Payment Card Industry (PCI)

PTS POI Security Requirements

Technical FAQs for use with Version 6

November 2020

Contents

POI Device Evaluation: Frequently Asked Questions

These technical FAQs provide answers to questions regarding the application of PCI's (Payment Card Industry) physical and logical POI device security requirements as addressed in the *PCI PTS Point of Interaction Device Security Requirements* manual. These FAQs provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered during the evaluation process.

Updates: New or questions modified for clarity are in **red.**

General Questions

Q 1 **If a device application includes prompts for non-PIN data and the device enforces PCI Requirement B15 compliant controls, can it be listed as an acquirer-controlled prompts device with the application excluded from the device identifiers?**

A *Yes, if an application cannot impact any of the functionality needed to comply with PCI requirements. Code within the device that does not provide and cannot impact security need not be represented by the identifiers of the approved device.*

Q 2 **Is it assumed that the surface of the potted area is visible without disassembly of the device?**

A *No. The potted, security sensitive components of the device are within the device enclosure and are therefore unlikely to be visible without opening the enclosure.*

Q 3 **Is it acceptable for a device to include removable components and add-ons provided by the vendor?**

A *Any removable components (privacy shields, docking stations, interface modules, etc.) must be evaluated by an approved laboratory to determine that they do not present any additional security risk. However, individual components will not receive a separate approval.*

Q 4 **February (update) 2014: Does the use of protective keypad overlays impact the approval status of a device?**

A *Yes. In general, overlays are not supported by the device approval program due to the potential for keypad tapping or hiding tamper evidence. Overlays may be used where they do not cover any portion of the PIN entry area. For example, in a touchscreen device where the touchscreen is used for both signature capture and PIN entry, an overlay may be used to protect the signature area from excessive wear. In this example only the area used for signature capture may be protected. The material used must be transparent, and not merely translucent, so as not to obstruct the key-entry area when viewed from any angle.*

Q 5 **December (update) 2017: Does the use of a protective case impact the approval status of a device?**

A *Yes. In general, cases are not supported by the device approval program due to the potential for hiding tamper evidence. Cases may be used where they do not cover any portion of the MSR or ICCR area. For example, a case used to protect a drop of a mobile device or the addition of a lanyard may not cover the ICCR or MSR. The interfaces must be clear and visible to the consumer such that wires or tamper evidence cannot be hidden. The material used must be transparent, and not merely translucent. Overlays for the PIN input area must comply with the preceding FAQ. If the POI has been approved for use with a protective case, the security policy shall provide a picture of the approved protective case as properly installed and tested by the lab.*

Q 6 **May (update) 2018: Does the entry of the authentication code (e.g., password) that is used for settlement/balancing at an ATM require the use of the secure EPP, or may it use an alternate mechanism such as the keyboard at the back of the ATM?**

A *The entry of the authentication code used for settlement/balancing at the ATM does not need to be entered through the EPP, and may use the keyboard installed in the rear of the ATM. However, in all cases it is not permitted to use the key(s) used for encryption of cardholder PINs in connection with a financial transaction to encrypt this authentication code. The PIN-encryption keys used for protection of cardholder PINs must not be used for protecting the settlement authentication code, whether that value is entered from the rear or through the EPP. A separate data key would have to be used for any protection of the settlement authentication code.*

Note that authentication codes entered to put the EPP into a sensitive state, such as those used to enable manual key loading, must be entered via a secure interface, i.e., through the EPP.

Q 7 **Some devices ship with firmware that may be convertible into a compliant version but is not compliant as shipped. When is this acceptable?**

A *This is only acceptable where the conversion is one way and cannot be reversed. A device can only be converted to a compliant version. It shall not be capable of converting a compliant version to a non-compliant version. The conversion must be performed at the initial key loading of the acquiring entity's secret keys. The transformation must result in the zeroization of any previously existing acquiring entity secret keys. The compliant version of firmware must be clearly distinguishable from the non-compliant version. Merely appending a suffix (one or more characters) to an existing firmware version is not acceptable. Rather the conversion must result in a high order version number that is clearly distinguishable to purchasers of such devices. Only the compliant version shall be approved and listed.*

Q 8 Some attacks are technically simple in that they do not require an extensive identification, like sniffing a communication on standard interfaces like USB/Ethernet between devices. How is the attack value calculation to be performed then?

A *For technically simple attacks that do not require an extensive identification, like sniffing a communication on standard interfaces like USB/Ethernet between devices, all cost factors besides time and expertise should be disregarded. Also, attack time and expertise are to be considered only for the identification of the general device setup and the property to be attacked (e.g., the interface type).*

Q 9 UPT Version 1 was no longer available for new evaluations after April 2011. Under what conditions is a delta for a Version 1 approved UPT allowed?

A *A vendor with an overall Version 1 UPT approval may get deltas on that device for changes that occur to the OEM components used, including replacement of any given OEM component with a different model—e.g., a separately approved OEM ICCR produced by one vendor is replaced in the final form factor UPT with a different model, even if from a different vendor. This applies as long as the vendor continues to have control over the final assembly and manufacture of the UPT.*

Changes that occur in the final form factor itself (e.g., the housing) because of the complexity of integration must undergo testing as a new evaluation against a version of requirements that has not been retired from use for new evaluations.

In all cases, though, any security requirements impacted will be assessed, including those not previously applicable—for example, if the new casing introduces additional cardholder-interface devices not present in the original evaluation.

Q 10 Does it make any difference if the OEM component vendor is also the vendor who gets the overall UPT approval, vs. a scenario where the OEM vendor sells its components/drop in module to other vendors such as kiosk or AFD vendors who then pursue an overall UPT approval?

A *No. The OEM components can be manufactured by any vendor, even if that vendor is different than the UPT vendor. However, if the vendors are different, those components must have already been PCI approved or the OEM vendor must give permission to the UPT vendor to have those components evaluated as part of the overall UPT approval.*

Q 11 June 2012: During an evaluation, it is determined that a new device includes the identical IP stack that was previously evaluated and approved under the most recent version of the Open Protocols Requirements module. Is it required to redo all Open Protocols testing?

A *If the vendor is able to provide evidence that supports the assertion that the IP stack is 100% identical, including the same version of various components and identical IP Protocols, IP Services and IP Security Protocols, no new testing needs to be performed. The report should document how it was verified that the IP stack is identical and shall include the IP stack information including the component version, the IP Protocols, IP Services and IP Security Protocols supported.*

Q 12 July 2014: POI devices may be approved with support for Open Protocols. Vendors provide a PCI prescribed security policy and other security guidance for the proper implementation of the Open Protocols that are part of the approval. If the entity deploying the device makes changes that are not in accordance with the security guidance necessary to deploy the device in compliance to the Open Protocols module, does it impact the approval? For example: adding additional services or protocols that were not listed in the guidance or using or otherwise replacing the IP stack with one imbedded in the application.

A *Yes, this would invalidate the approval status of the device for any implementation making such changes. Any such change must result in the device successfully undergoing a delta evaluation in order to maintain approval.*

The Open Protocols module is to ensure that open protocols and services in POI devices do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device. In that regard, it does not matter what type of network (public or private) the device is used with.

The vendor defines what protocols and services are supported by the device and provides guidance to their use. The protocols and services are evaluated by the lab. Adding or enabling additional services and protocols or failing to follow the issued security guidance after the evaluation would invalidate the approval status of that device for that implementation.

Q 13 January 2015: There are a number of FAQs on the use of wireless technologies, such as Bluetooth and Wi-Fi. What is the intent of these FAQs, and does PCI have any specific requirements for other types of communications technologies?

A *The intent of the FAQs on all wireless communications for POI devices is to ensure that the interfaces of the POI are protected such that:*

- *Card data cannot be easily intercepted.*
- *Command interfaces to the terminal cannot be easily accessed, intercepted for attack (such as MITM), or used as an attack vector into the device.*
- *Compromise of the interface does not lead to, support, or facilitate further compromise of security assets of the POI.*

PCI does not mandate or require the use of any specific communication technology, but any implementation must meet the above requirements through some aspect of the physical or logical layers of communication. Physical or direct wired communication often achieves this through the nature of its physical interface. Wireless communications cannot rely on this and therefore must rely instead on security at the link or application layers through use of a Security Protocol to establish a trusted path for all communications over the wireless link. This Security Protocol must have been tested and approved under the open-protocols module of the PCI PTS evaluation of that device, and examples of acceptable Security Protocol implementations include WPA2 (implemented at the link layer), or VPN encrypted tunnels (implemented at the application layer).

Q 14 December (update) 2016: Can a PTS device be used as a beacon (iBeacon or BLE beacon) transmitter?

A *Beacons for any version of BLE (e.g., 4.0, 4.1) are allowed providing the following conditions exists and are validated by a PTS approved lab:*

- *The beacon is listed as a device interface in the PTS POI report.*
- *Over the Air (OTA) provisioning is not allowed at any time. Provisioning and updating of beacons must be consistent with existing PTS standards. (i.e., Section J, B4 or B4.1)*
- *Must be referenced in the security policy.*
- *Beacons are transmit-only. The lab must validate that BLE communication cannot be used to respond to any external requests, connect, pair, or otherwise provide two-way communication to any other device.*
- *The vendor provides documentation on the secure use and provisioning of the beacon and that the documentation clearly states the beacon is used for transmit only, and that OTA provisioning is not allowed.*
- *The vendor will document the purpose of use of the beacon functionality—i.e., its intended use. The documentation must include what data is transmitted and ensure that no sensitive data can be transmitted.*
- *The PTS device is never allowed to receive beacon transmissions.*

Q 15 What requirements must a Secure Card Reader be validated against?

A *SCRs must meet, as applicable, the ICCR and/or MSR requirements designated in Appendix B of the PCI PTS POI Security Requirements and all other requirements pertaining to the protection of account data as designated in Appendix B. Also, all of the non-designated account data protection requirements should be considered for applicability. In most cases they will not be applicable and will not require any assessment beyond that determination.*

If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), requirements specified in the Open Protocols Module must also be met. Other requirements, such as B1, self-tests, and B7, random numbers, may apply depending on device functionality. In all cases, if a security requirement is impacted, the device must be assessed against it.

