Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

Modular Evaluation Vendor Questionnaire
Version 3.1

September 2011

Document Changes

Date	Version	Description
April 2010	3.0	Initial public release
September 2011	3.1	Clarifications and errata, updates for Non-PIN POIs

Table of Contents

Related Publications

The following references are applicable and related to the information in this manual.

Banking – Retail Financial Services Symmetric Key Management	ANSI X9.24
Triple Data Encryption Algorithm (TDEA) Implementation	ANSI X9.65
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ANSI TR-31
Personal Identification Number (PIN) Management and Security	ISO 9564
Banking – Key Management (Retail)	ISO 11568
Banking – Secure Cryptographic Devices (Retail)	ISO 13491
Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers	ISO/IEC 18033-3
Guidelines on Triple DES Modes of Operation.	ISO TR 19038
Identification Cards – Integrated Circuit Cards	ISO 7816
Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008 – Book 2: Security and Key Management	EMV 4.2
PCI DSS v1.2.1	PCI SSC
PCI DSS Wireless Guidelines	PCI SSC
PCI PTS POI Evaluation Vendor Questionnaire	PCI SSC
PCI PTS POI Security Requirements	PCI SSC
PCI PTS POI DTRs	PCI SSC

Note: *These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.*

Questionnaire Instructions

1. Complete the information below for the device being evaluated.
2. Identify all sections of the questionnaire corresponding to those questions in the form of the *PCI PTS POI Security Requirements* manual ("PCI PTS POI Security Requirements") for which you answered "**YES**."
3. Complete each item in those identified sections.
4. Provide sufficient detail to thoroughly describe the device attribute or function.
5. Refer to and provide additional documentation as necessary.
6. Provide detail in the comments section for all "N/A" answers.

   Example: Question A1.1 in the form of the *PCI PTS POI Security Requirements* manual was answered with a "**YES**." Therefore, all items (1 through 8) in Section A1.1 of this questionnaire must be answered.

Device Identifier	
Device Manufacturer:	
Marketing Model Name/Number:	
Hardware Version Number:	
Firmware Version Number:	
Application Version Number: (if applicable)	

Questionnaire completed by:

Signature ↑	*Date* ↑
Printed Name ↑	*Title* ↑

Core Physical Security Characteristics

Section A1.1

If the answer to A1.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanisms protecting against tampering.
2	The tamper action(s) that trigger(s) the mechanisms.
3	The response of the device to tamper detection. (This should include a written description of how the tamper mechanisms work and how erasure of secret information and/or inoperability is accomplished.)
4	In addition to tamper detection, the protection methods that exist to prevent access to sensitive information, or bug insertion.
5	The mechanisms protecting against physical penetration of the device.
6	The rationale for why the device implementation is such that penetrating and altering the device to disclose sensitive information or to insert a PIN-disclosing bug requires an attack potential of at least 26, with a minimum of 13 for exploitation.
7	The secrets that are erased and the mechanisms used to accomplish this.
8	How any secret information that is not erased is protected.
9	How the merchant or acquirer can easily detect a terminal compromise, e.g., by information on the display or a broken security seal visible to the eye when the terminal is in regular use.

Comments:

Section A1.2

If the answer to A1.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The combinations of tamper detection and/or tamper evidence.
2	How the security mechanisms work.
3	How the security mechanisms are independent.
4	Why the security mechanisms do not rely upon insecure services and characteristics.

Comments:

Section A2

If the answer to A2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the relevant device components permit access to internal areas for maintenance or service. Yes ☐ No ☐
2	If the answer 1 above is **"YES,"** how access to sensitive data such as PIN or cryptographic data is prevented by the design of the internal areas.
3	If the answer 1 above is **"YES,"** the mechanism that causes immediate erasure of sensitive data.
4	How the mechanism is triggered.
5	What sensitive data is erased?
6	The erasure method.

Comments:

Section A3

If the answer to A3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The operational and environmental conditions for which the device was designed.
2	Why the security of the device is not compromised by operational and environmental conditions.
3	The tests performed to ensure the security on the changing operational and environmental conditions (provide test reports).
4	Why the measures are sufficient and effective.

