Payment Card Industry (PCI)
POS PED Security Requirements and EPP Security Requirements

Technical FAQs for use with Version 2.0

July 2010

Table of Contents

Section 1: POS PED Evaluation *Frequently Asked Questions*

These technical FAQs provide answers to questions regarding the application of PCI's (Payment Card Industry) physical and logical POS PED security requirements as addressed in the *PCI POS PIN Entry 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 PED application includes prompts for non-PIN data and the PED enforces PCI Requirement A8.3 compliant controls, can it be listed as a class B device with the application excluded from the PED 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 PED.*

Q 2 When is an "N/A" response to a requirement acceptable?

A *An "N/A" response is acceptable in two cases: First, if compliance is achieved by meeting another requirement option, such as meeting A1. Second, if the characteristics governed by the requirement are absent in the PED, such as A5 if the PED does not emit any audible tones. The evaluation laboratory will verify that all responses are appropriate.*

Q 3 What is the definition of "Secret Information?"

A *"Secret information" is any cryptographic keys or passwords that the PED relies on to maintain security characteristics governed by PCI requirements.*

Q 4 Some components of a PED may include cryptographic keys that cannot be erased. Are there any instances when this would be acceptable? See Requirements A1 and A7.

A *Cryptographic keys that are never used to encrypt or decrypt data; or are not used for authentication, do not need to be considered secret data, and therefore do not need to be erased.*

Q 5 What type of epoxy is acceptable for encapsulation?

A *Acceptable epoxy will possess the following characteristics:*

- *Opaqueness: Epoxy must be opaque in the visible spectrum.*
- *Hardness: Epoxy must be hard enough so that a sharp object cannot be used to penetrate the epoxy to the depth of the underlying circuitry.*
- *Tamper Evidence: The epoxy must show visible evidence of tamper when an attempt to penetrate the epoxy with a sharp object is made.*
- *Adhesion: Epoxy must resist attempts to forcibly separate it from the circuit board. When enough force is applied to remove the epoxy, severe damage should result such that the device is non-functional.*

Q 6 Is it assumed that the surface of the potted area is visible without disassembly of the PED?

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

Q 7 Is it acceptable for a PED 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 8 Vendors are allowed to make revisions to approved devices, provided the changes are evaluated by an approved lab. What limits are placed on the number and type of changes that are allowed?

A *The large number of possible changes and their impacts cannot be determined in advance. Changes will be assessed on a case-by-case basis. Vendors should contact one of the recognized laboratories for guidance. Laboratories will consult with PCI on an as needed basis to determine if a change is too great to be addressed under the delta process. In all cases, changes that impact security require assessment. The laboratories will determine whether the change impacts security.*

Revisions to approved devices are termed "deltas." Delta reviews involve the laboratory assessing the changes based on the current major version (e.g. 1.x, 2.x, etc.) of the requirements that were used for the approval of the device. Examples of deltas include:

- *Revisions to existing firmware or hardware on existing approved devices to add or modify functionality*
- *Adding EMV level 1 to an existing approval*
- *Maintenance fixes on devices that have expired and are no longer approved for new deployments*
- *Assessment of a device for offline PIN entry where the existing approval is only for online PIN entry, or vice versa*
- *The porting of a new set of firmware to an existing approved device.*

Q 9 Does the PED and ICC reader have to show the version numbers of the hardware, firmware and Application?

A *The PED and ICC reader must show the version numbers of hardware and firmware like they have been approved and they are shown in the list of approved devices. The hardware number must be shown on a label attached to the PED and ICC reader. The firmware number and optionally the hardware number must be shown on the display or printed during startup or on request.*

Q 10 Does the use of protective keypad overlays impact the approval status of a PED?

A *In general, overlays are not supported by the PED approval program due to the potential for keypad tapping. Overlays may be used where they do not cover any portion of the PIN entry area. For example, in a touchscreen device whereby 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 11 Is it acceptable to make changes to an approved device's hardware or firmware and keep the existing version #s?

A *No. Any hardware changes to an approved device that has been deployed must result in a new hardware version #. Any firmware changes to an approved device must result in a new firmware version. As described in the PCI PTS Device Testing and Approval Program Guide vendors may use a combination of fixed and variable alphanumeric characters in the version numbers. However, variable characters are not permitted for any physical or logical device characteristics that impact security. Device characteristics that impact security must be denoted using fixed characters. The use of variable characters shall be validated by the test laboratory so as to not impact security. The use of variable characters is appropriate to delineate differences such as country usage code, customer code, communication interface, device color, etc.*

Q 12 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 13 When submitting hardware and/or firmware changes on existing approved devices, must a vendor submit the device to the same lab as the one that did the initial evaluation?

A *Vendors may select a different lab then the lab that was used to perform the initial evaluation. However, the subsequent lab is free to determine the level of reliance they wish to place upon the prior lab's work, which may result in additional work than would otherwise be necessary. For version 3 reports, the delta lab or the final form factor lab shall have access to the prior lab's report(s), including any delta or OEM component reports subsequent to the original evaluation. If those reports are not available, then the delta lab shall decline the engagement or else must complete a full evaluation of the device.*

Q 14 The DTRs indicate that software developed to enable an attack can be considered bespoke equipment (Appendix B, under "Equipment"). Does this mean that PIN-disclosing bug software should be considered bespoke equipment?

A *Software required for a PIN-disclosing bug is typically straightforward to implement and would not be considered bespoke. Bespoke software would be software that requires significant time and expertise to develop such as is required for side channel attacks. PCI requires strong justification to be provided when bespoke equipment is indicated as necessary for an attack.*

Q 15 How do the point calculations take into account the development of a PIN-disclosing bug? Does PCI provide fixed values for use by the labs?

A *PIN bugs must often be customized for a specific PED. Due to numerous possible variations in bug form, function, and complexity, PCI does not provide standard point values for PIN bugs. The evaluation lab is responsible for addressing this as part of the PED evaluation. The development of an appropriate PIN-disclosing bug is to be included in the Identification calculation, as are other aspects of attack development.*

Q 16 When can multiple devices be costed in the calculation to support the compliance of a device to those requirements that have a minimum attack potential?

A *The requirement for multiple devices during either the identification or the exploitation phase of an attack cost calculation depends upon the difficulty of attacking a device, and the risk that the device may be tampered during the attack. However, PCI expects that most attacks can be performed with only one or two samples in the identification phase, and a single sample in the exploitation phase. Strong justification explaining why multiple sample devices are necessary must be provided when such additional samples are necessary to meet the minimum attack potential.*

Q 17 Are PC-based instruments like protocol sniffers, USB attached oscilloscope adapters and graphical multimeters, etc. considered standard or specialized equipment.

A *PC-based instrument like those mentioned above shall be considered standard equipment, especially if they do not require dedicated hardware or adapters.*

Q 18 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 cost 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 is to be considered only for the identification of the general device setup and the property to be attacked (e.g., the interface type).*

Q 19 If a device is submitted for evaluation of offline PIN entry, is it acceptable for the device to only support plaintext PIN or to only support enciphered PIN?

A *No. In order to receive an approval for offline PIN entry, a device must be capable of supporting both plaintext and enciphered PIN.*

Q 20 Several requirements, such as those for access to sensitive services, key loading, and removal detection, provide for the use of authentication using passwords or PINs. Are there any restrictions on this type of authentication data?

A *Yes, any passwords, PINs or similar used to meet a PCI requirement must be at least a five character minimum. These passwords/PINs must either be unique per device (and per user where dual control is required), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Passwords/PINs that are unique per device can be made optionally changeable by the acquirer or their agent (e.g., merchant), but this is not required. These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device. In all cases, the authentication values (passwords, PINs or similar) for each user on a given device must be different for each user.*

Q 21 Kiosks and other unattended devices may be constructed using either EPPs or POS PEDs for use in PIN entry. EPPs must meet requirement A8 for removal detection. If a POS PED is used in an unattended device, does it have to meet the requirement for removal detection?

A *Yes, any PIN acceptance device used in ATMs or UPTs must meet the criteria for removal detection. POS PEDs that are intended to be used as either an unattended POS device or housed within an ATM or UPT must be evaluated against EPP requirement A8 for removal detection. POS PEDs that are used for PIN acceptance in an ATM or UPT and which have not been evaluated against EPP requirement A8 are not considered approved when used in that fashion.*

Q 22 In occurrences where it is necessary to return a device to the device vendor for maintenance, are there any restrictions on what must happen to the secret keys in the device?

A *When a device is returned to the vendor for maintenance, mechanisms must be in place to automatically cause the erasure of all previously loaded Acquirer secret keys upon servicing the device. (e.g., loading a new public RSA key causes the erasure of all previously loaded secret keys)*

Q 23 Security requirements are normally available for a four year period from date of publication for new evaluations of products. Products are approved until six years after the retirement/expiration of the version of security requirements against which they were approved. This results in approvals that are a minimum of six years and a maximum of ten years, depending on the timeframe in which the approval occurs in relations to the life cycle of the applicable security requirements. Modifications for approved devices, termed deltas, can occur at any time during the products approval.

Can products for which the approval has expired undergo deltas?

