response times for developing and releasing mitigations.

Overall, this leaves these devices more vulnerable to emerging threats than their version 6.x counterparts.

Detail

This issue is addressed in later versions of the security requirements. Version 3.x did not include requirements on how vendors handle vulnerability disclosure. Version 4.x through requirements J2 & J3 implicitly encouraged timely communication by requiring vendors to “promptly classify and provide mitigation” for new vulnerabilities, but publicly this wasn’t very specific. Version 6.2 added an explicit requirement for vulnerability disclosure measures (E12). Under this, a vendor must have documented procedures for distributing information on newly found vulnerabilities in a timely manner, including identification, description, risk assessment, and mitigation measures or fixes.

Essentially, by version 6.x, vendors need a clear policy (often a public-facing one) for notifying customers or users about security issues and providing updates or instructions to address them. Version 5.1 did not yet explicitly call this out (though many vendors did have PSIRTs by then), version 6 however did.

[1] PSIRT: Product Security Incident Response Team

Firmware Rollback Attacks

Secure Firmware Updates & Lifecycle Integrity

Description

An attacker loads a legitimate but older device firmware version with known flaws to undermine a device’s security.

Impact

An attacker could downgrade the device firmware, which in turn reintroduces patched vulnerabilities to a device.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Partially Addressed

Version 5.x: Partially Addressed

Version 6.x: Addressed

Current Risk Level

For v6.x-certified devices, rollback risk is significantly reduced through enforced update authentication and anti-replay mechanisms. However, devices certified under v4.x or v5.x remain exposed if those controls are not properly implemented or firmware updates are not enforced.

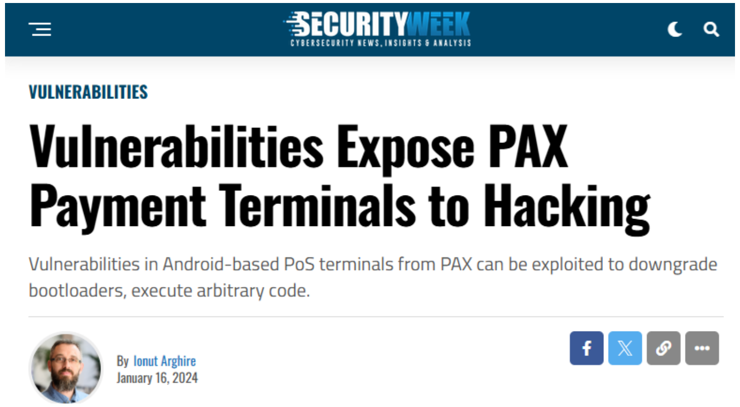
Version 6.x further strengthens protections by enforcing firmware revalidation and expiration, making it significantly harder for attackers to exploit old firmware even if rollback is technically possible.

Detail

Later versions of the security requirements require secure update mechanisms that prevent the use of outdated code. In version 4.x, firmware authenticity checks were required if updates were supported, but devices could opt out by not supporting updates. Version 5.x explicitly mandated field-updatable firmware with cryptographic authentication, ensuring patches can be applied and preventing insecure downgrades of firmware.

Furthermore, a derived testing requirement was introduced for anti-replay attack protections in update protocols (to reject replays of old update files), which mitigates the threat of a firmware version rollback. It is noted however that the PTS POI security requirements don’t explicitly forbid downgrades.

Real-World Example



SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

VULNERABILITIES

Vulnerabilities Expose PAX Payment Terminals to Hacking

Vulnerabilities in Android-based PoS terminals from PAX can be exploited to downgrade bootloaders, execute arbitrary code.

By Ionut Arghire
January 16, 2024

Bootloader Downgrade (2023) – A flaw in PAX A920 (CVE-2023-4818) allowed downgrading the bootloader to a vulnerable version. This kind of attack is exactly what modern secure update processes aim to prevent[1].

[1] Security Week article: https://www.securityweek.com/vulnerabilities-expose-pax-payment-terminals-to-hacking/

Man-In-The-Middle (MITM) Attacks

Communication & Protocol-Level Attacks

Description

Interception or alteration of data in transit between the POI and external systems (or between internal modules).

Impact

An attacker could eavesdrop or inject commands (e.g., between PIN pad and ICC reader, or on network communications).

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

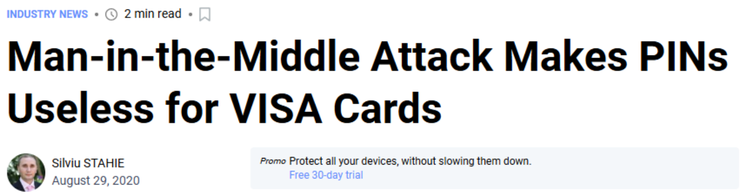
Version 5.x: Addressed

Version 6.x: Addressed

Detail

In v3.x, the optional Open Protocols module required encryption/authentication for public network interfaces. Version v4.x then integrated strict network security requirements, e.g., authenticated encryption for PIN transmission between PIN entry and ICC reader and use of up-to-date TLS/secure protocols. Under v4.x, a device must validate certificates, use strong ciphers, and resist known network attacks. By v4.1c, open protocols testing procedures ensured no known protocol vulnerabilities (like SSLv3/TLS1.0 weaknesses) remain. Versions V5.x/V6.x continue to enforce mutual authentication and encryption for any network interface, closing MITM vectors.