Comments:

Section A4

If the answer to A4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	What sensitive information and functions exist?
2	Where sensitive functions are executed and where sensitive information is used.
3	How sensitive information and functions dealing with sensitive information are protected from modification.
4	The rationale for why the measures are sufficient and effective and would require a per-device attack potential of at least 26 to defeat, with a minimum of 13 for exploitation.
5	How public keys used for functions that impact security-related functions are protected from modification and substitution.
6	How secret and private keys used for functions that impact security-related functions are protected from modification or substitution or disclosure.

Comments:

Section A5

If the answer to A5 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The audible tone for each digit.
2	The tone generator.
3	The power signal to the tone generator.

Comments:

Section A6

If the answer to A6 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The device protections that guard against PIN digits being determined by monitoring sound. (This does not refer to the audible tone, but other sounds when the key is pressed.)
2	The device protections against monitoring electro-magnetic emissions.
3	Any electro-magnetic emissions testing that has been performed. Provide data for the tests performed.
4	The device protections against monitoring power consumption. Provide data for tests performed.
5	Any other external characteristics considered. If applicable, provide data for tests performed.
6	The rationale for why the determination of the entered PIN by monitoring sound, electro-magnetic emissions, or power consumption requires an attack potential of at least 26, with a minimum of 13 for exploitation.

Comments:

Section A7

If the answer to A7 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The device components that store or use cryptographic keys related to the operations under the scope of the device requirements.
2	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components' design.
3	Whether the device includes any tamper-detection and response mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section A1.1.
4	Whether the device includes any tamper-resistance mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section A1.1.
5	The rationale for why the device implementation is such that the cost of determining any PIN-security-related cryptographic key resident in the device—either by penetration of the device or by monitoring emanations from the device (including power fluctuations)—exceeds an attack potential of at least 35, with a minimum of 15 for exploitation.

Comments:

Section A8

If the answer to A8 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	What are the protections against the alteration of prompts for non-PIN data?
2	What is the response of the device to an attempt to alter prompts for non-PIN data?
3	The rationale for why the unauthorized alteration of prompts for non-PIN data entry into the device such that PINs are compromised, cannot occur without an attack potential of at least 18 per device with a minimum of 9 for initial exploitation.

Comments:

Section A9

If the answer to A9 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The means provided by the device to deter the visual observation of PIN values as they are entered by the cardholder.
2	If visual observation deterrent is a PIN shield, how the PIN shield is attached to the device frame and whether it could be removed.

Comments:

Section A10

If the answer to A10 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanisms used to prevent skimming attacks against the device.
2	The mechanisms such that it is not feasible to modify or penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader or the device's hardware or software, in order to determine or modify magnetic-stripe track data.
3	If the mechanism causes the device to be locked as part of the action taken, describe how the unlocking takes place.
4	The rationale for why modification or penetration of the device to make any additions, substitutions, or modifications to the magnetic-stripe reader or the device's hardware or software, in order to determine or modify magnetic-stripe track data requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation.

Comments:

Section A11

If the answer to A11 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanism(s) used to protect the secure component(s) against unauthorized removal.
2	The mechanism's design.
3	Whether the mechanism(s) are active or passive?
4	What happens when one of the mechanisms is triggered?
5	The method of installation, activation, temporary de-activation and re-activation.
6	If passwords or other secret data are used for the mechanism, describe the initialization and use.
7	The rationale for why the component implementation is such that disabling the tamper mechanisms requires an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation.

Comments:

Core Logical Security Characteristics

Section B1

If the answer to B1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The set of relevant device components.
2	All self-tests performed by the relevant device components.
3	The response of the device to a self-test failure for each type of component.
4	The types of events that initiate self-tests for each type of test.

Comments:

Section B2

If the answer to B2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which commands are accepted by the affected device components?
2	How the commands are linked to the device modes.
3	What type of parameter- and data-checking is performed?
4	Why the functionality is not influenced by logical anomalies.
5	Any tests that have been performed to ensure the functionality is not influenced by logical anomalies. Provide a rationale why the test coverage is sufficient.
6	How sensitive information or the PIN is prevented from being outputted in clear-text.

Comments:

Section B3

If the answer to B3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The documented firmware review process and frequency.
2	The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.

Comments:

Section B4

If the answer to B4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which components of the device allow updates of firmware and/or software?
2	The mechanisms used and the device components affected by the firmware/software update.
3	What cryptographic algorithms and key sizes are used for firmware/software authentication?
4	What is the device's response if firmware/software to be updated cannot be authenticated?
5	How the firmware/software is deleted if rejected.