A *Yes. Vendors may need to make maintenance fixes to devices that the vendor has already sold, but must still provide support for. In addition, vendors may wish to port updated versions of firmware that were approved against newer security requirements to products for which the approval has expired. This may occur because customers of a vendor wish to standardize their deployment against a given version of firmware and/or to add functionality to that device.*

Q 24 Technical FAQs are updated on a regular basis, and add clarifications for the application of defined security requirements. Are new FAQs applicable to devices that are currently in evaluation? Furthermore, must FAQs that were not in existence at the time of the original evaluation be considered in subsequent delta evaluations?

A *Yes. Technical FAQs not only add clarifications to requirements in order to provide a consistent and level playing field in the applications of those requirements, but may also address new security threats that have arisen. As such, technical FAQs are generally effective immediately upon publication.*

The intent is not to cause a device in evaluation to fail if otherwise it would not unless known exploitations exist. Unless such an exploitation exists, a product currently in evaluation will generally not be subject to new FAQs issued during the product's evaluation. This does not exempt a product from the applicability of the FAQ if the product must be reworked and resubmitted at a later date because of other issues that cause it to fail the evaluation. The product is also subject during delta evaluations to any FAQs issued subsequent to the original approval, even though the FAQ impacts an area that is not part of the modification made by the vendor.

In all cases, the evaluation laboratory must advise PCI SSC of the circumstances and PCI SSC will make the final decision based upon the circumstances. Additionally, for both new and delta evaluations, the laboratory will also state in their submission the security requirements used in the evaluations, as well as the publication date of the technical FAQs used.

Q 25 Compound devices, such as Unattended Payment Terminals, may be evaluated as part of a single evaluation of all applicable components, or may be evaluated with one or more previously approved OEM components. Where a compound device incorporates previously approved components, what considerations must be made for the evaluation?

A *There are several considerations:*

- *UPT evaluation reports containing separately approved OEM components must at a minimum contain a summary table of all requirements (whether Yes or N/A) of any module that is relevant to the final form factor of the UPT. This table may reference the pertinent OEM component for compliance to any specific requirement.*
- *All requirements impacted (e.g., additional cardholder input mechanisms, displays, controllers, removal detection, etc.) by the final form factor of the UPT must be addressed in detail for each impacted requirement.*
- *Where the lab evaluating the final form factor is not the same lab as the lab that evaluated OEM component(s), the lab **should** have access to the OEM component lab report(s). If those reports are not available, e.g., because submitting vendors are different or for any other restriction, the lab must determine the extent of additional work required.*
- *If the lab is unable to place reliance, where necessary, on information that is available in reports that are not available to the lab, and the lab is unable to perform the degree of necessary additional work to achieve such reliance, then they must decline the engagement.*
- *In all cases, PCI SSC may reject the report if in the judgment of PCI SSC the report does not contain adequate information to substantiate the conclusions of compliance to overall UPT criteria.*

Q 26 Are OEM components, such as EPPs, approved against an earlier version of security requirements allowed for use in achieving an overall UPT approval without additional testing of requirements that were already evaluated, even if those requirements were updated as part of the POI v3 security requirements?

A *OEM components approved against earlier security requirements are only allowed for use in obtaining an overall UPT approval evaluation without additional testing of those components if they are no more than one major version of requirements earlier. For example, EPPs evaluated and approved using PCI EPP v2.x can be used without additional testing of requirements they have previously met as part of an overall POI v3 evaluation. However, EPPs that were evaluated and approved using PCI EPP v1.x must undergo a full evaluation against all applicable POI v3 requirements.*

In addition, other modules such as Integration, SRED and Open Protocols, as well as additional individual security requirements in POI v3 that were not previously evaluated shall still apply if applicable to the overall UPT evaluation. Furthermore, for devices that embed other PCI-approved devices, and are therefore basing their security on these sub-components (even partially), the renewal/expiration date shall be the earliest to expire date among all evaluations, including the embedded device itself.

Q 27 **UPT version 1 shall no longer be 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 which 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 28 **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 their 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 29 **The program manual states that hardware and firmware version number identifiers may consist of a combination of fixed and variable alphanumeric characters, whereby a lower "x" is used by PCI to designate all variable fields. The "x" represents fields that the vendor can change at anytime to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device color, etc. What are examples of options that can not be addressed by use of a variable field, but must be addressed by a fixed character?**

A *Options that cannot be a variable character include those that directly pertain to meeting security requirements. For example, requirements exist for magnetic stripe readers (MSRs) and integrated circuitry card readers (ICCRs). A variable character cannot be use to designate whether a device contains a MSR or ICCR. A requirement exist for the deterrence of visual observation of PIN values as they are being entered by the cardholder, which can be met by privacy shields or the device's installed environment or a combination thereof. It is not appropriate to wildcard options if the device supports more than one means of observation deterrence.*

Q 30 **The program manual stipulates that "Vendors or other third parties licensing approved products from other vendors to market or distribute under their own names are not required to pay a new evaluation fee if the only change is to the name plate. If firmware or other hardware changes are made that require a PCI-recognized test laboratory to evaluate the changes for potential security impact, then the licensee shall be required to pay the new evaluation fee. In all cases the licensed device will receive a new approval number and the licensee vendor or third party shall be billed the annual listing fee for each such approval."**

What are additional considerations for a third party to license an approved product from a vendor, whereby the third party wants to distribute it as their own product?

A *There are several additional considerations:*

- *The licensee vendor cannot directly make the request. The licensor vendor must make the request on their behalf.*
- *All such requests must be received by PCI SSC as a delta letter from one of the PCI SSC PTS recognized laboratories. If the only change is to the nameplate of the product, there is not any new evaluation fee (currently $2,000), but as noted above, there will be an annual listing fee (currently $1,000).*
- *There is not any requirement for the licensee's version of the product to reference or list the original vendor.*
- *Products may be licensed from another vendor even if the version of the security requirements against which the original product was approved is retired from use for new evaluations, as long as the approval has not expired.*
- *As noted, licensed products requiring physical and/or logical changes will incur a new evaluation fee. However, as long as the original vendor continues the manufacture of the device on behalf of the licensee vendor, the licensed product can be evaluated against the security requirement's version against which the original product was evaluated and approved, even though those requirements may be expired for new approvals.*
- *If the licensee vendor wishes to directly manufacture the licensed product, or have a third party other than the original vendor manufacture the licensed product on their behalf, then the product must be reassessed as a new evaluation against the current version of security requirements, unless the licensor vendor can demonstrate that it retains both the intellectual property and engineering control. This is due to the potential for changes in plastics, etc. that may impact the security of the device.*

POS Requirement A1

Q 31 **Do attack scenarios considered under A1 include replacement of the enclosure to conceal tamper evidence?**

A1 allows the evaluator to use any *method of attack feasible against the terminal limited only by the attack potential of 25. The POS PED must be able to withstand attack from any side, including front and rear case replacement up to the attack potential value.*

Q 32 **The Derived Test Requirements of A1 have the Guidance note: "Attack scenarios should consider keypad removal or replacement associated with unattended payment terminals, such as in connection with overlay attacks." How can this be addressed by the device's design?**

A *Since in vending machines or other unattended acceptance/payment terminals only the keypad area of a PED is usually visible to the cardholder, attacks may be mounted which use PED removal and the insertion of keypad overlays or keypad substitutes as an attack element. These attacks may be easier to perform than direct attacks to the PED. The attack scenarios must therefore consider removal/replacement attacks as part of an overall attack scenario. The PED must have design properties to detect and respond to removal/replacement attacks. Examples of countermeasures include, but are not limited to, removal detectors, movement detectors, special mounting brackets or special keypad designs. Future releases of the requirements will require specific countermeasures.*

Q 33 Requirements A1 and D1 specify minimum attack potentials of 25 for the PED and 16 for the ICC reader for penetration attacks designed to determine or modify sensitive data. In Version 1 requirements, alternative options included meeting a minimum of ten hours of exploitation time. Does exploitation time enter into either of these two requirements?

A *Yes. In addition to the specified minimum attack potential values, any feasible penetration attack against either the PED or the ICC reader for the purpose of determining or modifying sensitive data must entail at least ten hours of exploitation time.*

Q 34 Are there circumstances under which a PED can comply with Requirement A1 while employing one tamper switch to protect the keypad area?

A *No. If switches are used as the primary protection for the area around a physical keypad area, then at least three blind, tamper switches must be implemented. The switches must be protected from attacks that use the application of adhesives or conductive liquids to disable the switches. The design must ensure that a minimum of three switches in the keypad area must be individually attacked to disable them. Note that these criteria are in addition to exploitation time and attack potential minimums and that the keypad in question is a physical keypad, not a touch screen.*

Q 35 What vulnerabilities must be taken into account for a touch screen?

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

The API for firmware & applications (if applicable) needs to be looked at carefully to determine the conditions under which plaintext data entry is allowed. Example: it should not be possible unless under the POS-B controls, for a third party to display an image (JPEG) that states "press enter when ready for PIN entry" and then have a plaintext keypad pop up on the next screen. The extra caution is warranted for touch screen devices because of the desire make touch screen 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 36 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 A7.**
- **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 37 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 the other keys encrypted by this key intact, 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 B11.*

POS Requirement A4

Q 38 Is A4 intended to address the ICC reader security?

A *No. A4 does not apply to the ICC reader. The security of the ICC reader and the path from the reader to the crypto-processor are addressed by D1, D2, and D3.*

POS Requirement A6

Q 39 What standards and methods are used for measuring "electro-magnetic emissions"?