Q 16 February 2014: Can an SCR be used for offline PIN acceptance?

A *SCRs or other POI devices that include an ICCR or hybrid reader must have "Offline" designated under PIN Support in order to be used for offline PIN acceptance.*

Q 17 February 2014: If a SCR processes PINs—i.e., it supports offline PIN authentication via an ICCR component, or it formats and encrypts a PIN block to send online directly to the host—does it have to be evaluated with a specific PIN entry device?

A *Yes, it must be validated in conjunction with a specific PIN entry device—e.g., PED or EPP—to validate the security of the interaction, including the establishment of the keying relationship. The PIN entry device must either be previously approved or obtain approval concurrent with the SCR in the same or a concurrent separate laboratory evaluation.*

Q 18 **June 2012: The approval requirements for an SCR or Non-PIN device do not include PCI PTS DTR A1, which requires active tamper-response mechanisms. Is it possible to meet the physical security requirements of an SCR or Non-PIN device using only tamper resistance and tamper evident characteristics, if the attack costing can be shown to exceed the minimum levels required for each of the physical security testing requirements?**

A *No, it is a requirement that all devices implement active tamper detection mechanisms to meet the physical security requirements of PCI PTS. SCR and Non-PIN devices must have permanently active tamper detection mechanisms that monitor for intrusion and respond to such events with the immediate erasure of sensitive information within the device, rendering the device inoperative.*

A device cannot meet PTS POI requirements without having an active tamper response mechanism to zeroize secret and private keys during a penetration attack regardless of which modules of the PTS POI standard the device is designed to comply with. Penetration of the device must cause the automatic and immediate erasure of any secret and private keys such that it becomes infeasible to recover the keying material. This is true of devices even if they do not accept customer PINs, or are not designed for the protection of customer PINs. Secret or private cryptographic keys that are never used to encrypt or decrypt data, or are not used for authentication, are excluded from this requirement as such keys would never be keys involved in protecting customer PINs or customer card data.

Q 19 **July 2013: Can a device with an ICCR be approved for online PIN only if it supports any offline PIN entry method (i.e., the device supports enciphered and/or plaintext PIN)?**

A *Devices with an ICCR that are not evaluated against the ICCR requirements for offline cannot have the approved version of the firmware support any offline PIN acceptance. Furthermore, devices that support online PIN must be evaluated for online PIN, or the approved version of firmware must have online PIN acceptance disabled.*

Q 20 **June 2012: If a device supports multiple IP enabled interfaces, does testing need to be performed on all IP enabled interfaces by the laboratory during the evaluation?**

A *If a device supports multiple IP enabled interfaces and the IP stack (including all IP Protocols, IP Services and IP Security Protocols) are identical for all interfaces, testing is only required to be performed on one of the IP enabled interfaces.*

Q 21 **December 2013: The PCI PTS requirements do not dictate any specific form factor for devices. Is there any restriction to the types of systems or devices that can be approved under the PCI PTS program?**

A *PCI PTS does not dictate device form factors to allow for vendors to develop innovative solutions to address market needs. However, PTS approval can only be obtained by devices that are designed for direct interaction with customers. Sub-components, such as microprocessors, magnetic card reader 'cans', ICC acceptors, and others that are designed for integration into another device which would prevent direct sight and interaction of the approved system by the cardholder cannot be approved under the PCI PTS requirements.*

Q 22 July (update) 2014: POS PIN pads without card interfaces can be approved for offline operation when validated for compliance with a PTS approved external card reader (this may be a PTS approved PED acting as external card reader or a secure card reader). What details need to be listed for such a configuration?

A *Under the listing the POS PIN pad shall be detailed with which specific PTS approved PED or SCR the PIN pad is able to perform offline PIN validation. A hyperlink to the approved PED or SCR will be included as an approved component. Where there are multiple devices with which it is possible to operate, all shall be listed. The use of the device with a non-listed reader invalidates the offline approval.*

Q 23 October (update) 2018: In light of the discovery of the Padding Oracle on Downgraded Legacy Encryption (POODLE) attack, is SSL still an allowed protocol.

A *SSL may continue to be supported, but the vendor must document (for version 4 and higher devices this includes the Security Policy published on the PCI website) that it is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan. For SSL 3, or older versions of TLS, if supported, all cipher suites using single DES or RC4 must be removed. Both of these objectives may be achieved by modifying the source code to remove support for SSL and non-allowed cipher suites and/or by modifications to the configuration file. In either case, the version information of the code, including where applicable the modified configuration file, shall be identifiable as part of the approved firmware.*

Furthermore, for all new POI evaluations using the Internet Protocol Suite, devices must support TLS 1.2 or higher. In addition, all delta evaluations for POI v3, v4, v5, or v6 devices where the open protocols module is impacted, must meet the same criteria.

PCI requires that devices must only support Cipher Suites for use in TLS 1.2 or higher that provide at least 112 bits of security. Cipher suites that comprise AES and other NIST-approved algorithms are acceptable to use. Cipher suites that use TDEA (3DES) are no longer allowed due to the limited amounts of data that can be processed under a single key i.e., the 64-bit block size does not provide adequate protection in applications such as TLS where large amounts of data are encrypted under the same key.

Q 24 May (update) 2018: PIN entry devices may physically integrate in the same device other functionality, such as mobile phone, PDA capabilities or POS terminal. Handheld configurations of PIN entry devices may accommodate the attachment (e.g., via a sled, sleeve or audio jack) of a mobile phone, PDA or POS terminal, where the attached device communicates with the PED. Such a configuration appears as a single device, with separate interfaces for input by the clerk and cardholder. What considerations must be taken into account for either of these configurations?

A *For any device where the cardholder is expected to use the same interface for PIN entry as the clerk would use for phone, PDA, payment application, etc. purposes, or where there are multiple interfaces in a single integrated device, the integrated device must be physically and logically hardened in accordance with the PTS POI security requirements.*

In a handheld configuration with an attached device, there is a risk that the cardholder enters the PIN on the wrong interface. Furthermore, the communication interface between the PED and the attached device may give the latter access to MSR functions without cryptographic controls, allowing skimming of card account data. In this integration model, then either:

- *Both devices are assessed and validated as compliant to the PTS POI requirements, or*

- *The PED device, which must also control the card reader(s), must implement and be validated against the PTS POI SRED module. The PED must enforce SRED functions for encryption of card data at all times. The PED is only allowed one state, and that is to encrypt all account data. It cannot be configured to enter a state where account data is not encrypted.*

Q 25 July 2015: Handheld PEDs that attach to a mobile phone, PDA or POS terminal via a sled, sleeve or audio jack are required to support SRED. Does this apply to PEDs that connect via wireless technologies such as Bluetooth or Wi-Fi to mobile phones and tablets?

A *Yes. Furthermore, for devices that do not implement SRED encryption, the Security Policy must clearly state that the system cannot be implemented to connect to a tablet or mobile phone, and any such use will violate the approval of the device. Systems that do have SRED approval must note that SRED functions must be enabled and enforced for such use cases to maintain their approval.*

Q 26 May (update) 2018: PIN Entry Devices that attach to a mobile phone, PDA or POS terminal via a sled, sleeve, audio jack, or wireless connection are required to support SRED. Does this apply to PEDs that are integrated with other devices (such as a tablet or mobile phone) that appear as a single device?

A *Yes. An integrated device is one where two physically and electronically distinct devices (e.g., a PED and a commercial off the shelf (COTS) device such as a mobile phone) appear as a single device through the use of the plastics to mask the connectivity.*

In such a configuration, there is a risk that the cardholder enters the PIN on the wrong interface. Furthermore, the communication interface between the PED and the integrated device may give the latter access to card reader functions without cryptographic controls, allowing skimming of card account data. In this integration model, then either:

- *Both the PED and non-PED are assessed and validated as compliant to the PTS POI requirements, or*
- *The PED, which must also control the card reader(s), must implement and be validated against the PTS POI SRED module and be both physically and electronically distinct from the non-PED system (for example, it is not acceptable to have the PED firmware execute within the same processor as the non-PED firmware). The PED must enforce SRED functions for encryption of card data at all times. The PED is only allowed one state, and that is to encrypt all account data. It cannot be configured to enter a state where account data is not encrypted.*

The Security Policy must also state that the non-PED has not been assessed under the PCI PTS program and security guidance is required to ensure the secure operation of the solution. An additional note will be added to the portal noting that the non-PED has not been assessed under the PTS program.

Q 27 July 2017: For purposes of PCI acceptance, a draft standard is a document that either has been published as a draft for trial use (e.g., ISO FDIS) or has been published as a draft for public comment (e.g., NIST drafts).

A *However, ANSI (X9) does neither of these; and further clarification must be made. For purposes of PCI acceptance, an ANSI (X9) draft standard is one that has been successfully balloted out of the assigned X9 working group (e.g., X9F1, X9F4, or X9F6). Prior to this point, working group procedures allow members to post documents in various stages of "draft" which may conflict with each other and may not reflect a consensus of the working group. A breach of the algorithm invalidates any standard—draft or final.*

Q 28 May 2018: Is it acceptable for a terminal application to parse input data, which dynamically changes its execution behavior at runtime? E.g., can a web browser or e-mail client parse and display HTML5, Java, JavaScript or any other scripting language?

A *Yes, as long as the data is being parsed, verified and displayed by the firmware.*

Q 29 October 2018: Are there minimum requirements for the version of Android to be used within a PTS device?

A *Yes, it is expected that the Android version is officially supported with security patches, at a minimum. Any reports, including deltas, where the Android version is not supported with regular security patches will be rejected. Where these patches are not provided by Google, evidence of security patches (implemented at least monthly) provided by the vendor must be documented in the report provided by PCI; evidence for this is expected to be validation of the update code by the laboratory for at least two previous patches, as well as validation by the laboratory that these patches have remediated existing known vulnerabilities in the version of Android used.*

Vendors should note that this means that consideration for the future patch status of any Android version used must be made during the initial design stages of the device, to prevent unexpected rejection of devices after an Android version becomes unsupported during the development of a solution.