Comments:

Section B5

If the answer to B5 in the *PCI PTS POI PED Security Requirements* was "YES," describe:

1	What is displayed to the cardholder when PIN digits are entered?
2	What is displayed to the terminal operator and/or sales clerk when PIN digits are entered?

Comments:

Section B6

If the answer to B6 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How it is ensured that the online PIN is encrypted within the EPP immediately after PIN entry is complete and has been signified as such by the cardholder.
2	How it is ensured that the PIN does not remain in plain-text form in any location after encryption.
3	The maximum time a plain-text PIN can exist after completion of PIN entry by the cardholder.
4	Which sensitive information (PIN/keys) is used by which component in the course of a transaction?
5	How the end of a transaction is defined.
6	The data that is automatically cleared from the device's internal buffers when a transaction is completed.
7	The location of all buffers that are cleared.
8	The process used to clear the buffers.
9	What is the time-out period for a device waiting for the response from the cardholder or background system?
10	The action taken by the device upon time-out.

Comments:

Section B7

If the answer to B7 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The sensitive functions provided by the device. *Sensitive functions are functions that are not intended to be accessed by end users (cardholders and merchants) that can impact the security of the device. Examples are key loading or the definition and maintenance of user roles.*
2	How the device controls the access and use of sensitive functions.
3	The authentication method used to access sensitive services.
4	The measures that ensure that entering or exiting sensitive services do not reveal or otherwise affect sensitive information.
5	The interface used to authenticate access to sensitive services.
6	Whether an external device is used to authenticate access to sensitive services.
7	How the authentication data used to access sensitive services in the device is protected, as it is input/output via the interface.
8	Which of the following is true for the data referred to in 7 above: ☐ Data inputs cannot be discerned from any displayed characters. ☐ Data inputs cannot be discerned by monitoring audible or electro-magnetic emissions. ☐ Sensitive data is cleared from internal buffers upon exiting a secure mode.

B7, continued

9	The management of any data used for authentication. *Examples of authentication data are passwords, cryptographic keys, and hardware tokens*. Include:	
	▪ The number of devices that share the same keys or passwords.	
	▪ Cryptographic algorithms used for authentication, if applicable.	
	▪ Data size (key or password length)	
	▪ How authentication data is distributed to legitimate users	
	▪ How authentication data can be updated	
10	The device's response to false authentication data.	

Comments:

Section B8

If the answer to B8 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	What is the limit on the number of actions that can be performed when using sensitive functions?
2	The rationale for the limit that was chosen.
3	How the chosen limit on the number of actions minimizes the risks from unauthorized use of sensitive services.
4	The device's response once the limit on the number of actions has been reached.
5	The maximum time the device may remain inactive once it has accessed sensitive functions.
6	The action taken by the device once the maximum time for inactivity has been reached.
7	The maximum time before the device returns to normal mode after initially accessing sensitive functions.
8	The action take by the device once the maximum time is reached.

Comments:

Section B9

If the answer to B9 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The implementation of the random number generator.
2	The tests performed to demonstrate that the numbers produced are sufficiently unpredictable.
3	How the random numbers generated by the device's RNG are used to protect sensitive data.

Comments:

Section B10

If the answer to B10 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The characteristics that prevent or significantly deter the use of a stolen device for exhaustive PIN determination.
2	How PIN entry is limited to an average of one per 30 seconds for any 120 consecutively entered PINs.

Comments:

Section B11

If the answer to B11 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The Fixed Key, Master Key/Session Key, or Unique Key Per Transaction (UKPT) PIN protection technique.	
2	Whether each key is used for only one cryptographic purpose. Yes ☐ No ☐	
	How is this enforced?	
3	How keys are protected during key storage against unauthorized disclosure and substitution.	
4	How key separation is ensured during key storage.	
5	All cryptographic algorithms implemented by the device.	
6	For all cryptographic keys that reside within an operational device, indicate the following:	
	▪ Name	
	▪ Key size	
	▪ Associated cryptographic algorithm	
	▪ The data that may be encrypted under the key	
	▪ The number of instances or registers for that key type	
	▪ How the key is identified by the device so that it is used only as intended	
7	Whether the device has the ability to erase cryptographic keys. Yes ☐ No ☐	
8	What keys may be erased?	
9	What process is used for erasure?	
10	Under what circumstances are keys erased? Describe for all device states (power-on, power-off, sleep mode).	