A *Vendors should take into account that EM emissions can be a risk to PIN data, and should design 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 PED 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.*

POS Requirement A7

Q 40 Does "The keys resident in the PED, *if determined*..." mean plain-text keys or does it include encrypted keys as well.

A *The requirement is referring to plain-text keys.*

POS Requirement A8

Q 41 Does "non-PIN data" include data that can be entered while the PED is in a maintenance mode?

A *No. A8 is applicable to the PED while in its normal working mode. A8 does not apply to data entered while the PED is in special modes that are not intended to be accessed by cardholders and merchants.*

Q 42 Does "non-PIN data" include control inputs such as "enter," "cancel," etc.?

A *No. Non-PIN data refers to numeric data entered via the keypad.*

Q 43 The intent of A8 is to eliminate the possibility that PIN values will be entered at an improper time and handled by the PED in a non-secure manner. One way for a vendor to address A8 is to only allow for the entry of PIN values. 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 PED to accept the input of a PIN value at an inappropriate time. For instance, it must not be possible for a PED 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 44 What restrictions exist if a PED 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 PED 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 45 Touch screen devices offer multiple possibilities for the data entry: traditional PIN pad layout, QWERTY layout, signature capture, handwriting recognition, etc. Does A8 apply to all of these methods of data entry, or only the traditional PIN pad?

A *A8 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.*

Q 46 A vendor can choose to comply with either A8.1, or A8.2. Both of these govern the alteration of prompts and specify an attack potential of at least 16. What criteria should a vendor use to determine which one to comply with?

A *A8.1 should be complied with for devices that allow prompts to be changed as part of firmware updates. A8.2 should be selected when the prompts are fixed and cannot be updated; for example, when they are stored in ROM. In addition, A8.3 is appropriate for devices that allow third parties to update prompts, subject to the specified criteria in the requirement.*

Q 47 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.*

POS Requirement A8.1

Q 48 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 PED 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 PED that complies with PCI PED requirements.*

Q 49 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 50 Would the display of plain-text PIN digits by the PED qualify as tamper evidence?

A *No. The cardholder may not be familiar with the typical behavior of a given PED and may not recognize that the PED is violating Requirement B5.*

Q 51 If a terminal includes a display under its control and a keypad with its own display, must the cryptographic unit of the PED 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 A8. This means the terminal and keypad are a single PED that must meet PCI requirements.*

POS Requirement A8.2

Q 52 Can the calculation for the attack potential of 16 per PED include the cost of development kits that provide application programming information?

A *No. The PED must include protections that require an attacker to achieve an attack potential of at least 16 to order to defeat them. Administrative controls on application programming information are not adequate to meet this requirement.*

Q 53 Is the attack potential of 16 per PED to be applied to a single PED, or averaged over multiple PEDs?

A *A8.2 addresses an attack performed on a single PED. If an attack has a potential of 16 to develop, A8.2 is met regardless of whether or not applying the attack to additional PEDs is less than 16.*

POS Requirement A8.3

Q 54 What constitutes appropriate algorithms and key sizes?

A *Appropriate algorithms and key sizes will change slowly over time, as the computing capability for brute force attacks will increase. At the moment, examples of appropriate algorithms and key sizes are:*

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	112	1024	160	1024/160

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

AES may also be used with a key size of at least 128 bits.

Principles of dual control/split knowledge apply as defined in ISO 11568.

Q 55 What log file characteristics and content are necessary to meet Requirement A8.3?

A *A device must automatically record events that are relevant to A8.3 to a file that is automatically saved. Because each PED vendor solution will be unique, the data set that is appropriate to be included in a log file can vary. At a minimum, it is expected that actions that involve cryptographic operations, the user(s) and the time and date of the action will be recorded in the log file. The logs may exist either internally or externally to the PED, and a mechanism must be implemented which prohibits the overwriting of log events without proper authentication.*

Q 56 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 57 Is it acceptable to use a non-secure device to enforce the dual control required by A8.3?

A *No. Dual control must be enforced by a TRSM. The TRSM can be the PED itself or another device. If a TRSM other than the PED enforces dual control, the vendor must either provide the TRSM to third parties, or describe how a TRSM must be used to comply with A.8.3. The description must include an example of a specific, existing TRSM that can be purchased and used to comply with A8.3. The PED must have an API that is compatible with the TRSM. 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 58 What logging requirements must be met by a TRSM under A8.3?

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 59 Some PED designs fit either class A or class B depending 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 PED is to be listed as both a class A and class B device, there must be a differentiation so customers can distinguish between the two (e.g. different hardware and/or firmware versions).*

Q 60 Can USB authentication tokens or smart cards be considered to be the TRSM required to enforce dual control under A8.3?

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

POS Requirement A9

Q 61 What methods may be employed to comply with this requirement?

A *The PIN Entry device must be equipped with a privacy shield, or designed so that the cardholder can shield it with his/her body to protect against observation of the PIN during PIN entry.*

Q 62 When a PED is not a handheld device, it must have a privacy shield to meet A10. Are there any special considerations if the shield is detachable?

A *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 PED requirements.*

Q 63 The DTR "Appendix A—Guidance for the Privacy Screen Design" specifies size and weight guidelines for handheld devices. Are handheld devices required to meet these guidelines?

A *No. In order to be considered a handheld device, it must by weight, size, and shape encourage its handheld operation; however, the guidelines listed are suggestions, not requirements.*

Q 64 Requirement A9 stipulates that the PED 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 PED 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 shielding barrier,*
- *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 PEDs only), and*
- *The installed PED's environment.*

Q 65 Is there any impact on the device's approval if the laboratory evaluated privacy method is not used?

A *Frequently, the deployers of PEDs rationalize that privacy protection mechanisms may be bulky or obtrusive, make it more difficult to see the PED'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 PED 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.*

POS Requirement B1

Q 66 What is required to meet B1?

A *The device must perform an internal self-test automatically at least once every day, in addition to at power-up. Firmware integrity tests may use techniques such as SHA-1 or CRC. Authenticity testing must use cryptographic methods (MACs, digital signature or encryption).*

Q 67 Is it acceptable to perform firmware integrity checks before each PIN transaction instead of once daily?

A *Yes. It is acceptable to perform firmware integrity checks before each PIN transaction as opposed to performing them at least once every 24 hours.*

Q 68 Is it acceptable to perform a self-test after several minutes of inactivity rather than once every 24 hours?

A *Yes, as long as it is 24 hours or less. Note that the power-up self-tests are still required.*

Q 69 B1 requires that firmware integrity be tested every twenty four hours. Some firmware, such as a boot block, is rarely executed. For such firmware, is it acceptable to perform an integrity check prior to execution, rather than every twenty four hours?

A *Yes, it is acceptable to test firmware immediately prior to each execution rather than once every twenty four hours. However, note that all firmware must additionally be checked as part of the self-test performed at startup.*

Q 70 Requirement B1 states that a self-test must check for both integrity and authenticity of the installed firmware. Is it necessary to perform both checks separately?

A *No. The self-test required by B1 must perform an authenticity check, using cryptographic means such as a digital signature or a MAC. As such, an authenticity check will also confirm the integrity of the installed firmware, an additional integrity check is not necessary, but optionally may be additionally performed using a non-authenticated digest such as a CRC.*

Q 71 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 72 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 B4 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 A7 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.

POS Requirement B3

Q 73 What is considered "firmware"? (OS, EPROM code, DLL's, parameter files, applications, kernel code)?

A *Firmware is considered to be any code within the PED that provides security protections needed to comply with PCI requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI requirements.*

Q 74 What methods are acceptable to "certify" firmware?

A *"Certify firmware" refers to self-certification. This requirement, in essence, requires the vendor to have implemented and to use internal quality control and change control systems. With these systems in place, the vendor is in control of the code and can attest to the fact that the code is free of hidden or unauthorized functions by answering yes to B3.*

Q 75 Many PEDs are designed so that third parties can create and load applications. Vendors often support this by provide third parties the tools needed to create and load applications. How can a vendor ensure that the application will not need to be controlled by the vendor?

A *If applications are not considered firmware, they do not need to be controlled by the vendor. The PED 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 loading, 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 POS A8.3 is met.

POS Requirement B4

Q 76 What parties may possess keys used for the cryptographic authentication of firmware updates?

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

Q 77 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 to only 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.

POS Requirement B5

Q 78 What symbols are acceptable as "non-significant"?

A *Any symbol can be used as long as it cannot be used to determine PIN values. Using a different symbol for different digit numbers or groups of numbers is not acceptable. Here is an example of symbol use that would NOT be allowed: 1=*, 2=@, 3=%.*

POS Requirement B6

Q 79 What does "encrypted immediately" mean in term of software or hardware architecture?

A *This means when the cardholder signifies that PIN entry is complete, either by pressing an "enter" button, or by entering the last digit of the PIN, the PED does not perform any processes other than those required to encrypt the PIN.*

Q 80 Requirement B6 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 PED 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 PED. 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.

POS Requirement B7

Q 81 Is it acceptable to XOR key components during key loading to satisfy the authentication requirements of B8?

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 82 Under what circumstances is key entry via the PED keypad permitted?