Real-World Example



INDUSTRY NEWS • 2 min read •

Man-in-the-Middle Attack Makes PINs Useless for VISA Cards

Silviu STAHIE
August 29, 2020

Promo Protect all your devices, without slowing them down.
Free 30-day trial

A 2020 article from security firm Bitdefender[1] detailed how a vulnerability in a the EMV protocol used for PIN authentication could be exploited to nullify the requirement for PINs.

The vulnerability, discovered by researchers, affected cards issued by VISA.

[1] Bitdefender Article: https://www.bitdefender.com/en-us/blog/hotforsecurity/man-in-the-middle-attack-makes-pins-useless-for-visa-cards

Replay Attacks on Transaction Data

Communication & Protocol-Level Attacks

Description

Reusing intercepted transaction data or commands to fraudulently repeat a transaction or spoof a device response.

Impact

An attacker could attempt to replay a PIN block or payment authorisation message to trick either the terminal or host system.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

The device and protocols incorporate nonces (numbers used once) and/or timestamps and sequence checks to foil simple replay attacks. In version 3.x, basic anti-replay capability was provided by host systems and the card networks, but the POI standard itself addressed it primarily via the Open Protocols module. Version 4.x introduced explicit language that any network update mechanism must include replay detection. Additionally, secure channel protocols required in versions 4 & 5 ensure each session or command is fresh (e.g., using unique session keys or random challenges).

By version 6.2, any data transmitted externally (PIN, account data, firmware updates) uses authenticated encryption or one-time challenges, as reflected in derived testing requirement rules for secure session management and exception handling. Therefore, a version 4+ device is better equipped to defend against replayed data. (Note: Replay of offline PINs is prevented by the ICC card's ARQC/ARPC cryptogram mechanism, which is outside the POI scope).

Real-World Example

EMV "Pre-play" Attack (2011) – A real attack, which has taken place on the HSBC card in 2011 on Malta and exploited predictable nonces to replay transaction cryptograms on Visa cards.

Later confirmed by the research "Chip and Skim: cloning EMV cards with the pre-play attack" by Computer Laboratory, University of Cambridge, UK[1].

[1] University of Cambridge research: https://www.cl.cam.ac.uk/~osc22/docs/preplay_oakland14.pdf

Unauthorised Firmware Installation

Malicious Software & Firmware, Device Authenticity

Description

Loading malicious or unapproved firmware onto a device.

Impact

An attacker could replace device software with backdoored code to capture PIN numbers and other sensitive data.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed (by multiple measures)

Detail

All versions require cryptographic firmware authenticity checks, but this requirement has evolved over newer versions of the security requirements. Version 3.1 had a requirement to authenticate updates (requirement B4) if firmware was updateable, but non-updatable devices were allowed (thus no mechanism for injection, but also no ability for patching). Version 4 made secure firmware loading a standard, by which the device must verify digital signatures of firmware and reject any that fail authenticity. However, version 4.x still allowed a device to forgo updates entirely.

Version 5.1 closed that loophole by mandating support for secure firmware updates. Under v5.1, every device must accept updates and rigorously authenticate them. By v6.2, the update process uses integrity, mutual authentication and replay resistance. Unauthorised firmware cannot run without breaking the device’s cryptographic signature checks (an extremely high attack burden).

Real-World Example

Verifone Firmware Signature Bypass (2019) – A vulnerability, presented by researchers during Blackhat Europe 2020 conference[1], which allowed installing unsigned firmware packages on Verifone MX series terminals (CVE-2019-14713)[2], which could let attackers load malicious code.

[1] Stennikov Research: https://i.blackhat.com/eu-20/Thursday/eu-20-Stennikov-POSWorld-Should-You-Be-Afraid-Of-Hand-Ons-Payment-Devices-wp.pdf

[2] CVE-2019-14713: https://nvd.nist.gov/vuln/detail/CVE-2019-14713

Malicious App Injection (Insecure Updates)

Malicious Software & Firmware

Description

Loading of a rogue application onto an open-platform POI (or modifying an existing app) through an update process that lacks proper security.

Impact

A fraudulent app could log PINs, transmit data, or otherwise compromise the device from within.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed (by multiple measures)

Detail

The POI strictly controls software updates and application installation. Versions 4.0+ introduced requirements for secure application loading. By v4.1c, devices supporting multiple applications must authenticate all apps similar to firmware (requirement B2.1). The vendor is required to have a code-signing process (requirement B2.2) with dual control, ensuring only vetted, signed applications can run. Version 3.1 did not explicitly cover downloading third-party apps (few v3 devices ran extensible operating systems), which presented a gap.