B11, continued

11	What other data are erased?	
	Under what circumstances?	
12	What keys are not erased?	
13	How all keys present or otherwise used in the device are loaded, including who (e.g., acquirer or manufacturer) generates and whether the keys are loaded encrypted or as plain-text or as encrypted or plain-text components/secret shares.	
14	Whether there is a key-distribution technique present that uses an asymmetric algorithm with a public key for the exchange of symmetric secret keys and address each of the following points.	
	▪ Utilizes a random/pseudo-random key-generation process such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others?	Yes ☐ No ☐ N/A ☐
	Is the random source tested in a suitable manner before key generation?	Yes ☐ No ☐
	▪ How is the authenticity of public keys ensured?	
	Is there a certificate hierarchy?	Yes ☐ No ☐
	How are certificates (signed public keys of the key-exchange partners) generated, i.e., who signs?	
	▪ Is there mutual device authentication?	Yes ☐ No ☐
	If certificates are used, how are they tested and accepted or rejected?	
	▪ Is there a secure formatting and padding of the message used containing the symmetric secret key?	Yes ☐ No ☐
	Is the correctness of the message structure tested by the receiver?	Yes ☐ No ☐
14	How the authenticity of origin is ensured—e.g., is the signature of the exchange message tested?	
	▪ What is the reaction of the device if an authenticity test fails?	
	▪ Which effective key length(s) is/are utilized for all the cryptographic algorithm(s) in question?	
	▪ Is the chosen key length appropriate for the algorithm and its protection purpose?	Yes ☐ No ☐
	▪ In case RSA is used, is the key length at least 2048 bit?	Yes ☐ No ☐

B11, continued

15	The hashing algorithm(s) that are used.
	The purpose of the usage(s).
16	Whether single component keys can be loaded and the algorithm used to encrypt them during key entry.
17	All storage and usage locations for each key ever present in or used by the device.
18	Each combination of key-exchange technique and key-storage mechanism supported by the device (e.g., ANSI TR-31).
19	Whether the device uses any key-derivation method. Yes ☐ No ☐
	If so, describe the method.
20	Whether any keys are calculated as a variant of another key. Yes ☐ No ☐
	If so, describe how the variant(s) are protected at an equivalent or greater level of security as the original key(s).

Comments:

Section B12

If the answer to B12 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the Triple-DES PIN-encryption implementation conforms to ISO 9564. Yes ☐ No ☐
	How does it conform?
2	The PIN block formats supported by the device.

Comments:

Section B13

If the answer to B13 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	For every key used for PIN encryption, indicate what type of data can be encrypted or decrypted.
2	How plain-text PIN data is distinguished from any other data that might be entered into a device.
3	How encrypted PIN data is distinguished from all other data encrypted or plain-text.
4	All key-encrypting keys.
5	What data can be encrypted using key-encrypting keys.
6	How this data is distinguished from all other data.
7	How encrypted keys are distinguished from all other data.
8	How the device enforces that data keys, key-encipherment keys, and PIN-encipherment keys have different values.

Comments:

Section B14

If the answer to B14 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether there is a mechanism that will allow the output of plain-text secret or private cryptographic keys or plain-text PINs. Yes ☐ No ☐
	If yes, describe the mechanism.
2	How the outputting of plain-text keys and plain-text PINs is prevented.
3	In what locations within the device cryptographic keys may exist in plain-text.
4	Under what circumstances a plain-text key may be transferred from each of the above locations to another location within the device.

Comments:

Section B15

If the answer to B15 in the *PCI POS PED Security Requirements* was "YES," describe:

1	Whether transactions intended to be performed solely by the cardholder (unaided by a merchant).
2	Whether the transaction amount is entered by the cardholder or the merchant.
3	How the amount entry and PIN are separate operations.

Comments:

Section B16.1

If the answer to B16.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The protections against the alteration of prompts for non-PIN data.
2	The response of the device to an attempt to alter prompts for non-PIN data.
3	The rationale for why circumvention cannot occur without an attack potential of at least 18 per device, with a minimum of 9 for exploitation.