A *Plain-text secret keys cannot be entered into the PED 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 PED is placed in a special maintenance mode. Access to special modes must be restricted through the use of passwords or other secret knowledge.*

Q 83 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 84 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 85 B7 defines sensitive functions as those functions that access sensitive data, such as cryptographic keys, and that authentication is required for such access. The guidance note for B7 stipulates that authentication shall be considered as dual control techniques when entering sensitive information through a secure user interface, or cryptographic techniques when entering electronic data. The use of other techniques to access sensitive services results in the device being unable to use previously existing keying material. How does this guidance apply to secret or private key loading?

A ***1)*** *When entering plain-text secret keys through the keypad, they must be entered as two or more components and require the use of at least two passwords/PINs. The passwords must be entered through the keypad or else conveyed encrypted into the device. These passwords/PINs 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/PINs that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/PINs are at least five characters.*

Entry of key components without the use of at least two separate passwords/PINs 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. For devices supporting multiple key hierarchies (e.g., multi-acquirer devices), only the hierarchy (specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, PINs or similar) for each user on a given device must be different for each user.

2) *For injecting plain-text secret or private keys from a key loader (which has to be some type of secure cryptographic device), either the key loader or the PED or both must require two or more PINs/passwords before injecting the plain-text key into the PED. (**Note:** This may be the entire key—if components, each component requires a separate password.) These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least five characters in length. These passwords/PINs 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. Plaintext keys or their components are never permitted over a network connection.*

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

3) *For encrypted values injected into the PED, either from a key loader or from a network host, or via loading through the keypad, the ability of the PED to successfully decrypt the value and use it is sufficient. In this case, the loading of the key encipherment key would have been done under dual control, e.g., in examples a) and b) above.*

4) *Remote key-loading techniques using public key methods requires compliance with PCI defined criteria for key sizes and mutual authentication between host and PED. For PEDs generating their own key values, the generation process must meet the criteria defined in the random number appendix of the DTRs and validation that appropriate key sizes are used. The protocol must meet the criteria stipulated in Annex A of the PCI PIN Security Requirements.*

POS Requirement B10

Q 86 Should the average delay between encryptions be calculated for the exhaustive attack of a single PIN block, or should the time be averaged over attacks on multiple PIN blocks?

A *The average time delay should be calculated for an attacker to determine a single PIN value.*

Q 87 In order to prevent exhaustive PIN determination, examples of preventive measures such as a unique key per transaction or the limiting of the rate of PIN encryption to thirty seconds or greater between encipherments as measured over 120 transactions are given. Are any other methods possible?

A *The list of examples is not exhaustive. Other methods are possible. For example, the exclusive use of ISO PIN block format 1 whereby each PIN is enciphered using a unique except by chance random pad of characters with permissible values of 0000 to 1111 may be used to prevent exhaustive PIN determination.*

Q 88 One example given to prevent exhaustive PIN determination is to limit the rate of PIN encryption to thirty seconds or greater between encipherments as measured over 120 transactions. Can this average of 30 seconds between encipherments be determined over a longer time frame than one hour?

A *The intent of the requirement statement is that for any 120 consecutive transactions, the average time between encryptions for a specific PIN entry averages out to approximately 30 seconds.*

POS Requirement B11

Q 89 Is it acceptable for a PED 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 mandated in ANSI X9.24 and ISO 11568.*

Q 90 What PIN block formats are allowed?

A *ISO 9564–1 PIN block formats 0, 1, or 3 are acceptable for online transactions. Format 2 must be used for PINs that are submitted from the IC reader to the IC for offline transactions. This applies whether the PIN is submitted in plain-text or enciphered using an encipherment key of the IC.*

PINs enciphered only for transmission between the PIN entry device and the IC reader shall use one of the PIN block formats specified in ISO 9564-1. Where Format 2 PIN blocks are used then a unique key per transaction method in accordance with ISO 11568 shall be used.

Q 91 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 92 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 93 PCI PIN Security Requirement #20 states that all secret and private cryptographic keys ever-present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device. How does this requirement apply to PED testing?

A *PEDs must implement unique secret and private keys for any function directly or indirectly related to PIN protection. The basic rule is that any private or secret key resident in the PED that is directly or indirectly used for PIN protection whose compromise would lead to the compromise of the same key in another PED must be unique per device. For example, this means not only the PIN-encryption key(s), but keys that are used to protect other keys, firmware-update keys and display prompt control keys. As stated in the requirement, this does not apply to public keys resident in the PED. This is not intended to require that the device compare keys across different key hierarchies associated with different acquirers.*

Q 94 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 95 Under what conditions is it acceptable for a PED to allow single component plain-text cryptographic keys to be loaded via the keypad?

A *None. A PED may 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 B7, B8)****.*

Q 96 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 PED?

A *The intent of the requirement is that the compromise of a key in one transaction-originating device (e.g., an EPP or POS PED) 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 their 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 97 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 a key encipherment key shall be at least of equal or greater strength than the key that it is protecting. What keys does this apply to in a PED?

A *This applies to any key encipherment keys used for the protection of secret or private keys stored in the device or for keys used to encrypt any secret or private keys for loading or transport to the device. For purpose of this requirement, the following algorithms and keys sizes by row are considered equivalent.*

Algorithm	DES	RSA	Elliptic Curve	DSA/D-H/MQV
Minimum key size in number of bits	112	1024	160	1024/160
Minimum key size in number of bits	168	2048	224	2048/224

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. DSA for digital signatures, and Diffie-Hellman and MQV key agreement key sizes refer to the size of the modulus (p) and the minimum size of a large subgroup (q).

AES keys, of 128 bits or larger are considered stronger than any of the aforementioned.

This does not apply to keys that are used for authentication purposes, such as keys used to validate firmware or display prompts. The sizes of those keys must at minimum be as stipulated in B4 and A8 (for POS PED).

Q 98 Version 2 stipulates that the device must provide support for TR-31 or an equivalent methodology for maintaining the TDES key bundle. Under what circumstances does this apply?

A *If the device supports the exchange of TDEA keys between itself and another device (e.g., a remote host) encrypted under a shared symmetric key, the device must provide support for TR-31 or an equivalent methodology for this key conveyance. This does not imply that the device must support TR-31 or an equivalent methodology between the device and an external ICC reader, but optionally may do so. The device may also optionally support TR-31 or an equivalent methodology for the storage of keys encrypted under a symmetric key. Any equivalent method must include the cryptographic binding of the key usage information to the key value using accepted methods. Any binding or unbinding of key usage information from the key must take place within the secure cryptographic boundary of the device.*

Q 99 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 100 A device may support key check values to validate the successful entry of symmetric key components and/or keys. Are there any restrictions on the use of key check values?

A *Yes. Any returned values shall not exceed six hexadecimal characters and should be at least four hexadecimal characters in length.*

Q 101 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 102 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 103 Requirement B11 stipulates that the device must support TR-31 or equivalent. Key blocks that support padding include a key length that allows the key to be distinguished from the pad characters. In TR-31, the key length information and padding are encrypted along with the key itself by the KEK (termed the Key Block Encryption Key). Does this violate the requirement that a cryptographic key be only used for one purpose, e.g., key encipherment?

A *No. For all TDEA modes of operation, the three cryptographic keys (K1, K2, K3) define a TDEA key bundle. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle cannot be unbundled for any purpose i.e., must never be used separately for any other purpose. A key used to encrypt the key bundle may include in the encrypted portion of the key bundle the key length information and padding as necessary to protect the integrity of the key bundle.*

Q 104 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. Its does not apply when cleartext symmetric keys or their components are loaded using standard dual control techniques.*

Q 105 Can secret keys or their components be used for other purposes such as passwords 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 106 Remote key distribution using asymmetric techniques methodologies must provide for protection against man-in-the-middle attacks and the hijacking of PIN acceptance devices where the devices are under a PKI hierarchy that facilitates more than one acquirer (e.g., a hierarchy under a PIN acceptance device vendor's Root). In order to achieve this, many vendors have implemented techniques that force the PIN acceptance device to "bind" to a specific transaction processing host's certificate, and not accept commands digitally signed by any other hosts. However, in the case of portfolio transfers or other situations where a device must be decommissioned (unbound), from a specific host, what techniques are acceptable for compliance?

A *Decommissions, such as sending a new host's certificate to replace the existing host's certificate without authentication are <u>not</u> acceptable. Any remote decommissioning must require cryptographic techniques and be specific per PIN acceptance device. For example:*

- *The existing bound host can digitally sign an "unbind" command to the PIN acceptance device, that when validated returns the PIN acceptance device to its original unbound state.*
- *In situations where the bound host's private key is not available to sign the command, or other similar scenarios, a forced decommission may occur. However, any such decommission done remotely requires a cryptographic (digital signature, MAC, etc.) technique, and must be unique per PIN acceptation device.*
- *Decommissions may also be done manually directly at the device, using system administration menus that authenticate users via PINs, passphrases, etc.*

In all cases of decommissioning, the existing acquirer related keys must be zeroized as a result of the decommission.

Q 107 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 cleartext key is loaded into the slot <u>without authentication using dual control</u>, then 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 108 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 configurations option. For implementing 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/PINs. The passwords must be entered through the keypad or else conveyed encrypted into the device.*

  These passwords/PINs 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/PINs that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/PINs are at least five characters.