In version 4.x, an open-architecture POI had to enforce code signing and provide guidance to integrators to use the vendor's signing tools. Version 5.1 continued this and made firmware/app update support mandatory, further emphasizing the importance of patching vulnerabilities. In version 6.2, any application code must be signed by the vendor's approved secure cryptographic device. There is effectively no method to inject unauthorised code or apps without possession of the vendor's signing keys (a process weakness outside of a device's control).

Real-World Example

PAX PoS Code Signing Flaw (2020)[1] – An update signature verification bug (CVE-2020-28891) allowed bypassing integrity checks on PAX S920 POS terminals. An attacker with access to the update interface could run unauthorised code, illustrating why strict code-signing is critical.

[1] PAX PoS Code Signing Flaw: https://global.ptsecurity.com/about/news/vulnerabilities-fixed-in-pax-pos-terminals-could-be-exploited-to-commit-fraud

Inadequate Vulnerability Management Program

Secure Firmware Updates & Lifecycle Integrity

Description

Absence of a proactive process by the vendor to monitor and address new vulnerabilities in their product.

Impact

New exploits (e.g., novel side-channel techniques or protocol flaws) may emerge after a device is approved; without vendor action, deployed devices remain at risk.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Version 3.1 had no explicit requirement for ongoing vulnerability monitoring or patching. Once approved, a device's security upkeep depended on the vendor's voluntary efforts. Version 4.1c introduced a new mandate (Requirement J2) for a vendor vulnerability detection and mitigation process. Per this, vendors must continuously monitor public vulnerability sources, perform security analyses, and test their devices against newly discovered threats. They are expected to promptly develop mitigation (e.g., patches, firmware updates or protective guidance) for any pertinent issues. This effectively requires a Product Security Incident Response Team (PSIRT)-like function for vendors. Version 5 sustains this requirement, making it an integral part of the device's lifecycle management (and by v5, testing labs and the PCI SSC were planning site inspections to verify such processes).

Version 6.2 (requirements E10 & E11) continued to enforce robust vulnerability management such that the vendor must demonstrate an effective process for detecting vulnerabilities (covering all device interfaces, per requirement D1) and that they perform thorough vulnerability assessments (including public domain searches and penetration testing). In short, from v4 onward it's "Yes" – vendors are required to actively stay ahead of threats and update their devices as needed.

Evolving Threat Environment

The NIST National Vulnerability Database contained examples of recently discovered vulnerabilities for specific brands of payment terminals.

For example, vulnerability CVE-2023-42134[1] is a 2023-discovered vulnerability affecting some devices issued by payment terminal provider PAX. The vulnerability allowed for an attacker to overwrite device code by gaining physical device access.

[1] NIST NVD for CVE-2023-42134: https://nvd.nist.gov/vuln/detail/CVE-2023-42134

Cryptographic Key Exposure/Misuse

Communication & Protocol-Level Attacks

Description

Any design that could lead to secret keys or PINs being exposed in the clear, or used in a way that weakens their security.

Impact

Any design that could lead to secret keys or PINs being exposed in the clear, or used in a way that weakens their security. Examples: Exporting a key in plaintext or under an attacker-controlled wrapping key; using the same key for multiple purposes (violating key separation); or allowing arbitrary data encryption that might leak information about a key.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

These fundamental principles have been in place since v3.x. A device must never output a secret or private key or any clear PIN, nor allow keys to be output under less secure parameters (version 3 had requirements K8 & K9 for this). Versions 4.x and v5.x continued the same rules: for instance, an encryption key cannot be output or used to wrap another key that could be taken off-device (requirement B13), and the device cannot encrypt random data under a PIN key or data key (which prevents using the device to test keys). All account data encryption keys, PIN encryption keys, etc., must be distinct and only used for their defined purpose. The standard also insists on industry-approved algorithms and key sizes only (no proprietary or weak ciphers). By v5.x, the introduction of key blocks further ensures that any key loaded or exported uses a standardised, secure format.

Real-World Example

PAX D210 Key Extraction (2020)[1] – A chain of vulnerabilities in a PAX D210 allowed attackers with physical access to extract encryption keys and sensitive data from the device.

[1] PAX Key Extraction: https://global.ptsecurity.com/about/news/vulnerabilities-fixed-in-pax-pos-terminals-could-be-exploited-to-commit-fraud

Network-Based Key Brute-Force Attacks

Communication & Protocol-Level Attacks

Description

Using the device as an oracle to brute-force cryptographic keys (e.g., by sending numerous encrypted messages or PIN blocks to see if the device will decrypt them with a guessed key).