Q 30 October 2018: DTRs state, "Evidence-based reporting, demonstrating device compliance through robust testing, is the fundamental basis for achieving device approval." What are the minimum expectations for testing/test evidence for any device resistance to attacks involving physical penetration/modification?

A *Although evidence of cutting and/or drilling into the device (exterior case, interior parts) is a primary test activity in most evaluations, cutting and/or drilling alone is rarely sufficient to demonstrate satisfactory resistance to all/any Security Requirements where a viable attack path has elements of physical penetration/modification. It is necessary for the evaluating lab to show, additionally, robust evidence of the device's resistance to physical attacks attempting to circumvent, for example (but not restricted to), tamper switches, meshes, PCBs, tamper circuits, keyboards, screens, card readers, boards, etc., and these device parts' components and/or components connecting these.*

POI Requirement A1

Q 1 **What vulnerabilities must be taken into account for a touchscreen?**

A *If the sides are accessible, an overlay attack utilizing a second, clear touchscreen could be a problem. The connection/path from the touchscreen to the processor (and any devices used for decoding the signals in between) needs to be verified to be secure. Bezels around the touchscreen are especially dangerous because they can conceal access to areas of concern that are described above.*

The API for firmware and applications (if applicable) needs to be looked at carefully to determine the conditions under which plain-text data entry is allowed. Example: It should not be possible unless under acquirer display prompt-controlled devices, for a third party to display an image (JPEG) that states "press enter when ready for PIN entry" and then have a plain-text keypad pop up on the next screen. The extra caution is warranted for touchscreen devices because of the desire to make touchscreen devices user-friendly and to run many different, unauthenticated, uncontrolled applications. This is especially true for the devices that are intended to be held because of the tendency to regard them as a PDA that can perform debit transactions.

Q 2 **In the event of tamper, the device must become immediately inoperable and result in the automatic and immediate erasure of any secret information that may be stored in the device, such that it becomes infeasible to recover the secret information. Guidance notes provide that secret or private keys do not need to be zeroized if either or both of the following conditions exist:**

- **If any of these keys are not zeroized, then other mechanisms must exist to disable the device, and these keys must be protected in accordance with Requirement A6.**
- **The keys are never used to encrypt or decrypt data, or are not used for authentication.**

Do any other conditions apply?

A *The keys (secret or private) are never used to encrypt or decrypt other keys. Keys that can be used to download other keys to make the device operable must either be zeroized or rendered inoperable for use in downloading new keys. E.g., both symmetric KEKs used for key loading using symmetric techniques and private keys associated with key loading using asymmetric techniques. The device must enforce that tampered devices require withdrawal from use for inspection, key reloading, and re-commissioning. It is not sufficient to rely upon procedural controls for this.*

Q 3 **A device uses a key that is randomly generated internally in the secure processor to protect other keys. This key is stored in the clear and protected within a register in the same secure processor. The secure processor resides within a secure area of the device. This key is used to encrypt other keys, which are stored encrypted outside the secure processor—e.g., in flash memory that also resides within the secure area of the device. Upon tamper, the device erases this internally generated key but leaves intact the other keys encrypted by this key, which can no longer be used because the device cannot decrypt them. Under A1, must the device also zeroize these encrypted keys upon tamper?**

A *The device need not zeroize these encrypted keys provided that they are encrypted using appropriate algorithms and key sizes as defined in Requirement B9.*

Q 4 May (update) 2018: Requirement A1 states that a device uses tamper-detection and response mechanisms that cause it to become immediately inoperable. If the device is tampered, can it still be used to process non-PIN based payment card transactions?

A *A PIN-acceptance device that is tampered must immediately cease processing all PIN based payment card transactions. If implemented only one reset shall be supported unless the device is removed for inspection and repair. Any intervention enabling transactions, must require an onsite presence which validates there was NO tamper of the device and is subject to the following conditions:*

- *Use of dual-control techniques;*
- *Provide accountability and traceability including logging of user IDs, date and time stamp, and actions performed;*
- *Sensitive information required for the authorization (e.g., passwords/authentication codes) is initialized or used in a way that prevents replay at the same or a different device.*

POI Requirement A2

Q 1 What vulnerabilities must be taken into account for a touchscreen?

A *If the sides are accessible, an overlay attack utilizing a second, clear touchscreen could be a problem. The connection/path from the touchscreen to the processor (and any devices used for decoding the signals in between) needs to be verified to be secure. Bezels around the touchscreen are especially dangerous because they can conceal access to areas of concern that are described above.*

The API for firmware and applications (if applicable) needs to be looked at carefully to determine the conditions under which plain-text data entry is allowed. Example: it should not be possible unless under acquirer display prompt-controlled devices, for a third party to display an image (JPEG) that states "press enter when ready for PIN entry" and then have a plain-text keypad pop up on the next screen. The extra caution is warranted for touchscreen devices because of the desire to make touchscreen devices user-friendly and to run many different, unauthenticated, uncontrolled applications. This is especially true for the devices that are intended to be held because of the tendency to regard them as a PDA that can perform debit transactions.

POI Requirement A4

Q 1 December 2011: What requirements exist for the security of public keys and key management functions on SCR approval class devices?

A *Public keys must be protected against change within the device, to prevent attacks to compromise the security of the system through this attack vector. Devices designed for compliance to the SCR approval classes, and which rely on public keys to provide security or authentication to functions such as firmware updates, must be assessed by the PCI PTS laboratory to Requirement A4.*

POI Requirement A5

Q 1 What standards and methods are used for measuring "electro-magnetic emissions"?

A *Vendors must take into account that EM emissions can be a risk to PIN data, and must design devices to address this risk. There are many methods for shielding and minimizing EM emissions. The vendor must describe to the laboratory in writing how EM emissions are addressed by the device design. The laboratory will examine evidence provided by the vendor to determine if the evidence supports the vendor's assertion. Evidence can include the device itself, design documents, third-party test results and approvals. Testing will be performed as necessary.*

Q 2 May 2017: Are there any situations where the evaluation report does not have to provide an attack costing.

A *Yes, for A5 (Monitoring During PIN Entry), where testing of any external characteristic available for monitoring demonstrably satisfying the applicable DTR test steps has not found any leakage, then it must be explained why any attack scenario cannot be feasible for less than 26 points, with a minimum of 13 for initial exploitation. In such a situation no formal attack calculation needs to be presented.*

POI Requirement A7

Q 1 July 2017: Evaluators typically use both source code review and testing of the implementation to verify that side channel protection methods are implemented. How must the evaluator proceed where protections are in code created by the chip vendor and this is only provided to the POI vendor as a library and not source code?

A *The evaluator must treat the device as a black box and extend testing beyond what would otherwise be required if the source code was available in order to determine that the device is resistant to attack. The Side-Channel Analysis Standards for PCI-PTS Evaluations appendix in the Derived Test Requirements provides guidance.*

The report must clearly stipulate what materials were provided for the evaluation and what specifically was tested, details of counter-measures put in place and implemented, including what code was reviewed. If the materials are not provided it must be treated as a black box evaluation as delineated in the prior paragraph and reported as such.

POI Requirements A8, B15 and C2.4

Q 1 The intent of A8, B15, and C2.4 is to eliminate the possibility that PIN values will be entered at an improper time and handled by the device in a non-secure manner. One way for a vendor to address A8, B15, or C2.4 is to allow for the entry of PIN values only. Would it be acceptable to allow the input of numerical data if the numerical data is three characters or less and therefore could not represent a PIN value?

A *This would be acceptable if there is no way for a device to accept the input of a PIN value at an inappropriate time. For instance, it must not be possible for a device to allow the entry of three characters, automatically change states without the cardholder pressing "enter" or some other control key, and then accept the remainder of the PIN value.*

Q 2 What restrictions exist if a device can display uncontrolled messages and the keypad is used to enter non-PIN data?

A *The prompts for non-PIN data entry must be under the control of the cryptographic unit and must be specific such that a cardholder would not enter a PIN at an inappropriate time. An uncontrolled message followed by an ambiguous prompt for non-PIN data could lead to a cardholder entering their PIN at an inappropriate time. For example, if the device displayed the uncontrolled message "Ready for PIN" then prompted for plain-text data while displaying "Enter Data," the cardholder may enter their PIN at this non-PIN data prompt.*

Q 3 Is it acceptable for uncontrolled messages to be displayed simultaneously with prompts for data entry?

A *No. Any text, including images, other than numbers and punctuation, displayed along with a prompt is considered a prompt and must comply with all requirements governing prompts.*

Q 4 Some device designs fit either vendor-controlled or acquirer-controlled display prompts on who is given custody of cryptographic keys protecting prompt updates are managed. Does such a device need to have different identifiers?

A *If the device is to be listed as both an acquirer-controlled and a vendor-controlled display prompts device, there must be a differentiation so customers can distinguish between the two (e.g., different hardware and/or firmware versions).*

Q 5 For devices that implement acquirer-controlled prompts, is it required to use a secure cryptographic device to implement the dual control required to manage those prompts?

A *Dual control must be enforced by an SCD. The SCD can be the PED itself or another device. If an SCD other than the PED enforces dual control, the vendor must either provide the SCD to third parties, or describe how an SCD must be used to comply with B15. The description must include an example of a specific, existing SCD that can be purchased and used to comply with B16. The PED must have an API that is compatible with the SCD. The complete solution must be fully developed. It is not acceptable to provide detailed instructions that require users to develop part of the solution.*

Q 6 December (update) 2017: For PEDs designed with multiple data acceptance interfaces, where there is a hard keypad dedicated to PIN (and other sensitive data) entry, and the other interface is a touch interface not intended to accept any sensitive data entry, what controls are required for the second interface?