  Entry of key components without the use of at least two separate passwords/PINs 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, PINs 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 PINs/passwords before injection of the key. These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least five characters in length. These passwords/PINs 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. Plaintext 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 PINs/passwords 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, PINs 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 109 The Guidance for DTR B11 states that "A PED 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. If an explicit configuration change is required, the change is considered a sensitive service and must meet the requirements of B7, protection of sensitive services.*

POS Requirement B12

Q 110 ISO 9564 stipulates that a PIN shall be not less than four and not more than twelve characters in length. What PIN lengths must an EPP or POS PED support?

A *EPPs and POS PEDs must be able to support from four to twelve digit PINs for payment card transactions.*

POS Requirement B13

Q 111 Is it acceptable for a PIN-encryption key to be used as a key-encrypting key, or for a key-encrypting key to be used as a PIN-encrypting key?

A *No. A key must be used for one purpose only as mandated by ANSI X9.24 and ISO 11568-3.*

Q 112 Can a PED 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.*

Q 113 The device must enforce that data keys, key encipherment keys and PIN-encryption keys have different values. Does this apply to replacement keys downloaded throughout the processing life of the device?

A *The intent of the requirement is to help ensure that these keys are not intentionally used for multiple purposes. Thus the uniqueness check applies for both when the device is initially loaded with these keys and for those that are subsequently loaded. The check must occur across all secret key hierarchies supported by the device. No two secret keys, regardless of purpose, can have the same value.*

Q 114 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.*

POS Requirement C1

Q 115 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 116 Is it acceptable for a PED that supports multiple key hierarchies to meet C1 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 117 What are acceptable means of external cryptographic keys selection?

A *Keys may be selected through the PED 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 118 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 119 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 120 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 PED must enforce authentication of commands used for external key selection. If the PED 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 their 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/PINs) either via the key loader or directly via the EPP. 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 121 When is C1 not applicable to POS-B devices?

A *C1 is not applicable to Class B devices that do not include commands for external key selection, or cannot hold multiple keys related to PIN encryption.*

POS Requirement D1

Q 122 The PCI v1.3 requirements specified that precautions against unauthorized removal were required for unattended devices (PCI POS PED v1.3 DTR 1.4). Are such precautions required for compliance to DTR D1 of the v2.0 requirements?

A *Yes, an unattended device that supports offline PIN entry using a separate ICC reader must provide protections against the unauthorized removal of that reader. Circumvention of these protections must require an attack potential of at least 16 points.*

POS Requirement D2

Q 123 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 124 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 125 What volume of space is allowed under D2?

A *The objective of D2 is to guard against a PIN-disclosing bug being inserted into the PED 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 D2 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.*

POS Requirement D3

Q 126 Some PED 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 D3 if a portion of the wire is visible between the slot and the concealing component.*

POS Requirement D4

Q 127 When is "No" or "N/A" an acceptable response to D4.1, D.4.2, D4.3, and D4.4?

A *"No" or "N/A" is only an acceptable response when the PED does not support the specified method of PIN submission to the IC Card.*

Q 128 How many options should be marked "Yes" if a PED supports more than one of the PIN submission options?

A *All applicable options must be checked "Yes." The evaluation laboratory will verify that all responses are appropriate.*

Section 2: EPP Evaluation *Frequently Asked Questions*

These technical FAQs provide answers to questions regarding PCI's (Payment Card Industry) physical and logical EPP security requirements as addressed in the *PCI Encrypting PIN Pad (EPP) 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 When is an "N/A" response to a requirement acceptable?

A *An "N/A" response is acceptable in two cases: First, if compliance is achieved by meeting another requirement option, such as meeting A1. Second, if the characteristics governed by the requirement are absent in the EPP, such as A5 if the EPP does not emit any audible tones. The evaluation laboratory will verify that all responses are appropriate.*

Q 2 What is the definition of "Secret Information?"

A *"Secret information" is any cryptographic keys or passwords that the EPP relies on to maintain security characteristics governed by PCI requirements.*

Q 3 Some components of an EPP may include cryptographic keys that cannot be erased. Are there any instances when this would be acceptable? See Requirements A1 and A7.

A *Cryptographic keys that are never used to encrypt or decrypt data; or are not used for authentication, do not need to be considered secret data, and therefore do not need to be erased.*

Q 4 What type of epoxy is acceptable for encapsulation?

A *Acceptable epoxy will possess the following characteristics:*

- *Opaqueness: Epoxy must be opaque in the visible spectrum.*
- *Hardness: Epoxy must be hard enough so that a sharp object cannot be used to penetrate the epoxy to the depth of the underlying circuitry.*
- *Tamper Evidence: The epoxy must show visible evidence of tamper when an attempt to penetrate the epoxy with a sharp object is made.*
- *Adhesion: Epoxy must resist attempts to forcibly separate it from the circuit board. When enough force is applied to remove the epoxy, severe damage should result such that the device is non-functional.*

Q 5 Is it assumed that the surface of the potted area is visible without disassembly of the EPP?

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

Q 6 Is it acceptable for an EPP 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 7 Vendors are allowed to make revisions to approved devices provided the changes are evaluated by an approved lab. What limits are placed on the number and type of changes that are allowed?

A *The large number of possible changes and their impacts cannot be determined in advance. Changes will be assessed on a case-by-case basis. Vendors should contact one of the recognized laboratories for guidance. Laboratories will consult with PCI on an as needed basis to determine if a change is too great to be addressed under the delta process. In all cases, changes that impact security require assessment. The laboratories will determine whether the change impacts security.*

Revisions to approved devices are termed "deltas." Delta reviews involve the laboratory assessing the changes based on the current major version (e.g. 1.x, 2.x, etc.) of the requirements that were used for the approval of the device. Examples of deltas include:

- *Revisions to existing firmware or hardware on existing approved devices to add or modify functionality*
- *Adding EMV level 1 to an existing approval*
- *Maintenance fixes on devices that have expired and are no longer approved for new deployments*
- *Assessment of a device for offline PIN entry where the existing approval is only for online PIN entry, or vice versa*
- *The porting of a new set of firmware to an existing approved device.*

Q 8 Does the EPP and ICC reader have to show the version numbers of the hardware, firmware and application?

A *The EPP and ICC reader must show the version numbers of hardware and firmware like they have been approved and they are shown in the list of approved devices. The hardware number must be shown on a label attached to the EPP and ICC reader. The firmware number and optionally the hardware number must be shown on the display or printed during startup or on request.*

Q 9 Does the use of protective keypad overlays impact the approval status of an EPP?

A *In general, overlays are not supported by the PED approval program due to the potential for keypad tapping. Overlays may be used where they do not cover any portion of the PIN entry area. For example, in a touchscreen device whereby 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 10 Is it acceptable to make changes to an approved device's hardware or firmware and keep the existing version #s?

A *No. Any hardware changes to an approved device that has been deployed must result in a new hardware version #. Any firmware changes to an approved device must result in a new firmware version. As described in the PCI PTS Device Testing and Approval Program Guide vendors may use a combination of fixed and variable alphanumeric characters in the version numbers. However, variable characters are not permitted for any physical or logical device characteristics that impact security. Device characteristics that impact security must be denoted using fixed characters. The use of variable characters shall be validated by the test laboratory so as to not impact security. The use of variable characters is appropriate to delineate differences such as country usage code, customer code, communication interface, device color, etc.*

Q 11 Does the entry of the authentication code (password or PIN) 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 (password or PIN) used for settlement/balancing at the ATM does not need to be entered through the EPP, but 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 Password, 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 PIN/password.*

Note that PINs or passcodes 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 12 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 13 When submitting hardware and/or firmware changes on existing approved devices, must a vendor submit the device to the same lab as the one that did the initial evaluation?

A *Vendors may select a different lab then the lab that was used to perform the initial evaluation. However, the subsequent lab is free to determine the level of reliance they wish to place upon the prior lab's work, which may result in additional work than would otherwise be necessary. For version 3 reports, the delta lab or the final form factor lab shall have access to the prior lab's report(s), including any delta or OEM component reports subsequent to the original evaluation. If those reports are not available, then the delta lab shall decline the engagement or else must complete a full evaluation of the device.*

Q 14 The DTRs indicate that software developed to enable an attack can be considered bespoke equipment (Appendix B, under "Equipment"). Does this mean that PIN-disclosing bug software should be considered bespoke equipment?

A *Software required for a PIN-disclosing bug is typically straightforward to implement and would not be considered bespoke. Bespoke software would be software that requires significant time and expertise to develop such as is required for side channel attacks. PCI requires strong justification to be provided when bespoke equipment is indicated as necessary for an attack.*

Q 15 How do the point calculations take into account the development of a PIN-disclosing bug? Does PCI provide fixed values for use by the labs?

A *PIN bugs must often be customized for a specific EPP. Due to numerous possible variations in bug form, function, and complexity, PCI does not provide standard point values for PIN bugs. The evaluation lab is responsible for addressing this as part of the EPP evaluation. The development of an appropriate PIN-disclosing bug is to be included in the Identification calculation, as are other aspects of attack development.*

Q 16 When can multiple devices be costed in the calculation to support the compliance of a device to those requirements that have a minimum attack potential?

A *The requirement for multiple devices during either the identification or the exploitation phase of an attack cost calculation depends upon the difficulty of attacking a device, and the risk that the device may be tampered during the attack. However, PCI expects that most attacks can be performed with only one or two samples in the identification phase, and a single sample in the exploitation phase. Strong justification explaining why multiple sample devices are necessary must be provided when such additional samples are necessary to meet the minimum attack potential.*

Q 17 Are PC-based instruments like protocol sniffers, USB attached oscilloscope adapters and graphical multimeters, etc. considered standard or specialized equipment.