Impact

If a POI exposed an interface to test large numbers of key guesses, an attacker might eventually derive encryption keys.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

A POI does not provide any interface to perform arbitrary cryptographic operations with secret keys. All versions enforce that sensitive keys (PIN, account keys) cannot be used to encrypt attacker-provided data or divulge test results that would aid a brute force attack. From version 3.x onward, key-management is per ISO standards (ISO 11568 & ANSI X9.24) and requires use of strong keys (TDES/AES). Versions 4.x & 5.x explicitly require that devices use unique keys, and that there is no key usage that would allow outputting known plaintext/ciphertext pairs for an unknown key. For example, a PIN-encrypting key cannot be repurposed to encrypt arbitrary data (requirement B12), and secret keys cannot be exported or wrapped in a weaker form (requirement B13). These measures, present throughout versions 3 to 6, mean the device never acts as a useful oracle for key guessing. An attacker would have to break the cryptography offline, which with mandated key lengths (double-length TDES/AES) is computationally infeasible.

Debug Port Exploitation (JTAG/UART)

Physical Security & Device Interface Protection

Description

Abuse of internal debug/service interfaces (like JTAG, SPI or serial ports) to extract secrets or manipulate the device.

Impact

If an attacker can access an exposed debug port (often by opening the casing), they might read firmware or memory, alter code, or disable security features.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

POI devices are designed so that test interfaces cannot be used without significant effort. Version 3.x required physical tamper resistance such that opening the device (i.e., to get at circuit boards/pins) triggers zeroization[1] (requirement A1). Additionally, any attempt to disable tamper mechanisms or inject a keylogger via internal ports needed a high attack potential (requirement A2). In practice, manufacturers in the version 3 era would remove or lock JTAG pins (often via epoxy or firmware lock bits). Version 4.x and above formalised this via evaluation, whereby labs must identify all hardware interfaces (derived testing requirement D1) and ensure no interface yields sensitive data or control without authorisation. Unused debug ports must be securely deactivated or protected. By v6.2, sensitive functions and data are confined to protected hardware areas that cannot be accessed or modified via external connections without at least a 26-point attack effort. Thus, exploiting JTAG/UART is infeasible under the required protections.

Real-World Example

Verifone Debug Backdoor (2019)[2] – Researchers found an undocumented debug mode in Verifone VX devices (CVE-2019-14715) that allowed memory writes via the bootloader. Exploiting it required opening the device, but on older hardware without proper port disabling, this kind of access was possible. Modern devices epoxy or lock down such ports. Detailed report was presented during Blackhat Europe 2020 conference.

[1] Zeroization: Securely erasing data

[2] Stennikov Research: https://i.blackhat.com/eu-20/Thursday/eu-20-Stennikov-POSWorld-Should-You-Be-Afraid-Of-Hand-Ons-Payment-Devices-wp.pdf

Tamper Grid Bypass (Drilling/Probing)

Physical Security & Device Interface Protection

Description

The use of physical penetration techniques that avoid triggering tamper sensors – e.g., drilling a small hole to cut around the tamper mesh or micro-probing a circuit board to extract data.

Impact

Device tampering allows an attacker to access internal components or data without the device zeroizing[1] itself, therefore enabling them to capture sensitive information.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

The device uses extensive tamper-detection covering all sensitive areas, and any penetration attempt causes key erasure and device shutdown. All versions require robust anti-tamper meshes and responses. Version 3.1 set a high bar through requiring devices to withstand an attack potential of ≥26 for penetration of a device by methods such as drills and disassembly (requirements A1 & A2). Version 4.x reinforced this by requiring multiple layers of protection, until version 5.0, which removed the explicit “two independent mechanisms” wording but kept the equivalent security level.

The device’s sensitive areas (keys, PIN mechanics) are enveloped such that drilling, cutting, or probing will either hit a responsive circuit or be so complex as to be impractical. Versions 5.x & 6.x devices maintain hardened enclosures (with sensors for light, casing open, drilling attempts, etc.). For example, the standard enumerates drills, lasers, solvents, and other physical attacks that the device must resist (requirement A1). In short, any attempt to bypass the tamper grid or mesh will result in immediate zeroization of secrets and a bricked device, unless the attacker expends unrealistic resources.

[1] Zeroization: Securely erasing data

Unsecured Device Shipment & Deployment

Supply Chain Compromises

Description

Weaknesses in controlling the device's security from the manufacturer to the point of initial deployment – e.g., lack of tracking, unauthenticated deliveries, or no way for the recipient to verify device integrity.

Impact

This opens the door to supply chain attacks, where a device could be tampered with or swapped before installation (implanting bugs or malware while in transit or storage).

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Partially Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Current Risk Level

While version 4.x does not fully address this issue, the risk posed is low. This is because the difference between versions 4.x and 5.x is that testing labs now assess supply chain security requirements, without any major variances in the actual requirements. Devices in theory should still be adhering to the same requirements, with a weaker level of assurance for this under version 4.x.