Comments:

Section B16.2

If the answer to A16.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The implemented cryptographic algorithms/mechanisms/protocols that protect the control of the device's display and device usage.
2	The device's response if the authentication fails.
	How unauthorized actions/replacements are rejected.
	How it is infeasible for an entity not possessing the unlocking mechanism to alter the display and how the output of unencrypted PIN data from the device is prevented for such an entity.
3	The controls that provide unique accountability to entities for functionality/actions of the software. Describe the unique assignment of cryptographic keys and the implemented cryptographic algorithm(s) that are applicable.
4	Which effective key length(s) is/are utilized for all the cryptographic algorithm(s) in question.
	Is the chosen key length appropriate for the algorithm and its protection purpose? Yes ☐ No ☐
5	The key management, key distribution and other techniques defined and used for the cryptographic key(s) in question. Describe who/which entity possesses which key(s) and under what circumstances.
6	How the principles of dual control and split of knowledge/secret-sharing are realized for secret parameters/keys.

Comments:

Section B17

If the answer to B17 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the device support multiple applications. Yes ☐ No ☐
	If yes, provide a list of these applications, and identify those with security impact.
	If yes, how is the separation between applications with security impact from those without security impacts enforced?
2	For each security relevant application, list by groups the data objects and their location.
3	Which mechanism prevents applications to access data objects not belonging to it.

Comments:

Section B18

If the answer to B18 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The method to ensure that the operating system contains only the components and the services necessary for the intended operation.
2	The procedures used for maintenance and updates of the operating system.
3	The rationale for why the method used to enforce least privilege is effective.
4	The rationale for why all the components and services listed in the configuration list are necessary.

Comments:

Section B19

If the answer to B19 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The documented review process and release cycle of updates for the integration documentation and the relationship of the release cycle to the design/manufacturing cycle.
2	The procedures that exist for the integration documentation to be shipped or otherwise made available to integrators.

Comments:

Online Security Characteristics

Section C1

If the answer to C1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any means available to a cardholder or merchant to issue commands that result in the selection of keys by the device (buttons that can be pressed to select between acquirers, for instance).
2	How the device prohibits against unauthorized key replacement and key misuse.
3	How the device authenticates key selection commands, if the device supports multiple key hierarchies.

Comments:

Offline Security Characteristics

Section D1

If the answer to D1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The protections used to prevent penetration of the device for the purpose of determining or modifying sensitive data.
2	The specialized skills and equipment that would be necessary to penetrate the device in order to determine or modify sensitive data.
3	Why it is not feasible to penetrate the ICC reader to modify the ICC reader hardware or software in order to determine or modify sensitive data without requiring an attack potential of at least 20, with a minimum of 10 for exploitation.

Comments:

Section D2

If the answer to D2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The rationale as to why the slot does not have sufficient space to hold a PIN-disclosing bug.
2	The size of the largest object that can be concealed within the ICC reader slot.
3	The dimensions of the space within the ICC reader.
4	Any design documentation references, such as assembly drawings, that have been submitted for evaluation that provide information about the geometry and dimensions of the ICC reader.
5	The rationale as to why the slot occupied by the ICC cannot feasibly be enlarged to provide space for a PIN-disclosing bug.
6	Any special materials or protections intended to prohibit ICC reader slot enlargement.
7	Whether there is sufficient space for two ICCs to be inserted at one time while still allowing a legitimate ICC to be read. Yes ☐ No ☐
8	The opening of the ICC reader and how its design ensures that obstructions or suspicious objects are detectable by the cardholder.
9	The ICC insertion process, including the role and functions of any slot cover.
10	The rationale as to why the ICC reader prevents or otherwise detect the successful implant of a sensitive-data-disclosing bug aiming at capturing offline PIN and IC card information
11	Any feature, mechanism or subsystem preventing he successful implant of a sensitive-data-disclosing bug aiming at capturing offline PIN and IC card information.

Comments:

Section D3

If the answer to D3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The rationale as to how the ICC reader is constructed so that wires running out of the slot to an external bug would be observed by a cardholder.
2	Whether the device has any seams or channels near the ICC reader slot opening. Yes ☐ No ☐
	If so, provide a rationale for why these cannot be used to obscure wires running from the opening to an external bug.