A *PC-based instruments like those mentioned above shall be considered standard equipment, especially if they do not require dedicated hardware or adapters.*

Q 18 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 cost 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 is to be considered only for the identification of the general device setup and the property to be attacked (e.g. the interface type).*

Q 19 If a device is submitted for evaluation of offline PIN entry, is it acceptable for the device to only support plaintext PIN or to only support enciphered PIN?

A *No. In order to receive an approval for offline PIN entry, a device must be capable of supporting both plaintext and enciphered PIN.*

Q 20 Several requirements, such as those for access to sensitive services, key loading, and removal detection, provide for the use of authentication using passwords or PINs. Are there any restrictions on this type of authentication data?

A *Yes, any passwords, PINs or similar used to meet a PCI requirement must be at least a five character minimum. These passwords/PINs must either be unique per device (and per user where dual control is required), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Passwords/PINs that are unique per device can be made optionally changeable by the acquirer or their agent (e.g., merchant), but this is not required. These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device. In all cases, the authentication values (passwords, PINs or similar) for each user on a given device must be different for each user.*

Q 21 EPPs may come with an integrated display and/or integrated ICC/Magnetic Stripe card readers. The EPP requirements do not contain criteria for either display management or for card readers. Do these integrated displays and card readers require evaluation?

A *Yes. EPPs containing integrated displays must be evaluated against requirement A8 of the PCI POS PED Security Requirements. EPPs containing an integrated ICC reader and seeking offline approval must meet the requirements in section D of the PCI POS PED Security Requirements. EPPs containing an integrated MSR and seeking online approval must meet requirement A11 of the PCI POS PED Security Requirements. Additional criteria may apply in an UPT evaluation.*

Q 22 In occurrences where it is necessary to return a device to the device vendor for maintenance, are there any restrictions on what must happen to the secret keys in the device?

A *When a device is returned to the vendor for maintenance, mechanisms must be in place to automatically cause the erasure of all previously loaded Acquirer secret keys upon servicing the device. (e.g., loading a new public RSA key causes the erasure of all previously loaded secret keys).*

Q 23 Security requirements are normally available for a four year period from date of publication for new evaluations of products. Products are approved until six years after the retirement/expiration of the version of security requirements against which they were approved. This results in approvals that are a minimum of six years and a maximum of ten years, depending on the timeframe in which the approval occurs in relations to the life cycle of the applicable security requirements. Modifications for approved devices, termed deltas, can occur at any time during the products approval.

Can products for which the approval has expired undergo deltas?

A *Yes. Vendors may need to make maintenance fixes to devices that the vendor has already sold, but must still provide support for. In addition, vendors may wish to port updated versions of firmware that were approved against newer security requirements to products for which the approval has expired. This may occur because customers of a vendor wish to standardize their deployment against a given version of firmware and/or to add functionality to that device.*

Q 24 Technical FAQs are updated on a regular basis, and add clarifications for the application of defined security requirements. Are new FAQs applicable to devices that are currently in evaluation? Furthermore, must FAQs that were not in existence at the time of the original evaluation be considered in subsequent delta evaluations?

A *Yes. Technical FAQs not only add clarifications to requirements in order to provide a consistent and level playing field in the applications of those requirements, but may also address new security threats that have arisen. As such, technical FAQs are generally effective immediately upon publication.*

The intent is not to cause a device in evaluation to fail if otherwise it would not unless known exploitations exist. Unless such an exploitation exists, a product currently in evaluation will generally not be subject to new FAQs issued during the product's evaluation. This does not exempt a product from the applicability of the FAQ if the product must be reworked and resubmitted at a later date because of other issues that cause it to fail the evaluation. The product is also subject during delta evaluations to any FAQs issued subsequent to the original approval, even though the FAQ impacts an area that is not part of the modification made by the vendor.

In all cases, the evaluation laboratory must advise PCI SSC of the circumstances and PCI SSC will make the final decision based upon the circumstances. Additionally, for both new and delta evaluations, the laboratory will also state in their submission the security requirements used in the evaluations, as well as the publication date of the technical FAQs used.

Q 25 Compound devices, such as Unattended Payment Terminals, may be evaluated as part of a single evaluation of all applicable components, or may be evaluated with one or more previously approved OEM components. Where a compound device incorporates previously approved components, what considerations must be made for the evaluation?

A *There are several considerations:*

- *UPT evaluation reports containing separately approved OEM components must at a minimum contain a summary table of all requirements (whether Yes or N/A) of any module that is relevant to the final form factor of the UPT. This table may reference the pertinent OEM component for compliance to any specific requirement.*
- *All requirements impacted (e.g., additional cardholder input mechanisms, displays, controllers, removal detection, etc.) by the final form factor of the UPT must be addressed in detail for each impacted requirement.*
- *Where the lab evaluating the final form factor is not the same lab as the lab that evaluated OEM component(s), the lab **should** have access to the OEM component lab report(s). If those reports are not available, e.g., because submitting vendors are different or for any other restriction, the lab must determine the extent of additional work required.*
- *If the lab is unable to place reliance, where necessary, on information that is available in reports that are not available to the lab, and the lab is unable to perform the degree of necessary additional work to achieve such reliance, then they must decline the engagement.*
- *In all cases, PCI SSC may reject the report if in the judgment of PCI SSC the report does not contain adequate information to substantiate the conclusions of compliance to overall UPT criteria.*

Q 26 Are OEM components, such as EPPs, approved against an earlier version of security requirements allowed for use in achieving an overall UPT approval without additional testing of requirements that were already evaluated, even if those requirements were updated as part of the POI v3 security requirements?

A *OEM components approved against earlier security requirements are only allowed for use in obtaining an overall UPT approval evaluation without additional testing of those components if they are no more than one major version of requirements earlier. For example, EPPs evaluated and approved using PCI EPP v2.x can be used without additional testing of requirements they have previously met as part of an overall POI v3 evaluation. However, EPPs that were evaluated and approved using PCI EPP v1.x must undergo a full evaluation against all applicable POI v3 requirements.*

In addition, other modules such as Integration, SRED and Open Protocols, as well as additional individual security requirements in POI v3 that were not previously evaluated shall still apply if applicable to the overall UPT evaluation. Furthermore, for devices that embed other PCI-approved devices, and are therefore basing their security on these sub-components (even partially), the renewal/expiration date shall be the earliest to expire date among all evaluations, including the embedded device itself.

Q 27 UPT version 1 shall no longer be 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 which 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 28 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 their 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 29 The program manual states that hardware and firmware version number identifiers may consist of a combination of fixed and variable alphanumeric characters, whereby a lower "x" is used by PCI to designate all variable fields. The "x" represents fields that the vendor can change at anytime to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device color, etc. What are examples of options that can not be addressed by use of a variable field, but must be addressed by a fixed character?

A *Options that cannot be a variable character include those that directly pertain to meeting security requirements. For example, requirements exist for magnetic stripe readers (MSRs) and integrated circuitry card readers (ICCRs). A variable character cannot be use to designate whether a device contains a MSR or ICCR. A requirement exist for the deterrence of visual observation of PIN values as they are being entered by the cardholder, which can be met by privacy shields or the device's installed environment or a combination thereof. It is not appropriate to wildcard options if the device supports more than one means of observation deterrence.*

Q 30 The program manual stipulates that "Vendors or other third parties licensing approved products from other vendors to market or distribute under their own names are not required to pay a new evaluation fee if the only change is to the name plate. If firmware or other hardware changes are made that require a PCI-recognized test laboratory to evaluate the changes for potential security impact, then the licensee shall be required to pay the new evaluation fee. In all cases the licensed device will receive a new approval number and the licensee vendor or third party shall be billed the annual listing fee for each such approval."

What are additional considerations for a third party to license an approved product from a vendor, whereby the third party wants to distribute it as their own product?

A *There are several additional considerations:*

- *The licensee vendor cannot directly make the request. The licensor vendor must make the request on their behalf.*
- *All such requests must be received by PCI SSC as a delta letter from one of the PCI SSC PTS recognized laboratories. If the only change is to the nameplate of the product, there is not any new evaluation fee (currently $2,000), but as noted above, there will be an annual listing fee (currently $1,000).*
- *There is not any requirement for the licensee's version of the product to reference or list the original vendor.*
- *Products may be licensed from another vendor even if the version of the security requirements against which the original product was approved is retired from use for new evaluations, as long as the approval has not expired.*
- *As noted, licensed products requiring physical and/or logical changes will incur a new evaluation fee. However, as long as the original vendor continues the manufacture of the device on behalf of the licensee vendor, the licensed product can be evaluated against the security requirement's version against which the original product was evaluated and approved, even though those requirements may be expired for new approvals.*
- *If the licensee vendor wishes to directly manufacture the licensed product, or have a third party other than the original vendor manufacture the licensed product on their behalf, then the product must be reassessed as a new evaluation against the current version of security requirements, unless the licensor vendor can demonstrate that it retains both the intellectual property and engineering control. This is due to the potential for changes in plastics, etc. that may impact the security of the device.*

EPP Requirement A1

Q 31 Do attack scenarios considered under A1 include replacement of the enclosure to conceal tamper evidence?