A *In this type of design, the following controls on the "non-sensitive" interface must be enforced, in addition to the existing restriction that applications must not ask for input of sensitive data:*

- *The firmware must be designed such that no sensitive data can be entered into the "non-sensitive" interface.*
- *If the x/y touch coordinates are sent to the authenticated applications on the device, the vendor must provide guidance to application developers to not ever send out touch coordinates. Additionally, the vendor also must review all applications and NOT sign/authenticate them if they are written to send out touch coordinates, thus not allowing them to be loaded; or*
- *If the PED authenticates the endpoint that receives the x/y coordinates and if the communication link between those instances is securely encrypted (for instance using a TLS v1.2 tunnel) then the device can provide x/y touch coordinates only to applications or servers that have been authenticated by the device.*

POI Requirement A8

Q 1 **Can the calculation for the attack potential of 18 per device include the cost of development kits that provide application programming information?**

A *No. The device must include protections that require an attacker to achieve an attack potential of at least 18 to order to defeat them. Administrative controls on application programming information are not adequate to meet this requirement.*

Q 2 **Touchscreen devices offer multiple possibilities for the data entry: traditional PIN pad layout, QWERTY layout, signature capture, handwriting recognition, etc. Does A6 apply to all of these methods of data entry, or only the traditional PIN pad?**

A *A6 applies to all methods of data entry that can be used by a cardholder to disclose their PIN, including QWERTY layout, signature capture, and handwriting recognition.*

POI Requirement A9

Q 1 **Requirement A9 stipulates that the device must provide a means to deter the visual observation of PIN values as they are being entered by the cardholder. What methods are acceptable?**

A *The POI Security Requirements provide for several options that may be used separately or in combination to provide privacy during PIN entry. These options are:*

- *A physical (privacy)shielding barrier. Note that in case the privacy shield is detachable, a user's guide must accompany the device that states that the privacy shield must be used to comply with ISO 9564. Optionally, the user's guide can also reference PCI device requirements;*
- *Designed so that the cardholder can shield it with his/her body to protect against observation of the PIN during PIN entry, e.g., a handheld device;*
- *Limited viewing angle (for example, a polarizing filter or recessed PIN pad);*
- *Housing that is part of the ATM or kiosk, cardholder's hand or body (applies to handheld devices only); and*
- *The installed device's environment.*

Q 2 **September (update) 2016: Is there any impact on the device's approval if the laboratory evaluated privacy method is not used?**

A *Frequently, the deployers of devices rationalize that privacy-protection mechanisms may be bulky or obtrusive, make it more difficult to see the device's screen, or, with less dexterous users, interfere with card payment and PIN entry. However, in order to maintain the device's approval, and any associated liability protection for compromise attributable to use of said device, it is required that the device meet the privacy-shield requirements as evaluated by the laboratory and upon which the approval was based. Devices deployed that do not use the privacy-shield requirements evaluated by the test laboratory are no longer considered approved devices. This must be disclosed in the security policy for the device.*

Q 3 **September 2016: Vendors must either provide a privacy shield providing privacy protections during PIN entry for the cardholder, or alternatively, the vendor may use less restrictive privacy-shield criteria provided that the vendor supplies rules and guidance as to how the visual observation is to be deterred by the environment in which the device is installed. Does this impact the security policy disclosure?**

A *Yes. The security policy must stipulate the rules and guidance under which the device was evaluated as to how the visual observation is to be deterred by the environment in which the device is installed. The policy must also disclose that deployment not using these considerations that were evaluated by the lab and upon which the approval was based will invalidate the device's approval.*

If the device comes with a removable privacy shield, the security policy must disclose that deployment without the shield invalidates the approval unless the device is deployed in accordance with instructions in the security policy validated by the lab for deploying the device with protections provided by the environment in which it is installed. The policy must also disclose that deployment not using these considerations that were evaluated by the lab and upon which the approval was based will invalidate the device's approval.

POI Requirement A10

Q 1 **September 2013: Can a device be validated to SRED if it receives account data that is entered on a non-integrated module or device—for example, where a device receives account data that is key-entered on another device?**

A *The external module or device where the account data is captured can receive SRED approval if evaluated in conjunction with the POI device. The SRED approval would be contingent on both devices meeting all applicable SRED requirements, including the protection of cryptographic keys. Account data (as defined in the glossary of the* PCI PTS POI Security Requirements*) traversing the communication path from the external point of capture must be encrypted in accordance with these requirements. Both devices would be part of the approval listing, and the substitution of the external device with another that is not validated to SRED invalidates the approval of SRED as a function provided.*

If the external device cannot meet SRED requirements, the primary device—even though it otherwise protects account data in accordance with SRED—cannot receive the SRED designation where it is capable of receiving account data from such a device, regardless of whether that data is received encrypted. In this situation, in order for the primary device to receive SRED approval, the firmware of the primary device must not support the receipt of the externally captured account data.

POI Requirement A11

Q 1 **November 2012: Where a whitelist is used to control whether PAN data exits the device in plaintext or ciphertext, does the whitelist updating have to be under the direct control of the vendor?**

A *No, the vendor may provide the mechanisms to the acquirer to directly control the updating of the whitelists in a manner consistent with acquirer-controlled display prompts—that is, the use of dual-control techniques and provisions for auditability and logging.*

The vendor may alternately provide user documentation detailing the management of cryptographic keys following these principles and implementing the use of a secure cryptographic device for management of these keys. The process exists upstream of the device, but the device must still provide enforcement—e.g., validate the MAC or digital signature.

POI Requirement A13

Q 1 **What is meant by "sufficient space to hold a PIN-disclosing 'bug'"?**

A *Space accessible via the ICC card slot large enough to conceal a PIN-disclosing bug is not allowed. Such a bug could utilize ICC technology. Therefore, there must not be space accessible via the card slot large enough to conceal an ICC chip and small battery.*

Q 2 **What volume of space is allowed under A13?**

A *The objective of A13 is to guard against a PIN-disclosing bug being inserted into the device through the card slot. The volume of space accessible via the card slot that could be utilized by an attacker can vary with the geometry of the space and attack methods. For this reason, the requirement does not prohibit a specific volume. Rather, the feasibility of effective bug placement is to be considered when assessing A14 compliance. Examples of these considerations are:*

- *Contact points must be present for the bug to connect to.*
- *The bug and wires must not obstruct normal operation.*
- *The placement of the bug must not cause tamper evidence that would be noticed by a typical cardholder.*

Q 3 **May 2018: The new SCRP approval class increases the level of protection required for the ICC I/O interface to 26 points. Why is this required when other approval classes continue to allow for a device meeting a level of 20 points of protection to be considered compliant?**

A *The intent behind the SCRP approval class is to ensure that the customer card data is protected and strongly encrypted before it is sent through the passed into the COTS environment device onto the backend systems for payment processing. This is an important part of the overall security of the Software Based PIN Entry on COTS (SPoC) PIN on COTS system solution, and helps to prevent correlation attacks and reduce the threat of the compromise of the PIN on the COTS device. Because protection of the ICC I/O signal requires protection from the physical interface to the customer card through to the security processor that performs the encryption of this data, requiring an increase in the attack point minimums for this therefore has the effect of increasing the overall protections required in the SCRP as a whole—which in turn has a carry-on effect to reducing the risk of PIN theft on the COTS device.*

Other approval classes where ICC cards are accepted may not process PINs at all, or are required to conform to other attack costing calculations and minimums within the PCI PTS requirements, and therefore do not rely so strongly on the separation of customer card data and PIN data. This is why the attack points can remain at 20 points for those other use cases.

POI Requirement A14

Q 1 **Is D2 intended to address the opening of the ICC reader, or the entire reader?**

A *D2 is written with the understanding that the opening (slot) is a potential point of attack for the insertion of a tapping mechanism.*

Q 2 **Some device designs include components (e.g., privacy shield) that are near the IC card slot, which could be used to conceal a wire. What criteria are used to determine compliance when such components are present?**

A *The design is considered compliant with A14 if a portion of the wire is visible between the slot and the concealing component.*

POI Requirement B1

Q 1 **If a device employs firmware on the MSR's read head to encrypt account data, is that firmware subject to authenticity checking as defined in Requirement B1?**

A *No. Authenticity checking as defined in Requirement B1 is for the management of firmware that is directly or indirectly involved in the protection of cardholder PINs as defined in the various security requirements. However, the firmware on the read head must be designed such that it cannot be updated.*

Q 2 **Under what circumstances can a device not use authenticity checking when self-testing its firmware?**

A *A device does not require authenticity checking when self-testing its firmware if (all apply):*

- *The authenticity checking of firmware—either internally and according to B2 or externally using appropriate procedures within a secured environment under the vendor's control—is performed whenever the firmware is established in that secure area;* ***and***
- *The effort to deliberately modify or replace the firmware or parts of it in order to get access to sensitive information (access to the memory device) must be addressed as an attack scenario under Requirements A1, A4, and A6 and meet the respective attack potentials;* ***and***
- *A periodic integrity check according to Requirement B1 is performed for the firmware, ensuring that random changes will be detected; and if cryptographic authenticity is not performed, the integrity check must be cryptographically based. Although an algorithm using a secret key, such as a keyed hash, can be used, it is not necessary for meeting the integrity criteria.*

These conditions apply regardless of any non-reconfigurable property of the device memory.

When firmware is externally authenticated, the level of security shall be of the same level as for key-injection facilities.

POI Requirement B2

Q 1 **What parties may possess keys used for the cryptographic authentication of firmware updates?**

A *The firmware is the responsibility of the device vendor, and as such the cryptographic keys that authenticate it within the device must be held solely by the vendor or their designated agent.*

Q 2 **Firmware updates must be cryptographically authenticated, and if the authentication fails, the update is rejected and deleted. Are there any circumstances where firmware can be updated without authentication?**

A *Some chipsets are not designed for firmware updates, but only to support firmware replacement. The deletion of the existing firmware and cryptographic keys during the replacement does not allow for the authentication of the new firmware to occur.*

In such cases it is acceptable to update the firmware without authentication if the process requires that the device be returned to the vendor's facilities and results in the secure zeroization of all secret and private keys contained within the device.