Detail

Over time, the PCI SSC has tightened supply-chain requirements. Versions 3 and 4 were largely similar through their "Device Management" section, with updates to requirement M1 strengthening authenticity and integrity checks in the supply chain. By v5.0, this became assessed part of the device lifecycle. Both v5.x & late v4.x updates require that devices are shipped under strict control. Furthermore, version 6.2's requirement F1 requires that if a device lacks active tamper-detection during shipping, it must be sent in serialised tamper-evident packaging and thoroughly inspected upon receipt.

Every party in the distribution chain must maintain auditable controls and handoff logs for each device. The vendor must provide documentation to customers on how to check the device's authenticity and integrity upon delivery (such as verifying holograms, seals, or a digital certificate).

Version 6.x also mandates that each device has a unique visible identifier (model/serial) that can be queried electronically (requirement F7) to support traceability. Moreover, version 6.2's requirement E7 requires that the device is authenticated at the initial key-loading or deployment facility using a unique secret or an authenticated public key installed at manufacture – ensuring that a rogue device would be spotted because it cannot authenticate.

Real-World Example

Supply-Chain Attack (2008)[1] – UK Police discovered criminals had inserted GSM eavesdropping modules into card terminals during manufacturing, which then sent PINs/card data via SMS to attackers. Dozens of tampered terminals were shipped to retailers undetected. This real case prompted the industry to require tamper-evident packaging, chain-of-custody logs, and device authentication on delivery (implemented by v5.x and later).

[1] Telegraph Article (paywalled): https://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html

Side-Channel Attacks (Power/EM)

Side-Channel & Fault Injection Resilience

Description

Exploiting unintentional emissions (power draw, electromagnetic radiation) from the device to derive secrets like PINs or keys.

Impact

An attacker with specialized equipment could capture PIN entry or cryptographic keys via signal analysis.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

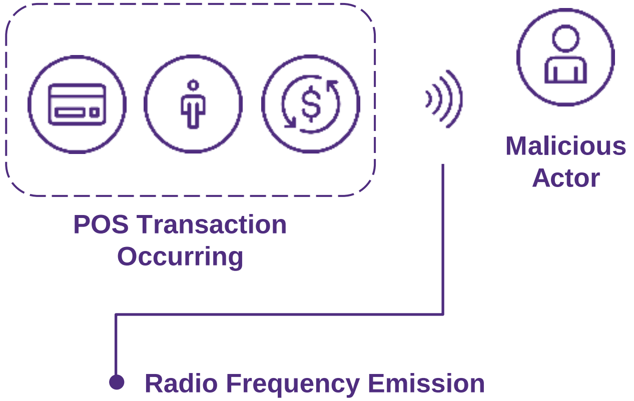
Version 5.x: Addressed

Version 6.x: Addressed

Detail

The security requirements raise hardware and firmware requirements to block side-channel leakage. Version 3.x set a baseline attack potential threshold (an attack potential of ≥26) for extracting keys via tampering or side-channel, but did not explicitly detail emanation testing. Version 4.x made side-channel resistance an area of focus – test labs were given detailed guidance to probe for PIN disclosure via emissions. Devices must be designed so that monitoring power, RF, or other emissions cannot feasibly yield any PIN digits (requirement A5) or cryptographic keys (requirement A7). Version 5.x continued these criteria with updated evaluation techniques, and v6.x devices are verified against advanced side-channel tools. All keys (PIN and account) require high attack effort to obtain via leakage, effectively foiling power analysis or EM intercepts.

Side-Channel Attacks in Practice



POS Transaction Occurring

Malicious Actor

Radio Frequency Emission

As a user enters their PIN number, the device releases radio frequency emissions. A device with improper side channel attack mitigations may do so in a way that allows the PIN to be derived by the attacker (e.g., the emission is different for each number).

PIN Harvesting via Acoustic/Timing

Side-Channel & Fault Injection Resilience

Description

Inferring PIN values by analysing acoustic signals (beeps) or timing information during PIN entry.

Impact

If each pressed key produced a distinguishable sound or timing pattern, an attacker could covertly record them to figure out the PIN.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

The Security Requirements ensure PIN entry feedback is uniform. Version 4.x added specific guidance to prevent acoustic leakage, whereby if the device provides audible tones for keypress, each PIN digit should sound identical. Under the requirements, a device never displays PIN digits (instead, they display masked information such as "***"). Furthermore, version 4.x test procedures included tests trying to discern PINs via sound or other side channels. Notably, version 3.x had no explicit acoustic requirement (some v3 devices had different tones for different keys, a weakness addressed in later versions).

By version 5.x, the uniform PIN entry tone and timing requirement remained, and labs also consider more subtle side channels during testing. The timing of PIN entry (which is largely user-dependent) is not something the device can randomise, but because the device provides no distinct feedback per key (and no difference in processing time that is observable externally), an attacker gains no advantage from this information. In summary, from v4 onward the POI ensures that nothing audible or externally observable distinguishes one PIN digit from another, defeating audio/timing PIN spying.