A *A1 allows the evaluator to use any method of attack feasible against the terminal limited only by the attack potential of 25. The EPP must be able to withstand any front-side attack up to the attack potential value. The EPP must be able to withstand any rear-side attack including case replacement up to the attack potential value.*

Q 32 The Derived Test Requirements of A1 have the Guidance note: "Attack scenarios should consider keypad removal or replacement associated with unattended payment terminals, such as in connection with overlay attacks." How can this be addressed by the device's design?

A *Since in vending machines or other unattended acceptance/payment terminals only the keypad area of a EPP is usually visible to the cardholder, attacks may be mounted which use EPP removal and the insertion of keypad overlays or keypad substitutes as an attack element. These attacks may be easier to perform than direct attacks to the EPP. The attack scenarios must therefore consider removal/replacement attacks as part of an overall attack scenario. The EPP must have design properties to detect and respond to removal/replacement attacks. Examples of countermeasures include, but are not limited to, removal detectors, movement detectors, special mounting brackets or special keypad designs. Specific requirements for removal sensors are included in Requirement A8.*

Q 33 Requirement A1 specifies minimum attack potentials of 25 for the EPP for penetration attacks designed to determine or modify sensitive data. In Version 1 requirements alternative options included meeting a minimum of ten hours of exploitation time. Does exploitation time enter into this requirement?

Yes. In addition to the specified minimum attack potential values, any feasible penetration attack against either the EPP for the purpose of determining or modifying sensitive data must entail at least ten hours of exploitation time.

Q 34 Are there circumstances under which an EPP can comply with Requirement A1 while employing one tamper switch to protect the keypad area?

A *No. If switches are used as the primary protection for the area around a physical keypad area, then at least three blind, tamper switches must be implemented. The switches must be protected from attacks that use the application of adhesives or conductive liquids to disable the switches. The design must ensure that a minimum of three switches in the keypad area must be individually attacked to disable them. Note that these criteria are in addition to exploitation time and attack potential minimums and that the keypad in question is a physical keypad, not a touch screen.*

Q 35 What vulnerabilities must be taken into account for a touch screen?

A *If the sides are accessible, an overlay attack utilizing a second, clear touch screen could be a problem. The connection/path from the touch screen to the processor (& any devices used for decoding the signals in between) needs to be verified to be secure. Bezels around the touch screen are especially dangerous because they can conceal access to areas of concern that are described above.*
The API for firmware & applications (if applicable) needs to be looked at carefully to determine the conditions under which plaintext data entry is allowed. Example: it should not be possible unless under the POS-B controls, for a third party to display an image (JPEG) that states "press enter when ready for PIN entry" and then have a plaintext keypad pop up on the next screen. The extra caution is warranted for touch screen devices because of the desire make touch screen 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 36 In the attack potential calculation for A1, is it allowed to include in the point calculation a value for disabling the removal detection mechanism of the EPP?

A *If attack scenarios in A1 do not necessarily require the removal of the EPP out of its location (e.g., the attack could take place at a time before field placement), the cost for disabling the removal sensor should not be included in the point calculation for A1. Removal detection is considered in requirement A8. However, if an attack considered in A1 requires the deactivation of the removal detection mechanisms, the effort for that can be included in the attack cost calculation. Most likely, this will increase the attack costs only marginally (e.g. by 1 or 2 points). In no circumstances can the attack costs determined under A8 simply be added to the attack costs determined under A1.*

Q 37 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 A7.**
- **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 38 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 the other keys encrypted by this key intact, 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 B11.*

EPP Requirement A4

Q 39 Is A4 intended to address the ICC reader security?

A *No. A4 does not apply to the ICC reader. The security of the ICC reader and the path from the reader to the crypto-processor are addressed by A1 and the ICC reader requirements.*

EPP Requirement A7

Q 40 What standards and methods are used for measuring "electro-magnetic emissions"?

A *Vendors should take into account that EM emissions can be a risk to PIN data, and should design 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 EPP 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.*

EPP Requirement A8

Q 41 Does "The keys resident in the EPP, *if determined*..." mean plain-text keys or does it include encrypted keys as well.

A *The requirement is referring to plain-text keys.*

Q 42 Requirement A8 states that the minimum attack potential for the removal of an EPP from its intended environment is 16 points. Does this figure include the cost required to produce and install an overlay bug after removal of the EPP?

A *No. The 16-point requirement for the removal of an EPP includes all stages of identification and exploitation up to the point that the EPP is removed from its installed environment. No further steps, such as the production or installation of an overlay to capture PINs after the removal of the EPP, are considered in the cost of the attack.*

EPP Requirement B1

Q 43 What is required to meet B1?

A *The device must perform an internal self-test automatically at least once every day, in addition to at power-up. Firmware integrity tests may use techniques such as SHA-1 or CRC. Authenticity testing must use cryptographic methods (MACs, digital signature or encryption).*

Q 44 Is it acceptable to perform firmware integrity checks before each PIN transaction instead of once daily?

A *Yes. It is acceptable to perform firmware integrity checks before each PIN transaction as opposed to performing them at least once every 24 hours.*

Q 45 Is it acceptable to perform a self-test after several minutes of inactivity rather than once every 24 hours?

A *Yes, as long as it is 24 hours or less. Note that the power-up self-tests are still required.*

Q 46 B1 requires that firmware integrity be tested every 24 hours. Some firmware, such as a boot block, is rarely executed. For such firmware, is it acceptable to perform an integrity check prior to execution, rather than every twenty four hours?

A *Yes, it is acceptable to test firmware immediately prior to each execution rather than once every 24 hours. However, note that all firmware must additionally be checked as part of the self-test performed at startup.*

Q 47 Requirement B1 states that a self-test must check for both integrity and authenticity of the installed firmware. Is it necessary to perform both checks separately?

A *No. The self-test required by B1 must perform an authenticity check, using cryptographic means such as a digital signature or a MAC. As such, an authenticity check will also confirm the integrity of the installed firmware, an additional integrity check is not necessary, but optionally may be additionally performed using a non-authenticated digest such as a CRC.*

Q 48 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 49 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 B4, 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 A7 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.

EPP Requirement B3

Q 50 What is considered "firmware"? (OS, EPROM code, DLL's, parameter files, applications, kernel code?)

A *Firmware is considered to be any code within the EPP that provides security protections needed to comply with PCI requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI requirements.*

Q 51 What methods are acceptable to "certify" firmware?

A *"Certify firmware" refers to self-certification. This requirement, in essence, requires the vendor to have implemented and to use internal quality control and change control systems. With these systems in place, the vendor is in control of the code and can attest to the fact that the code is free of hidden or unauthorized functions by answering yes to B3.*

Q 52 Many EPPs 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 the application will not need to be controlled by the vendor?

A *If applications are not considered firmware, they do not need to be controlled by the vendor. The EPP 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 loading, 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.*

EPP Requirement B4

Q 53 What parties may possess keys used for the cryptographic authentication of remote firmware updates?

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

Q 54 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 to only 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.

EPP Requirement B6

Q 55 What does "encrypted immediately" mean in term of software or hardware architecture?

A *This means when the cardholder signifies that PIN entry is complete, either by pressing an "enter" button, or by entering the last digit of the PIN, the EPP does not perform any processes other than those required to encrypt the PIN.*

Q 56 Requirement B6 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 EPP 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 EPP. 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 57 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 B6?

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.*

EPP Requirement B7

Q 58 Is it acceptable to XOR key components during key loading to satisfy the authentication requirements of B7?

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 59 Under what circumstances is key entry via the EPP keypad permitted?

A *Plain-text secret keys cannot be entered into the EPP 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 EPP is placed in a special maintenance mode. Access to special modes must be restricted through the use of passwords or other secret knowledge.*

Q 60 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 61 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 62 B7 defines sensitive functions as those functions that access sensitive data, such as cryptographic keys, and that authentication is required for such access. The guidance note for B7 stipulates that authentication shall be considered as dual control techniques when entering sensitive information through a secure user interface, or cryptographic techniques when entering electronic data. The use of other techniques to access sensitive services results in the device being unable to use previously existing keying material. How does this guidance apply to secret or private key loading?

A ***1)*** *When entering plain-text secret keys through the keypad, they must be entered as two or more components and require the use of at least two passwords/PINs. The passwords must be entered through the keypad or else conveyed encrypted into the device. These passwords/PINs 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/PINs that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/PINs are at least five characters.*

Entry of key components without the use of at least two separate passwords/PINs 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. For devices supporting multiple key hierarchies (e.g., multi-acquirer devices), only the hierarchy (specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, PINs or similar) for each user on a given device must be different for each user.

2) *For injecting plain-text secret or private keys from a key loader (which has to be some type of secure cryptographic device), either the key loader or the EPP or both must require two or more PINs/passwords before injecting the plain-text key into the EPP. (**Note:** This may be the entire key—if components, each component requires a separate password.) These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least five characters in length. These passwords/PINs 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. Plaintext keys or their components are never permitted over a network connection.*

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

3) *For encrypted values injected into the EPP, either from a key loader or from a network host, or via loading through the keypad, the ability of the EPP to successfully decrypt the value and use it is sufficient. In this case, the loading of the key encipherment key would have been done under dual control, e.g., in examples a) and b) above.*

4) *Remote key-loading techniques using public key methods requires compliance with PCI defined criteria for key sizes and mutual authentication between host and EPP. For EPPs generating their own key values, the generation process must meet the criteria defined in the random number appendix of the DTRs and validation that appropriate key sizes are used. The protocol must meet the criteria stipulated in Annex A of the PCI PIN Security Requirements.*

EPP Requirement B10

Q 63 Should the average delay between encryptions be calculated for the exhaustive attack of a single PIN block, or should the time be averaged over attacks on multiple PIN blocks?