Q 3 **December 2011: If a device supports firmware updates, the device must cryptographically authenticate the firmware, and if the firmware is not confirmed, the firmware update must be rejected and deleted. Can a device completely load new firmware before checking its authenticity and overwrite its primary copy of existing authenticated code if it retains a secure backup copy of the existing authenticated code?**

A *Yes, provided the following is true:*

- *The new code is cryptographically authenticated prior to execution.*

  If the new code fails authentication, the backup copy of code is cryptographically authenticated, and if the backup copy is successfully authenticated, the device boots from the backup copy and the backup is then used to overwrite the new code that failed authentication.

- *If both firmware versions fail authentication, the device fails in a secure manner.*

Q 4 **February 2017: If the device uses digital signatures for authenticating firmware updates (compliant with B2), does it need to use a secure protocol to meet B22?**

A *B2 stipulates that firmware loaded into the device must be authenticated regardless of how the file is delivered to the device.*

B2 ensures that the management platform delivers the files to the device securely and that the interface cannot be used as an attack vector into the device.

- *For remote access—i.e., the files are delivered to the device across a private or public network—the use of a security protocol is required and must be validated.*

- *For manual access—i.e., where the operator has physical control of the terminal and the files, and the files are not delivered across a network—the device must ensure that the interface cannot be exploited (e.g., by restricting access/functionality on the interface, requiring administrative rights, using cryptographic authentication techniques, etc.).*

B22 states it is for remote access only and does not include a manual element, a security protocol would be required to ensure the interface cannot be exploited.

POI Requirement B2.2

Q 1 **March 2011: Authenticated applications may be developed by the POI vendor or by other third parties. The applications are to be developed using techniques consistent with PA-DSS and must be cryptographically authenticated by the POI. Are there any other considerations?**

A *Yes. The technique used to manage the authentication mechanism (e.g., digital signatures) must use an SCD and dual-control techniques. For third parties, the device vendor must either provide the SCD to the third parties or describe how an SCD must be used to comply with B7. The description must include an example of a specific, existing SCD that can be purchased and used to comply with B5. The POI must have an API that is compatible with the SCD. The complete solution must be fully developed. It is not acceptable to provide detailed instructions that require users to develop part of the solution.*

POI Requirement B4

Q 1 **Requirement B4 requires that a PIN be encrypted immediately. Typically, this means that the secure processor forms and encrypts the PIN block before performing any other operation. However, some device designs place a microprocessor between the keypad and the secure processor. Under what conditions, if any, would such a design be allowed?**

A *Such a design is considered compliant if the microprocessor, the secure processor, and the path between them are completely within the protective boundary of the device. This boundary is established by the method chosen to meet A1.*

An alternate method of meeting the requirement would be for the microprocessor to immediately encrypt the PIN before passing it to the secure processor, which would then decrypt it and create the encrypted PIN block. Note that in this type of design, the microprocessor software used to encrypt the PIN data is being used to meet PCI requirements. Therefore, this software must be considered "firmware" as addressed by PCI requirements. As such Requirements B3 and B4 would apply to this firmware.

Q 2 **It is common practice for encrypting PIN pads used in ATMs to support the use of one command to initiate PIN entry and another command to encrypt the PIN. Is this acceptable under B4?**

A *Yes. It is acceptable for an EPP to allow one command to initiate PIN entry and a second command to initiate PIN encryption. However, it must not be possible for the encryption command to be used to encrypt the PIN multiple times to output the encrypted PIN from the EPP under different cryptographic keys or to output the PIN in plain-text. Also, the plain-text PIN value must only exist in tamper protected memory or equivalent.*

Q 3 **September 2012: Devices may support the encipherment of the PIN multiple times as part of a transaction series. B4 stipulates that the encipherments must use the same encryption key for this series. Can the transaction series be encrypted by a series of keys if the current key is a derivation of a predecessor key?**

A *The purpose of the requirement is to prevent an adversary from using the authorized key to send the transaction online for authorization and another key to log the transaction for later recovery. In that regard a UKPT methodology may be used for the transaction series, whereby the keys are part of the same series and the entire hierarchy is secured in the same manner and it is infeasible in the design to insert a rogue key.*

Q 4 **April 2013: B4 requires that online PINs must be encrypted immediately after PIN entry is complete. It is further stipulated that plaintext PINs must not exist for more than one minute from the completion of the cardholder's PIN entry. In all cases, erasure of the plaintext PIN must occur before the tamper-detection mechanisms can be disabled using attack methods described in A1. Are there any circumstances where a plaintext PIN can exist for more than one minute?**

A *Some ATMs have implemented intelligent deposit technologies to enhance the customer experience. As a result, some deposit transactions take longer than one minute and result in the PIN being cleared from the buffer after one minute and the cardholder then needing to start the transaction over, and in some cases, unable to complete the transaction at all. In those cases, the ATM applications require modification to prompt for PIN re-entry if a transaction goes over the time out period, rather than requiring the entire transaction to be re-started.*

In order to allow a sufficient time for the modification of those applications, PCI will allow three years from the publication of this FAQ for those applications to be modified. During this three-year abeyance, the unenciphered PIN may remain in the buffer for up to five minutes. However, the PIN must remain protected from compromise using attack methods described in A1, and the test laboratory shall take into consideration the lack of timely encipherment when designing attacks.

This abeyance only applies to encrypting PIN Pads designed and used for ATMs.

POI Requirement B5

Q 1 Is it acceptable to XOR key components during key loading to satisfy the authentication requirements of B5?

A *The XOR of key components alone is not enough to constitute authentication. Some type of authentication of the users that use the key loading function, or authentication of the key-loading command is required.*

Q 2 May (update) 2018: Under what circumstances is key entry via the device keypad permitted?

A *Plain-text single component secret keys cannot be entered into the device using the keypad. Plain-text key components may be entered via the keypad in accordance with ISO 11568-2. Encrypted keys may also be entered via the keypad. Entry of key components or encrypted keys must be restricted to authorized individuals. Functions used to enter keys must only be available when the device is in a sensitive state. Access to sensitive functions must be restricted through the use of passwords/authentication codes or other secret knowledge.*

Q 3 Do maintenance menus that provide services such as LCD Contract Adjustment, Self-tests, Printer Maintenance, and Key Tests constitute a "sensitive service?"

A *If the services provided in these normally non-permitted functions do not affect the security of the terminal or the cardholder data, they are not considered sensitive services. Only services that could compromise the security of the terminal are sensitive services.*

Q 4 For devices that require the use of authentication data to access sensitive functions, and the authentication data are static, can the authentication data be sent with the device?

A *The authentication data can be sent with the device only when the authentication data is in tamper-evident packaging, such as the use of PIN mailers. Otherwise separate communication channels must be used with pre-designated recipients.*

Q 5 March 2011: Plain-text secret or private keys and their components may be injected into a PIN pad using a key loader (which has to be some type of secure cryptographic device). Are there any restrictions on loading keys via this methodology?

A *Yes, the loading of plain-text secret or private keys and their components using a key-loader device is restricted to secure key-loading facilities. Unattended devices deployed in the field shall have plain-text secret or private key loading restricted to key components entered via the keypad of the PIN pad. If encrypted, those keys can be loaded over another interface, such as a serial or USB port.*

Q 6 December 2011: Devices may have functions for zeroizing secret and private keys in the device. Are these functions considered sensitive services that require authentication?

A *Yes, the intentional zeroization of secret or private keys in a non-tamper event is the execution of functions that are not available during normal use. This requires authentication consistent with the implementations of other sensitive services, such as the use of PINs/passphrases. If implemented, the device must force the authentication values to be changed from default values upon configuration of the device. The authentication mechanism may optionally employ dual control techniques.*

Q 7 **June (update) 2015: Devices may have functions for zeroizing secret and private keys in the device. This functionality is regarded as a sensitive service that requires authentication. In some cases there is an upstream effect where software changes must occur on interfaces points, such as ATM platforms, applications, switches and hosts that interface with EPPs. Is there any dispensation from this requirement?**

A *All devices implementing this functionality must meet the requirement. However, the device may do so by implementing a new authenticated deletion command to the EPP command set, in addition to the existing commands. This must be coded as an either/or option such that both methods would not be available at the same time. Once the authenticated option is chosen, this would permanently lock out the non-authenticated commands.*

In all cases a time bound validity period must exist to force the upstream software changes to be implemented within a set timeframe. PCI will allow three years from the publication of this FAQ for those applications to be modified. This abeyance only applies to encrypting PIN Pads designed and used for ATMs.

Effective 1 January 2017, all newly approved EPPS must only support authenticated deletion capability. EPPs approved prior to January 2017 with non-authenticated deletion capability are not required to be upgraded to authenticated deletion capability to maintain PCI compliance.

Q 8 **November 2020: POI devices must support one or more of four specified techniques for the loading of private or secret keys. Methods a and b are for plaintext key loading and methods c and d are for encrypted key loading. The requirement specifies that EPPs and OEM PEDs intended for use in an unattended environment shall only support methods a, c, and d. It further specifies that SCRPs shall only support the loading of encrypted keying material. Are there any other restrictions?**

A *Yes. For all new evaluations (i.e., evaluations that result in a new approval) of POI v5 devices, the POI devices must support at least one of the encrypted key loading methods for the loading of private or secret keys.*

POI Requirement B7

Q 1 **January 2015: It is a requirement of DTR B21 that a POI generate the EMV Unpredictable Number (UN) for any PIN based transaction using the internal RNG, as tested under requirement B7. Are non-PIN based transactions also required to generate the UN from the RNG of the POI?**

Yes, the RNG of the POI must be used to generate all random and unpredictable values that are used for the security of card data and PIN transactions. When the POI is used to generate the EMV UN, the RNG of the POI must be used to generate EMV UN values, regardless of the Cardholder Verification Method implemented for that transaction. Note that the EMV UN generation process may incorporate other data such as internal registers and transaction data (see for example the EMV UN Generation algorithm at http://www.emvco.com.