Real-World Example

"PinDrop" Acoustic Attack (2022)[1] - Researchers demonstrated that the sound of different keys on an ATM keypad can be profiled to infer PINs. With a microphone 30 cm away, they recovered 94% of 5-digit PINs. PCI v4's requirements for uniform audio feedback directly counter this: modern terminals use identical tone (or no tone) for each keypress, foiling such attacks.

[1] PinDrop Attack: https://par.nsf.gov/biblio/10427383-we-can-hear-your-pin-drop-acoustic-side-channel-attack-atm-pin-pads

Memory Scraping Malware

Other Risks and Vulnerabilities

Description

Malware on a device attempts to scrape sensitive data (PIN, PAN, keys) from memory buffers after entry.

Impact

Cleartext cardholder data could be harvested if it lingers in RAM.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

PCI mandates minimal retention of sensitive data. Version 3.1 required that PINs be encrypted immediately, and PIN buffers cleared after use (e.g., v3.1 B6), but residual non-PIN data might not have been explicitly covered. Version 4.x broadened this, such that devices must clear all sensitive buffers once a transaction completes or times out. SRED-approved version 4 devices encrypt account data at entry or confine it to secure memory. Versions 5.x & 6.x maintain these requirements, such that online PINs encrypt immediately, and full track data or temp values are automatically erased post-use, thwarting memory-scraping malware. Daily self-tests (introduced in version 4) with memory re-initialisation every 24 hours also ensure no malicious code stays resident indefinitely.

Fault Injection Attacks (Glitching)

Other Risks and Vulnerabilities

Description

Using sudden voltage drops, clock glitches, or other induced faults to make a device behave insecurely (e.g., bypass a check or spill secrets).

Impact

An attacker with physical access to a device could momentarily disrupt normal operation to disable security features or force error conditions that reveal data.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Devices must tolerate abnormal conditions without compromising security. Version 3.x had a generic requirement that environmental or operational extremes (out-of-range voltage, temperature, etc.) “cannot be used to undermine security”, but specific fault-injection scenarios (inducing glitches to leak data) were not explicitly tested. Version 4.1c introduced a dedicated requirement (e.g., K19) that a device must not output clear data even if subjected to such extremes or malfunctions. In practice, this means sensitive processes have robust error handling – a drop in voltage or overclock event will cause the device to fail safe (e.g., reset or crash) rather than operate in an insecure state. Versions 5.x & 6.x continue to enforce this; combined with tamper sensors (e.g., voltage/temp detectors), the device resists glitch attacks that could otherwise bypass cryptography or access controls.

Brute-Force PIN Guessing

Other Risks and Vulnerabilities

Description

Attempting to guess a cardholder's PIN by trying a high volume of different combinations.

Impact

If a device allowed unlimited PIN entry attempts (especially offline PIN), an attacker could eventually discover a PIN.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

PCI POI devices include features to deter exhaustive PIN trials. Version 3.x already required characteristics to prevent PIN brute-force attacks (such as requirement B10). For example, tamper-responsive PIN pads that erase keys upon physical disassembly, and/or firmware-enforced attempt counters or delays. Version 4.x maintained this, such that the device must make exhaustive PIN determination impractical. This can be achieved by limiting PIN entry tries, adding time delays, or locking out if too many incorrect PINs are entered. Versions 5.x & 6.x uphold the same protection. As a result, using a POI device to systematically guess PINs (online or offline) is not feasible without an extremely high attack potential.

Brute-Force PAN/Account Data Guessing

Other Risks and Vulnerabilities

Description

Using the device to iteratively test account numbers or magnetic stripe data in search of valid details.

Impact

An attacker might attempt to have a device verify or reveal information about large sets of primary account numbers (PANs) or other account data.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Versions 4.0+ explicitly added requirements to thwart using the terminal for exhaustive searches on account data. V4.1c introduced a new SRED requirement (K18) that the device have mechanisms to prevent automated PAN guessing. For instance, a device might rate-limit card reads or incorporate firmware checks to detect and abort sequential or rapid-fire transactions.

Version 3.1 had no explicit anti-PAN-bruteforce rule (only PIN attempts were considered), so a non-SRED version 3 device might be misused in this way. Versions 5.x and 6.x continue to include this protection (now integrated into core requirements), ensuring that attackers cannot use the device to test large numbers of PANs and learn which ones are valid based on how the device responds.

Physical Skimming (Internal Implants)

Other Risks and Vulnerabilities

Description

Installation of clandestine hardware inside a device to collect card data (e.g., a wiretap on the magstripe reader or PIN keypad).