A *The average time delay should be calculated for an attacker to determine a single PIN value.*

Q 64 In order to prevent exhaustive PIN determination, examples of preventive measures such as a unique key per transaction or the limiting of the rate of PIN encryption to thirty seconds or greater between encipherments as measured over 120 transactions are given. Are any other methods possible?

A *The list of examples is not exhaustive. Other methods are possible. For example, the exclusive use of ISO PIN block format 1 whereby each PIN is enciphered using a unique except by chance random pad of characters with permissible values of 0000 to 1111 may be used to prevent exhaustive PIN determination.*

Q 65 One example given to prevent exhaustive PIN determination is to limit the rate of PIN encryption to thirty seconds or greater between encipherments as measured over 120 transactions. Can this average of 30 seconds between encipherments be determined over a longer time frame than one hour?

A *The intent of the requirement statement is that for any 120 consecutive transactions, the average time between encryptions for a specific PIN entry averages out to approximately 30 seconds.*

EPP Requirement B11

Q 66 Is it acceptable for an EPP 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 mandated in ANSI X9.24 and ISO 11568.*

Q 67 What PIN block formats are allowed?

A *ISO 9564–1 PIN block formats 0, 1 or 3 are acceptable for online transactions. Format 2 must be used for PINs that are submitted from the IC reader to the IC for offline transactions. This applies whether the PIN is submitted in plain-text or enciphered using an encipherment key of the IC.*

PINs enciphered only for transmission between the PIN entry device and the IC reader shall use one of the PIN block formats specified in ISO 9564-1. Where Format 2 PIN blocks are used then a unique key per transaction method in accordance with ISO 11568 shall be used.

Q 68 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 69 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 70 PCI PIN Security Requirement #20 states that all secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal that processes PINs must be unique (except by chance) to that device. How does this requirement apply to EPP testing?

A *EPPs must implement unique secret and private keys for any function directly or indirectly related to PIN protection. The basic rule is that any private or secret key resident in the EPP that is directly or indirectly used for PIN protection whose compromise would lead to the compromise of the same key in another EPP must be unique per device. For example, this means not only the PIN-encryption key(s), but keys that are used to protect other keys, firmware-update keys and display prompt control keys. As stated in the requirement, this does not apply to public keys resident in the EPP. This is not intended to require that the device compare keys across different key hierarchies associated with different acquirers.*

Q 71 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 72 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 an EPP?

A *The intent of the requirement is that the compromise of a key in one transaction-originating device (e.g., an EPP or POS PED) 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 their 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 73 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 a key encipherment key shall be at least of equal or greater strength than the key that it is protecting. What keys does this apply to in an EPP?

A *This applies to any key encipherment keys used for the protection of secret or private keys stored in the device or for keys used to encrypt any secret or private keys for loading or transport to the device. For purpose of this requirement, the following algorithms and keys sizes by row are considered equivalent.*

Algorithm	DES	RSA	Elliptic Curve	DSA/D-H/MQV
Minimum key size in number of bits	112	1024	160	1024/160
Minimum key size in number of bits	168	2048	224	2048/224

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. DSA for digital signatures, and Diffie-Hellman and MQV key agreement key sizes refer to the size of the modulus (p) and the minimum size of a large subgroup (q).

AES keys, of 128 bits or larger are considered stronger than any of the aforementioned.

This does not apply to keys that are used for authentication purposes, such as keys used to validate firmware or display prompts. The sizes of those keys must at minimum be as stipulated in B4 and A8 (for POS PED).

Q 74 Under what conditions is it acceptable for an EPP to allow single component plain-text cryptographic keys to be loaded via the keypad?

A *None. An EPP may not accept entry of single component plain-text secret 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* ***(EPP B6, B7)****.*

Q 75 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 76 Version 2 stipulates that the device must provide support for TR-31 or an equivalent methodology for maintaining the TDES key bundle. Under what circumstances does this apply?

A *If the device supports the exchange of TDEA keys between itself and another device (e.g., a remote host) encrypted under a shared symmetric key, the device must provide support for TR-31 or an equivalent methodology for this key conveyance. This does not imply that the device must support TR-31 or an equivalent methodology between the device and an external ICC reader, but optionally may do so. The device may also optionally support TR-31 or an equivalent methodology for the storage of keys encrypted under a symmetric key. Any equivalent method must include the cryptographic binding of the key usage information to the key value using accepted methods. Any binding or unbinding of key usage information from the key must take place within the secure cryptographic boundary of the device.*

Q 77 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 78 A device may support key check values to validate the successful entry of symmetric key components and/or keys. Are there any restrictions on the use of key check values?

A *Yes. Any returned values shall not exceed six hexadecimal characters and should be at least four hexadecimal characters in length.*

Q 79 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 80 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 81 Requirement B11 stipulates that the device must support TR-31 or equivalent. Key blocks that support padding include a key length that allows the key to be distinguished from the pad characters. In TR-31, the key length information and padding are encrypted along with the key itself by the KEK (termed the Key Block Encryption Key). Does this violate the requirement that a cryptographic key be only used for one purpose, e.g., key encipherment?

A *No. For all TDEA modes of operation, the three cryptographic keys (K1, K2, K3) define a TDEA key bundle. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle cannot be unbundled for any purpose i.e., must never be used separately for any other purpose. A key used to encrypt the key bundle may include in the encrypted portion of the key bundle the key length information and padding as necessary to protect the integrity of the key bundle.*

Q 82 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. Its does not apply when cleartext symmetric keys or their components are loaded using standard dual control techniques.*

Q 83 Can secret keys or their components be used for other purposes such as passwords 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 84 Remote key distribution using asymmetric techniques methodologies must provide for protection against man-in-the-middle attacks and the hijacking of PIN acceptance devices where the devices are under a PKI hierarchy that facilitates more than one acquirer (e.g., a hierarchy under a PIN acceptance device vendor's Root). In order to achieve this, many vendors have implemented techniques that force the PIN acceptance device to "bind" to a specific transaction processing host's certificate, and not accept commands digitally signed by any other hosts. However, in the case of portfolio transfers or other situations where a device must be decommissioned (unbound), from a specific host, what techniques are acceptable for compliance?

A *Decommissions, such as sending a new host's certificate to replace the existing host's certificate without authentication are not acceptable. Any remote decommissioning must require cryptographic techniques and be specific per PIN acceptance device. For example:*

- *The existing bound host can digitally sign an "unbind" command to the PIN acceptance device, that when validated returns the PIN acceptance device to its original unbound state.*
- *In situations where the bound host's private key is not available to sign the command, or other similar scenarios, a forced decommission may occur. However, any such decommission done remotely requires a cryptographic (digital signature, MAC, etc.) technique, and must be unique per PIN acceptation device.*
- *Decommissions may also be done manually directly at the device, using system administration menus that authenticate users via PINs, passphrases, etc.*

In all cases of decommissioning, the existing acquirer related keys must be zeroized as a result of the decommission.

Q 85 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 cleartext key is loaded into the slot without authentication using dual control, then 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 86 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 configurations option. For implementing 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/PINs. The passwords must be entered through the keypad or else conveyed encrypted into the device. These passwords/PINs 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/PINs that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/PINs are at least five characters.*

  Entry of key components without the use of at least two separate passwords/PINs 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, PINs 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 PINs/passwords before injection of the key. These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least five characters in length. These passwords/PINs 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. Plaintext 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 PINs/passwords 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, PINs 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 87 The Guidance for DTR B11 states that "An EPP 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. If an explicit configuration change is required, the change is considered a sensitive service and must meet the requirements of B7, protection of sensitive services.*

EPP Requirement B12

Q 88 ISO 9564 stipulates that a PIN shall be not less than four and not more than twelve characters in length. What PIN lengths must an EPP or POS PED support?

A *EPPs and POS PEDs must be able to support from four to twelve digit PINs for payment card transactions.*

EPP Requirement B13

Q 89 Is it acceptable for a PIN-encryption key to be used as a key-encrypting key, or for a key-encrypting key to be used as a PIN-encrypting key?

A *No. A key must be used for one purpose only as mandated by ANSI X9.24 and ISO 11568-3.*

Q 90 Can an EPP 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.*

Q 91 The device must enforce that data keys, key encipherment keys and PIN-encryption keys have different values. Does this apply to replacement keys downloaded throughout the processing life of the device?

A *The intent of the requirement is to help ensure that these keys are not intentionally used for multiple purposes. Thus the uniqueness check applies for both when the device is initially loaded with these keys and for those that are subsequently loaded. The check must occur across all secret key hierarchies supported by the device. No two secret keys, regardless of purpose, can have the same value.*

EPP Requirement B15

Q 92 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 93 Is it acceptable for an EPP that supports multiple key hierarchies to meet B15 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 94 What are acceptable means of external cryptographic keys selection?

A *Keys may be selected through the EPP 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 95 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 96 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 97 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 EPP must enforce authentication of commands used for external key selection. If the EPP 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 their 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/PINs) either via the key loader or directly via the EPP. 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.