POI Requirement B9

Q 1 **Is it acceptable for a device to have the ability to use Master Keys as both key-encryption keys for session key and as fixed keys—i.e., the Master Key could be used to encrypt PIN blocks and to decrypt session keys?**

A *No. A key must be used for one purpose only as required in ANSI X9.24 and ISO 11568.*

Q 2 **Is it acceptable to use the same authentication technique for loading both cryptographic keys and firmware?**

A *The technique may be the same, but the secrets used for authentication must be different. Example: If RSA signatures are used, the RSA private key used to sign cryptographic keys for loading must be different from the private key used to sign firmware.*

Q 3 **Is it acceptable to use TDES ECB mode encryption for session keys when using the Master Key/session key technique?**

A *Yes. TDES ECB mode can be used to encrypt session keys.*

Q 4 **Is it acceptable to load double-length 128-bit TDES key components into a device in smaller bit-values (e.g., two 64-bit parts held by key custodian 1 and two 64-bit parts held by key custodian 2)?**

A *Yes, provided the 128-bit cryptographic TDES keys (and key components) are generated and managed as full double-length 128-bit TDES keys during their entire life cycle in accordance with ANSI X9.24 and ISO 11568.*

For example, it would be acceptable to generate a full-length 128-bit TDES key component, but load it into the device as two 64-bit component halves.

It would not be acceptable to generate 64-bit keys or key components separately, and then concatenate them for use as a double length key after generation.

If key-check values are used to ensure key integrity, they must be calculated over the entire 128-bit key component or the resultant 128-bit key, but never on a portion of the key or key component. In addition, the resultant key inside the device must be recombined in accordance with PCI requirements and ANSI/ISO standards. Similarly for triple-length keys, the entire 192-bit key component or the resultant 192-bit key must be used to calculate the key-check values.

Q 5 **Under what conditions is it acceptable for a device to allow single component plain-text cryptographic keys to be loaded via the keypad?**

A *None. A device must not accept entry of single component plain-text cryptographic keys via the keypad. Full-length key components and encrypted keys may be loaded via the keypad if the requirements for sensitive functions are met* ***(PCI B5, B6)****.*

Q 6 **ISO 11568-2 *Symmetric ciphers, their key management and life cycle* and ANSI X9.24-1 *Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques* stipulate that any key that exists in a transaction-originating device shall not exist in any other such device. Does that apply to all secret and private keys contained in a device?**

A *The intent of the requirement is that the compromise of a key in one transaction-originating device (e.g., an EPP or POS device) does not impact the security of another similar device. In that regard, any private or secret key present or otherwise used in a transaction originating device must be unique to that device except by chance. This includes keys used for PIN encipherment, firmware validation, display prompt control or the protection of any of those same keys during loading to the device or storage within the device. Note that each of these functions requires its own unique key.*

This requirement applies to both vendor and acquirer-originated or controlled keys. This does not include public keys present or used by the device.

Q 7 **Devices may support the remote loading of secret acquirer keys using asymmetric techniques. Any such remote key-loading protocol must provide for a mechanism to minimize the probability of man-in-the-middle attacks where a device may be spoofed into communicating with a non-legitimate host. One common mechanism is to "bind" the host to the device such that the device will not accept communications that are not digitally signed by the legitimate host and authenticated by the device. Different scenarios exist where it may become necessary to change hosts and/or host asymmetric key pairs. When unbinding a host's key pairs from a device, which may be done manually at the device, or remotely using a digitally signed and authenticated command, are there any special provisions that must be made?**

A *Upon receipt of a valid instruction to unbind a host key pair from a device, the device must zeroize any existing acquiring entity's secret keys. Most scenarios involving a need to unbind a host are due to a change in the acquiring entity. In all cases though, the device must be initialized with new secret keys for the acquiring entity before placing the device back into service.*

Q 8 **TR-31 defines three keys. A key-block protection key (KBPK), a key-block encryption key (KBEK) and a key-block MAC key (KBMK). The KBPK is used to calculate the KBEK and the KBMK. Can the KBPK be used for any other purpose?**

A *No, in order to meet the requirement that a key is used only for a single purpose as defined in ANSI X9.24, the key block protection key is only used to calculate the KBEK and the KBMK, and is not used for any other purpose. Only the KBPK is used to generate the KBEK and the KBMK key; no other key is used for this purpose.*

Q 9 **TR-31 or an equivalent methodology must be used whenever a symmetric key is downloaded from a remote host enciphered by a shared symmetric key. Are there other circumstances where TR-31 or an equivalent methodology applies or does not apply?**

A *Devices must support TR-31 or an equivalent methodology for key loading whenever a symmetric key is loaded encrypted by another symmetric key. This applies whether symmetric keys are loaded manually (i.e., through the keypad), using a key-injection device, or from a remote host. It does not apply when clear-text symmetric keys or their components are loaded using standard dual-control techniques.*

Q 10 **In support of the conversion of deployed devices to the use of TR-31, can a key previously loaded for another purpose, such as a KEK, be re-statused as a TR-31 Key Block Protection Key.**

A *No, loading of a key into a slot (register) must set the slot to its given function. If the slot's function is changed - or if a new clear-text key is loaded into the slot without authentication using dual control - all other keys in the device (or at least all keys that were previously protected under the key that was previously in the slot) must be erased. This mechanism helps ensure that a device cannot be maliciously taken over.*

Q 11 May (update) 2018: TR-31 or equivalent support is required as an option for any device that allows the loading of symmetric keys that are encrypted by another symmetric key as a configuration option. To implement TR-31 or equivalent for devices that are currently implementing a non-TR-31 symmetric methodology, what characteristics must the device have to support this migration?

A *The device must enforce the following where applicable:*

- *The conversion from a less secure methodology (non-TR-31 or non-TR-31 equivalent) to a more secure (TR-31 or equivalent) methodology must be nonreversible.*
- *When entering the plain-text KBPK (or equivalent) through the keypad, it must be entered as two or more components and require the use of at least two passwords/authentication codes. The passwords/authentication codes must be entered through the keypad or else conveyed encrypted into the device.*

  These passwords/authentication codes must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Passwords/authentication codes that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/authentication codes are at least seven characters.

  Entry of key components without the use of at least two separate passwords/authentication codes results in the zeroization of pre-existing acquirer secret keys—i.e., the invoking of the key loading function/command causes the zeroization prior to the actual loading of the new key. For devices supporting multiple-acquirer key hierarchies (e.g., multi-acquirer devices), only the hierarchy (e.g., specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, authentication codes or similar) for each user on a given device must be different for each user.

- *Loading of a plaintext KBPK (or equivalent) using a key loader must be done using dual control and require the use of two or more passwords/authentication codes before injection of the key. These passwords/authentication codes are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least seven characters in length. These passwords/authentication codes must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Plain-text keys or their components are never permitted over a network connection.*

  Injection of plain-text secret keys or their components where the receiving device does not itself require the use of at least two passwords/authentication codes for injection results in the zeroization of pre-existing acquirer secret keys. For devices supporting multiple-acquirer key hierarchies (e.g., multi-acquirer devices), only the hierarchy (e.g., specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, authentication codes or similar) for each user on a given device must be different for each user.

- *It is not permitted to load the KBPK to the device encrypted by a non-TR-31 or non-TR-31 equivalent symmetric key. However, the KBPK may be loaded using asymmetric techniques.*

Q 12 The Guidance for DTR B9 states, "A device may include more than one compliant key-exchange and storage scheme. This does not imply that the device must enforce TR-31 or an equivalent scheme, but it must be capable of implementing such a scheme as a configuration option." If the use of TR-31 as the key-exchange mechanism is optional, must there be an explicit device configuration change to enable/disable TR-31 as the "active" key-exchange scheme?

A *Yes, an explicit configuration change is required. The change is considered a sensitive service and must meet the requirements of B5, protection of sensitive services.*

Q 13 August 2011: When a device is converted to or otherwise implements TR-31, the conversion must be one way. On a device supporting multiple independent key hierarchies, such as one designed to support multiple acquirers, does the implementation apply to all key hierarchies on the device?

A *No, a device supporting multiple independent hierarchies may implement TR-31 (or equivalent) on a hierarchy-by-hierarchy basis.*

Q 14 Are there any restrictions on how the terminal master key is loaded into the device?

A *The initial terminal master key (TMK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key may use asymmetric techniques, manual techniques, or the existing TMK to encrypt the replacement TMK for download. Keys are not allowed to be reloaded by any methodology in the event of a compromised device, which must be withdrawn from use.*

Q 15 Some devices allow the use of a decrypt data function that if not controlled may allow sensitive information—e.g., keys or PINs—to be output in the clear. How must a device protect against the outputting of sensitive data?

A *It must be managed using at least one of five techniques:*

- *The key-usage information of any downloaded key must be cryptographically bound to the key value using accepted methods, and the device must enforce that the key is only used for the intended use.*
- *The addition of a new key type (slot) subsequent to the initial configuration of the device causes the zeroization of all other secret keys, Devices supporting remote key-distribution techniques using asymmetric techniques shall only support the use of such techniques for the loading of TMKs. Support shall not exist to use remote key-distribution techniques for working keys (e.g., PIN, data, MAC, etc.) unless the key-usage information is cryptographically bound to each individual key.*
- *Downloaded data key types must not be accepted by the device unless enciphered by a different terminal master key than sensitive keys such as the PEK or MAC key types.*
- *The device does not provide any support for a decrypt data or similar function.*
- *The device must ensure that keys with different purposes can never have the same value; this requirement must be maintained until the device is decommissioned (or until the applicable TMK(s) changes).*

Q 16 May (update) 2018: Can secret keys or their components be used for other purposes such as passwords/authentication codes to enable the use of sensitive services?

A *No. The use of secret keys or their components for other purposes violates the requirement that keys be used for their sole intended purpose, e.g., key encipherment or PIN encipherment, etc.*

Q 17 September (update) 2016: The PCI PIN Security Requirements stipulate that any cryptographic device used in connection with the acquisition of PIN data that is removed from service must have all keys stored within the device destroyed that have been used (or potentially could be) for any cryptographic purpose. If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys. Does this apply only to symmetric keys?