Impact

A criminal could insert a thin tapping device or “shim” to record magnetic stripe data or PINs, bypassing external tamper sensors.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

A device’s design and tamper detection mechanisms prevent adding any such eavesdropping implant without triggering alarms or requiring an inordinate attack effort. Version 3.1 introduced “Secure Reading and Exchange of Data (SRED)” as an optional module, mandating encryption of account data at capture or protecting the data path. Thus, a version 3.x SRED-approved device encrypts all card data upon entry or keeps it in a secure module where wiretapping is ineffective.

Even without SRED, core physical requirements in versions 3.x and 4.x state that there is no way to intercept clear-text card data inside the device without fully compromising its security (requirement A10). Version 4.x & 5.x devices continued to integrate tamper-responsive enclosures and encrypted reading for magstripe and chip. For example, the card reader integration must not allow any “bug” to snoop data between the reader and secure controller (requirement A12). Version 6.2 maintains these protections, whereby any attempt to tap the card data lines or insert a foreign object in the card slot will either be detected or require an attack above the acceptable threshold.

Weak Random Number Generation

Other Risks and Vulnerabilities

Description

The use of predictable or low-quality random numbers in security functions (e.g., cryptographic key generation, challenge nonces / numbers used once).

Impact

A poor random number generator could allow attackers to predict values like encryption keys, authentication codes or one-time PIN challenges, hence undermining device security.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Later versions of the security requirements demand stringent randomness assessments than their predecessors. Version 3.1 required that any security protocol using random numbers employs a “high-quality” random number generator (noting that the testing lab would verify basic randomness), but the criteria for this were less formal. Version 4.1c added an explicit requirement that if the device generates random numbers for security, the random number generator must be assessed to ensure outputs are sufficiently unpredictable (requirement B7). This brought random number generator testing in line with recognised security standards (e.g., NIST SP 800-22/90 tests). Versions 5.x & 6.x continue to enforce robust random number generator quality such that version 4 & 5 documentation highlights compliance with stricter validation of randomness. Therefore, the risk of exploiting predictable random outputs (for example, to guess session keys or PIN pads’ responses) is mitigated in version 4-and-onward devices.

Inadequate Application Separation

Other Risks and Vulnerabilities

Description

One application on the device interfering with or snooping on another due to insufficient isolation (relevant for devices supporting multiple applications beyond payment).

Impact

A non-payment app or malware could steal PAN/PIN data or keys from the payment app or alter the device operating system.

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Multi-application POI devices must enforce strict separation of execution and data spaces. Version 3.1 already required that if multiple applications are present, they cannot tamper with each other or the operating system (version 3.1 had requirement B17 for this). Version 4.1c carried this forward (requirement B17 in v4.x) and further emphasised that any prompts or user interface elements used by one app (especially for PIN entry) must be controlled by the secure kernel to prevent spoofing by another app.

By versions 5.x & 6.x, this principle is firmly entrenched; devices provide hardware/enforced logical partitions between applications (e.g., memory segregation, hypervisors or privilege separation). The operating system itself must be minimal and run with least privilege to reduce the device's attack surface. All versions from version 3.1 onward address this, but versions 4+ had more explicit test evaluations. A rogue or third-party app thus should not be able to access sensitive resources of the payment application.

Environmental (Voltage/Temperature) Manipulation

Other Risks and Vulnerabilities

Description

Manipulating the device’s environment beyond normal operating ranges (extreme temperatures, overvoltage, undervoltage) to defeat security mechanisms. This is related to fault injection, but also long-term stress.

Impact

This vulnerability could cause the device to malfunction in a way that disables security (e.g., clock slowdown at low temperature might cause a device to skip a self-test for compromises).

Security Requirement Versions

Version 3.x: Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

A device must remain secure under all specified environmental conditions. Version 3.x already required that no security compromise occurs from subjecting the device to out-of-spec conditions through a core physical security requirement. Version 4.x expanded testing on this front, as noted, including the K19 requirement against fault-induced data leakage. Additionally, devices often include environmental sensors. For instance, if voltage goes out of bounds, the device may reset or error out rather than continue operating in an unsafe state. Versions 5.x & 6.x continue to mandate resilience. Under these versions, the device should either operate securely or fail secure under temperature, voltage, or other environmental stress (and not, for example, inadvertently revert to factory mode or reveal data). This overlaps with both physical tamper (to detect prolonged extreme conditions) and fault tolerance. All versions rate this as “No” feasible attack under the required attack potential for devices to withstand.

Hidden / Undocumented Functions (Backdoors)

Other Risks and Vulnerabilities

Description

Device firmware containing undocumented features or backdoor code that could be exploited (e.g., a hardcoded maintenance passcode, test mode that outputs keys, etc.).

Impact

Attackers (or malicious insiders) could leverage these hidden functions to compromise a device with little effort.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Starting with version 4.0, the security requirements explicitly address software backdoors. Version 4.1c introduced a requirement that the firmware is reviewed and certified free of any hidden or unauthorised functions (and added corresponding testing). Vendors must follow documented change-control procedures to ensure no unvetted code is present.