A *No, this applies to any secret or private key used by the device for PIN encipherment, firmware validation, display prompt control or the protection of any of those same keys during loading to the device or storage within the device, including private keys used in connection with remote key distribution using asymmetric techniques. This requirement applies to both vendor and acquirer-originated or controlled keys. This does not include public keys present or used by the device.*

The vendor must provide decommissioning instructions and associated mechanisms for rendering all such keys non-recoverable to an adversary that are verifiable by the evaluation laboratory. These techniques include, but are not limited to:

- *Specific menu commands to zeroize stored keys*
- *Inducement of a tamper event to zeroize those keys*
- *Encryption by a key of equal or greater strength that is itself zeroized, i.e., only cryptograms of the protected keys are recoverable.*

Q 18 May 2018: ANSI TR-34 describes two protocols for implementing the distribution of symmetric keys using asymmetric techniques. The two techniques are described as the Two Pass method and the One Pass method and should be used as follows:

- **The Two Pass method is appropriate for where the POI and KDH can communicate in real time. It uses random nonces for the prevention of replay attacks.**
- **The One Pass method is appropriate for environments where the POI and KDH will not be able to communicate in real-time—i.e., the POI cannot initiate the sequence of cryptographic protocol messages. In these environments, the KDH will generate the cryptographic message that can be transported to the POI over untrusted channels in non-real time. It includes the use of time-stamps in lieu of random nonces to prevent replay attacks.**

The malicious keying of a POI device by a second KDH under the same PKI is possible where the POI has already exchanged credentials with a first KDH. In order to prevent this attack, binding (or an equivalent method as noted in the DTR B9 guidance) is necessary for all POI devices, and is a pre-requisite for both the Two Pass and One Pass key exchange protocols.

Are POI devices required to support both methods?

A *No, a device may support only one. Whether the device supports only one or both, the vendor must describe in the device's security policy that is posted to the PCI website the environments and circumstances under which it is appropriate to implement the supported method(s).*

Q 19 September 2020: PIN Security Requirement 18-3 requires the implementation of key blocks. Interoperable methods include those defined in ASC X9 TR-31 and ISO 20038. The requirement also allows for any equivalent method whereby the equivalent method includes the cryptographic binding of the key-usage information to the key value using accepted methods. How are equivalent methods determined?

A *Equivalent methods must be subject to an independent expert review and said review is publicly available for peer review:*

- *The review by the independent expert must include proof that in the equivalent method the encrypted key and its attributes in the Key Block have integrity protection such that it is computationally infeasible for the key to be used if the key or its attributes have been modified. Modification includes, but is not limited to:*
  - *Changing or replacing any bit(s) in the attributes or encrypted key*
  - *Interchanging any bits of the protected Key Block with bits from another part of the block*
- *The independent expert must be qualified via a combination of education, training and experience in cryptology to provide objective technical evaluations that are independent of any ties to vendors and special interests. Independent expert is further defined below.*
- *The PTS laboratory will validate that any device vendors implementing this methodology have done so following all guidelines of said evaluation and peer review, including any recommendations for associated key management.*

An Independent Expert possesses the following qualifications:

- *Holds one or more professional credentials applicable to the field, e.g., doctoral-level qualifications in a relevant discipline or government certification in cryptography by an authoritative body (e.g., NSA, CES, or GCHQ) and*
- *Has ten or more years of experience in the relevant subject and*
- *Subscribes to an ethical code of conduct and would be subject to an ethics compliance process if warranted and*
  - *Has published at least two articles in peer-reviewed publications on the relevant subject or*
  - *Is recognized by his/her peers in the field (e.g., awarded the Fellow or Distinguished Fellow or similar professional recognition by an appropriate body, e.g., ACM, BCS, IEEE, IET, IACR).*

Independence requires that the entity is not subject to control, restriction, modification, or limitation from a given outside source. Specifically, independence requires that a person, firm or corporation who holds itself out for employment as a cryptologist or similar expert to more than one client company is not a regular employee of that company, does not work exclusively for one company and where paid, is paid in each case assigned for time consumed and expenses incurred.

Q 20 September 2020: Devices must support the ANSI TR-31 key-derivation methodology for TDES keys, and for AES keys must support either the TR-31 methodology or the ISO 20038 methodology. In either case, equivalent methods can be used where subject to an independent expert review and said review is publicly available as described. What characteristics enforced in TR-31 and ISO 20038 must be considered in determining equivalence?

A *"Equivalency" must be demonstrated in the context of security proofs. The equivalent method must provably accomplish the functions of key integrity, restricting key usage, preventing key reuse, and the secrecy of keys. Specifically, an equivalent key block scheme must minimally offer the following properties:*

a) *It must prevent the loading of PIN, MAC, and/or Data keys - or any keys used to manage these within the key hierarchy - from being used for another purpose. IPEK, KEKs, and derivation keys must be uniquely identified where supported.*
b) *It must prevent the determination of key length for variable length keys.*
c) *It must ensure that the key can only be used for a specific algorithm (such as TDES or AES, but not both).*
d) *It must ensure a modified key or key block can be rejected prior to use, regardless of the utility of the key after modification. Modification includes changing any bits of the key, as well as the reordering or manipulation of individual single DES keys within a TDES key block.*
e) *Where different key block formats are supported, with some providing the above protections and some not, it must be humanly readable from the key block prior to loading/use which format is implemented. E.g., by looking at the commands sent to the device.*
f) *It must support all symmetric algorithms implemented by the device(s) that are to use the key blocks.*
g) *Where asymmetric algorithms are supported, the algorithm type, padding and signature formats must be identified in the key block.*
h) *It must use NIST approved modes of operation, with separate keys used for confidentially and authenticity. Any keys used must not be related in a reversible way.*

The equivalent key block may optionally support other characteristics such as:

i. A key version number that prevents the use of older or expired keys.
ii. Support for key 'direction' (uni-directional keys) so that a MAC key may be identified as 'verify only', or a data key as 'encrypt only'.
iii. Support for key purposes other than PIN, MAC, and Data.
iv. Support for both TDES and AES (where devices implementing the key blocks only support one of these algorithms – transitional only – new devices must support AES).
v. To implement confidentiality controls over any key metadata other than the key length.
vi. Support for asymmetric algorithms.

Q 21 **September 2020: POI devices are required to support key blocks using the ASC X9 TR-31 key-derivation methodology for TDES keys, and for AES keys must support either the TR-31 methodology and/or the ISO 20038 methodology. TR-31 and ISO 20038 are methods to package keys (the key blocks) for conveyance or storage, but they use symmetric mechanisms for that and for key conveyance require a symmetric key exchange key that is pre-shared for use as the key block protection key. Where a symmetric key is not previously established with a POI device for remote key distribution, and asymmetric methods will be used, is it required to support a key block methodology?**

A *Yes. A method such as ASC X9 TR 34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport must be used. Under TR-34, similar to TR-31 and ISO 20038, the Key Block consists of three parts:*

- *The Key Block Header (KBH) which contains attribute information about the Key and the Key Block*
- *The confidential data that is being exchanged/stored*
- *The Key Block Binding Method.*

However, TR-34 uses asymmetric methods for the Key Block Binding Method, instead of the symmetric methods used in TR-31 or ISO 20038 which require that a symmetric key was previously exchanged between the POI device and the KDH.

POI Requirement B10

Q 1 **June (update) 2016: Requirement B10 states that any method used to produce encrypted text that relies on "non-standard" modes of operations (for example, format-preserving Feistel-based Encryption Mode (FFX)) shall be approved by at least one independent security-evaluation organization (for example, a standards body) and subjected to independent expert review. How is this requirement met if the method is not included in a published standard?**

A *All account data shall be encrypted using only ANSI X9 or ISO approved encryption algorithms (for example, AES, TDES). Additionally, the mode of operation that is used shall be either:*

1. *One that is described in ISO/IEC 10116:2006 (or equivalent) and follows secure padding guidelines.*

OR

2. *Exist on a draft standard from a standards body applicable to the financial payments industry i.e., ANSI, ISO or NIST*

AND

3. *Be subject to an independent expert review and said review is publicly available and is reviewed by the PCI PTS evaluation laboratory.*

The review by the independent expert must include proof that this FPE secures against "Message Recovery" as defined in Bellare, M., Ristenpart, T., Rogaway, P., & Stegers, T. (2009, August). Format-preserving encryption. In Selected Areas in Cryptography (pp. 295-312). Springer Berlin Heidelberg (https://eprint.iacr.org/2009/251.pdf).

The independent expert must be qualified via a combination of education, training and experience in cryptology to provide objective technical evaluations that are independent of any ties to vendors and special interests. Independent expert is further defined in the glossary.

The PTS laboratory will validate that the device vendor has implemented the FPE solution following all guidelines of said evaluation and peer review, including any recommendations for associated key management.

POI Requirement B12

Q 2 **Can a device use a key-encrypting key to encrypt or decrypt key-tag information along with a key?**

A *Yes, associated key-tag information such as the algorithm, key expiration, usage, or key MAC may be encrypted or decrypted along with the key using a key-encrypting key. The key and its tag are bound together using a chaining mode of encipherment as defined in IS0 10116.*

POI Requirement B15

Q 1 What is the definition of "cryptographic unit"?

A *The cryptographic unit is the microprocessor that encrypts the PIN block. This processor is subject* to *PCI device requirements*, *and is therefore considered secure when within a compliant device. This means that a general-purpose micro-controller can be used as long as it is within a device that complies with PCI device requirements.*

Q 2 Is it acceptable to use an LED controlled exclusively by the crypto-processor as the prompt for PIN entry?

A *No. Cardholders expect the prompt for PIN to come from the same display as other prompts. If it does not, there is a greater possibility of cardholders being misdirected.*

Q 3 Would the display of plain-text PIN digits by the device qualify as tamper evidence?

A *No. The cardholder may not be familiar with the typical behavior of a given device and may not recognize that the device is violating Requirement B3.*

Q 4 If a terminal includes a display under its control and a keypad with its own display, must the cryptographic unit of the device control both displays?

A *Yes. If a single device has two displays that could prompt the cardholder for data, then both displays would be governed under B15. This means the terminal and keypad are a single device that must meet PCI requirements.*

Q 5 Cryptographic keys used for updating display prompts must be managed under the principles of dual control and split knowledge, and any secret or private keys used must not appear in the clear outside of a secure cryptographic device. Can the authentication data used to enable use of a signing or MACing key travel through an unprotected environment—e.g., the unprotected RAM of a computer?

A *The authentication data may exist in the clear outside of a secure cryptographic device. However, the vendor must provide to the lab customer instructions for using a secure room, dedicated PC, implementation of dual control techniques, equipment inspection procedures, etc.*

Q 6 What logging requirements must be met by an SCD under B15?

A *The logs must provide sufficient evidentiary matter to demonstrate to the lab that the control techniques and mechanisms specified by the vendor exist.*

Q 7 May (update) 2018: Can USB authentication tokens or smart cards be considered to be the SCD required to enforce dual control under B15?

A *The use of dual tokens alone would not meet the requirement. The tokens would need to enforce the use of passwords/authentication codes, and they would need to include security to protect their contents.*

Q 8 **May 2011: If a device complies with B15, what are the requirements for controlling the updates of these prompts?**

A *B15 is assessed when a device uses firmware updates to control the changing of display prompts. Therefore, updating of prompts for devices that comply with B15 requires the creation of a new firmware version, and a resultant change in the firmware version number of the PED.*

It is not acceptable to have vendor-controlled prompts that are updated separately of the firmware, without the generation of a new firmware version. It is acceptable for prompt updates to use a separate cryptographic key to that used for other firmware updates—but any separate update method must be assessed by the laboratory as being compliant to Requirements E2 and B2. At all times, the cryptographic keys used to update prompts and firmware must be different than those used to update non-firmware code, such as applications.

Q 9 **May 2011: If a device complies with B15, does this mean I need to re-submit the device for lab evaluation every time I change the prompts?**

A *If there are suitable wildcards in the firmware version listing to accommodate new prompt versions that have been previously reviewed and confirmed as appropriate by a PCI laboratory, the review of each change by a PCI laboratory is not necessary.*

Q 10 **May 2011: Requirement B15 does not specify any minimum attack potential. What requirements are placed on the physical security of a device that allows for display prompts to be updated by third parties using cryptographically based controls?**

A *All prompts that may be used to request plaintext data entry from the cardholder must be secured against an attack potential of at least 18 PCI points with a minimum of 9 for exploitation. This includes prompts that may be updated by third parties using cryptographically based controls.*

Q 11 **March 2015: PIN pads designed for use with ATMs typically support both a secure (encrypts the data entered) and non-secure state. Does the transition between states require authentication?**

A *Yes, cryptographic mechanisms consistent with Appendix D of the POI Derived Test Requirements must be used for the authentication. Specifically:*

- *A secure channel is required between the PIN pad interface and the (ATM) controller to manage changes between PIN and plaintext data entry modes*
- *For touchscreens, the management of the keypad "buttons" is done in a secure way to prevent the determination of the customer PIN through exploitation of potential differences in the displayed keypad and the organization of the numeric buttons on the touch interface.*

This is not to imply that the device must force the implementation, but rather that it must provide support for such an implementation.

POI Requirement B17

Q 1 **August 2011: The operating system of the device must contain only necessary components and must be configured securely and run with least privilege. What is considered an "operating system" for PCI purposes?**

A *In the scope of PCI-PTS, any underlying software providing services for code running in the device is considered part of the operating system. Examples of such services include system initialization and boot, hardware abstraction layers, memory management, multitasking, synchronization primitives, file systems, device drivers, and networking stacks. Services that provide security or may impact security are, in addition, considered firmware.*
Operating systems may range from hardware abstraction layer libraries and embedded micro-kernels to complex, multi-user operating systems.

POI Requirement B18

Q 1 **What are acceptable methods of meeting this requirement?**

A *The use of accepted key-management techniques will typically satisfy this requirement:*

- *When Master/session key-management technique is used this requirement is met because successful key substitution requires the attacker to know the Master Key contained within the device.*
- *This requirement is satisfied when using DUKPT key-management technique because the PIN keys are derived from secret information contained within the device.*

However, when the device is intended to support multiple acquirers and the acquirer is selected by a user (i.e., merchant pressing a button), the device must verify that the correct acquirer has been chosen.

Q 2 **Is it acceptable for a device that supports multiple key hierarchies to meet B18 by ensuring that specific applications can only access keys that are associated with them?**

A *Yes. It is acceptable provided each application can only access a single key-hierarchy's keys.*

Q 3 **What are acceptable means of external cryptographic keys selection?**

A *Keys may be selected through the device keypad, or commands sent from another device such as an electronic cash register. Any commands sent from another device must be cryptographically authenticated to protect against man-in-the-middle and replay attacks.*

Q 4 **If a key externally selected is not the encryption key used to directly encrypt the PIN block, is this selection required to be authenticated?**

A *If the external selection is associated with the PIN encryption, the authentication would apply. For example, externally selecting the Master Key under which a session key will be decrypted for use in PIN block encryption would need to be authenticated.*

Q 5 **Is it acceptable for PIN keys to be externally selected indirectly by selecting the acquirer if the acquirer selection is performed with a cryptographically authenticated command? It is assumed that there are multiple key hierarchies related to PIN encryption under each acquirer.**

A *Yes, as long as there is a mechanism that ensures that keys under each acquirer are associated exclusively with that acquirer.*

Q 6 **May (update) 2018: External key selection includes selection performed by either a local or remote host. Under what circumstances is a device supporting multiple key hierarchies not required to enforce authentication for each external key-selection command?**

A *If an application can select keys from multiple key hierarchies, the device must enforce authentication of commands used for external key selection. If the device only allows an application to select keys from a single hierarchy, then command authentication is not required.*

Alternatively, authentication is not required under either of the following two circumstances:

- *Key hierarchies for PIN encryption are only established directly by the vendor at its secure facility or at an authorized facility operated by a third party that regularly performs key loading on behalf of the vendor and is registered to do so under applicable payment brand rules; and subsequent to leaving the facility it is physically and/or logically impossible to load additional key hierarchies without returning to the facility.*
- *Key hierarchies can only be established in accordance with Requirement B7. New key hierarchies must be authenticated using dual control (passwords/authentication codes) either via the key loader or directly via the EPP or POS PED. Existing key hierarchies may be replaced without using authentication if the loading results in the zeroization of pre-existing secret keys—i.e., the invoking of the key-loading function/command causes the zeroization prior to the actual loading of the new key. In addition, existing key hierarchies may be replaced or new key hierarchies may be established through the use of remote key distribution using asymmetric techniques that are in compliance with the PCI PIN Security Requirements, Annex A.*

Q 7 **When is B18 not applicable to acquirer-controlled display prompt devices?**

A *B18 is not applicable to acquirer-controlled display prompt B devices that do not include commands for external key selection, or cannot hold multiple keys related to PIN encryption.*

POI Requirement B20

Q 1 **June 2015: Is there any impact on the device's approval if the laboratory evaluated security policy is changed by the vendor?**

A *Beginning with V4, the content of the security policy is part of the evaluation of a device by the laboratory and is an integral input upon which the approval of a device is based. Deployers rely on the security policy in order to ensure that they do not breach the conditions of a device's approval. Any change to the security policy which impacts on the security requirements of the device must be evaluated in order for the device to remain approved. Additionally, any change to the functionality offered by the device impacting information required to be contained in the security policy must be reflected in an update to the listed security policy document.*

Depending on the nature of the changes, this may be reflected in updates (e.g., appendices) to an existing security policy, or as additional security policies posted to the website. In all cases, all approved product versions must be addressed in security policies posted to the PCI website.

Q 2 **October (update) 2018: The PCI PTS Lab Requirements prohibit a PTS lab from creating any vendor documentation. Are there any scenarios where a PTS lab may assist a vendor in creating documentation?**

A *In some cases, a PTS lab may revise a Security Policy for grammar, formatting, or spelling edits for a device under evaluation. This may be done to assist the vendor in creating a document sufficient to be submitted to PCI. In this case, the PTS lab will provide the following as part of the evaluation report submission:*

- *A track-changed/redlined version of the edited Security Policy, showing the original text created by the vendor as well as the updated text.*
- *A clean copy of the edited Security Policy for posting.*

POI Requirement B21

Q 1 **ISO 9564 stipulates that if the PIN is to be submitted to the IC card in enciphered form, then the device shall encipher the PIN using the authenticated encipherment key of the IC card and submit the enciphered PIN to the IC card. Are there any restrictions on where the authentication must occur?**

A *The device must protect the integrity of all public keys (ICC, applicable issuer, and payment brand) using techniques defined in ISO 11568. In all cases the authentication must occur in a secure component of the device, such as the PIN pad or ICCR. This includes the authentication of the ICC public key(s) as well as the associated issuer public key in the certificate chain up to the applicable payment brand key.*

POI Requirement B23

Q 1 **June 2012: The guidance states that encrypting mode is defined to be when the device's encryption of account data functionality is enabled and operational. Can a device output all or some account data in the clear when in encrypting mode?**

A *Yes, even for devices that only support encrypting mode. For example, a device can implement cryptographically authenticated whitelists for outputting account data in the clear, even if that whitelist causes all account data to be output in the clear. The absence of the whitelist causes all account data to be encrypted.*

POI Requirement E2

Q 1 **Many devices are designed so that third parties can create and load applications. Vendors often support this by providing third parties the tools needed to create and load applications. How can a vendor ensure that it is not responsible for controlling the application?**

A *If applications are not considered firmware, they do not need to be controlled by the vendor. The device design must prevent applications from impacting functions and features governed by the requirements. Examples of functions that must not be influenced by "non-firmware" applications include: key management (key selection, key authentication, key generation, key loading, etc.), self-tests, time between PIN block encryptions, access to sensitive services, limits on sensitive services, firmware update and authentication, tamper response, etc.*

Alteration of prompts by third parties is a special case that can be impacted by non-firmware applications provided that PCI POI B15 is met.

SRED applications developed by third parties are also an exception. They must meet all applicable criteria in the SRED module, including any associated FAQs.