Version 3.1 did not explicitly call this out – it relied on lab scrutiny and vendor attestation, but there was no formal requirement for code review of “hidden features.” By version 4.x, testing labs examine source code and development documentation to confirm there are no secret features or debug modes left enabled. Versions 5.x & 6.x carry this forward (version 6’s requirement E2 requires a documented process certifying the firmware is free of hidden functions). Therefore, the presence of backdoor code is actively checked and considered a failure against the requirements from version 4 onward.

Development & Release Process Gaps

Other Risks and Vulnerabilities

Description

Weaknesses in the vendor’s development lifecycle – e.g., lack of change control, code signing discipline, or secure build processes – can introduce vulnerabilities (accidental or intentional).

Impact

Security features might be negated by inconsistent version control or unvetted code (e.g., a developer could insert a backdoor, or a fix might be lost in an update).

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Version 3.1 had basic change-control, such that any security-relevant change required re-certification, but it did not require proof of an ongoing vulnerability management or code-integrity program. Versions 4.0/4.1c significantly strengthened this. Under these, vendors must maintain formal configuration management and integrity controls for all hardware/software components (introduced as new Section J1 in v4). The vendor needs comprehensive documentation of how to securely configure and maintain the device through its lifecycle and ensure that any change affecting security results in a new version identifier.

Additionally, version 4.x added a requirement for code review, whereby the firmware must be inspected and certified as being free of hidden or unauthorised functions (meaning the vendor implements security code reviews and audits). By versions 5.x & 6.x, these practices are well-established. Version 6.2’s E1 & E2 mandate auditable change control and firmware inspection processes. Version 6.x also includes development environment security (requirement E8) – requiring the vendor to document and follow strict security measures in their development and maintenance facilities to protect design integrity. In summary, since version 4 the PCI PTS program expects a mature SDLC, such that very firmware build is under dual-control signing, every change is tracked, and no code goes in without review.

Lack of User Security Policy

Other Risks and Vulnerabilities

Description

The deploying entity (merchant, bank, etc.) is not given guidance on how to use and manage a device securely.

Impact

Even a secure device can be undermined by operational errors – e.g., not inspecting for tampering, improper key loading, or using it in unsupportive environments – if the end user is not adequately instructed on secure device management.

Security Requirement Versions

Version 3.x: Not Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Starting in version 4.0, the PCI SSC mandated that vendors provide a User Security Policy document. Version 3.1 had no such requirement. Although some vendors provided already manuals, these did not consistently cover security practices. Version 4.1c added requirement B20, requiring that a user-available security policy must be published for each device. This policy (often listed on the PCI website) instructs customers on the secure usage of the POI, including key management responsibilities, device handling, operational environment requirements, role definitions, and approved functions. It ensures merchants and integrators know how to maintain the device's security, addressing items such as periodic inspections for tampering and proper password management for admin functions.

Versions 5.x and 6.x continue this requirement (requirement E20 in version 6 corresponds to the security policy). In essence, since version 4.0, every device comes with a formal security policy to aid in the prevention of process weaknesses on the user's side. Under versions without it like v3.x, there was a risk of inconsistent or poor operational security. With it (versions 4+), stakeholders are much better informed on secure device management.

Inadequate Lifecycle & Configuration Documentation

Other Risks and Vulnerabilities

Description

A lack of comprehensive documentation and secure procedures for device configuration throughout the device's lifecycle (from manufacturing to deployment).

Impact

Without proper documentation, integrators or deployers may misconfigure a device (e.g., enable insecure interfaces, use default passwords, or install it incorrectly), or might not understand how to maintain a device's security over time.

Security Requirement Versions

Version 3.x: Partially Addressed

Version 4.x: Addressed

Version 5.x: Addressed

Version 6.x: Addressed

Detail

Requirements for documentation and guidance have expanded. Version 3.1 had some integrator guidance (B19 required the vendor to provide guidance for integrating secure components) but this was limited. Version 4.1c added Section J1, obligating the vendor to maintain extensive configuration and maintenance guidance covering all aspects of the device (firmware, applications, settings, keys, etc.). This documentation must delineate how to securely configure the device in all phases (development, manufacturing, delivery, installation, and operation). It must assert that if the documented procedures are followed, no unauthorised modifications are possible. Importantly, version 4's requirement J1 also stated that any security-relevant change (e.g., a firmware update that fixes a vulnerability) must result in a new device identifier/version, so that customers can distinguish devices with different security patches. In versions 5.x and 6.x, these requirements persist, and are folded into Life Cycle sections E and F. By version 6.2, the vendor must provide not only the user security policy for end-users, but also integrator guidance (requirement B19 in v6) for integrating components and all necessary info to maintain security. Additionally, version 6's E8 and E10 ensure that the development and production processes are documented in a way that security is preserved through the device's lifecycle.

Grant Thornton