Comments:

Section D4

If the answer to D4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the device supports both enciphered and plain-text methods of ICC user authentication. Yes ☐ No ☐
2	How the PIN is enciphered between the devices, if the ICC reader and the device encrypting the PIN are separate. Specify algorithms and keys used for this.
3	The key and algorithm used to encipher the PIN when it is submitted to the ICC, if the ICC reader and the device encrypting the PIN are integrated.
4	The circumstances where a plain-text PIN (or PIN block) may transit outside of the device encrypting the PIN or ICC reader.
5	A justification for all "No" and "N/A" answers provided to D4 in the *PCI Unattended Payment Terminal Security Requirements* manual. Note that a "Yes" answer is required for all methods of PIN transmission between the device encrypting the PIN and ICC reader that are supported by the device.

Comments:

POS Terminal Integration

Section E1

If the answer to E1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information about the physical and logical security perimeter (related to PIN entry and card-reading functions).

Comments:

Section E2.1

If the answer to E2.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how the logical and physical integration of a PCI-approved secure component (or components) into a PIN entry POI terminal does not impact the overall PIN-protection level.
2	How the integration of every approved secure component has been performed strictly according to the component manufacturer's recommendations.
3	Why the failure, removal, or absence of an approved secure component does not lead to another approved secure component revealing any PIN-related sensitive information.
4	The mechanisms that prevent the failure, removal, or absence of an approved secure component from leading to the device used for PIN entry to fall back into a non-safe mode.
5	The tests used to verify the effectiveness of the measures.

Comments:

Section E2.2

If the answer to E2.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how the overall device does not facilitate the fraudulent placement of an overlay over the PIN pad.
2	The rationale for why the implementation is such that placing an overlay with a PIN-disclosing bug requires an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation.

Comments:

Section E3.1

If the answer to E3.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how the logical and physical integration of an approved secure component into a PIN entry POI terminal does not create new attack paths to the PIN.
2	How the integration of approved secure component(s) has been performed strictly according to the component manufacturer's recommendations.
3	Why the failure of a secure component does not create new attack paths to the PIN—e.g., the device used for PIN entry does not fall back into a non-safe mode.

Comments:

Section E3.2

If the answer to E3.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The device protections that prevent against attacks aiming, retaining, and stealing the payment card (e.g., Lebanese Loop attack).
2	Whether active or passive mechanisms are used.
3	If the mechanism causes the device to be locked as part of the action taken, describe how the unlocking takes place.
4	The rationale for why in the device implementation Lebanese Loop attacks are effectively prevented.
5	The tests used to verify the effectiveness of the measures.

Comments:

Section E3.3

If the answer to E3.3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any documentation references such as a user guide, specification of the device's logical structure, the device's interface specification, or the software implementation which define the logical and physical segregation between secure components and non-secure components.

Comments:

Section E3.4

If the answer to E3.4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The transaction flow, and which hardware and software components control the display and the device.
2	By which means the correspondence between the display messages visible to the cardholder and the operating state (i.e., secure or non-secure mode) of the device is enforced?
3	If cryptographic methods are used, describe the technique, the components involved and the key management.
4	Whether commands impacting the correspondence between the display messages and the operating state of the device received from an external device. Yes ☐ No ☐
	If yes, which method of authentication is used? Include in the description the algorithms, keys, and key management involved.
5	The rationale for why alteration of the correspondence between the display messages and the operating state cannot occur without an attack potential of at least 18 per device, with a minimum of 9 for exploitation.

Comments:

Section E3.5

If the answer to E3.5 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which interface(s) of the device can accept numeric entry?
2	Which interface of the device is intended for the payment card PIN?
3	If another interface is present which can be used for numeric entry, and therefore may by misused for PIN entry, what mechanism(s) prevents its use for PIN entry?

Comments:

Section E4.1

If the answer to E4.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the device contains secure components previously assessed under A11. Yes ☐ No ☐
2	The mechanism(s) used to protect the component against unauthorized removal.
3	The mechanism's design.
4	Whether the mechanism(s) are active or passive.
5	What happens when one of the mechanisms is triggered?
6	The method of installation, activation, temporary de-activation and re-activation.
7	If passwords or other secret data are used for the mechanism, describe the initialization and use.
8	The rationale for why the implementation is such that disabling the tamper mechanisms requires an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation.

Comments:

Section E4.2

If the answer to E4.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how to implement the protection system(s) against unauthorized removal.
2	The documented review process and release cycle of updates for the integration documentation and the relationship of the release cycle to the design/manufacturing cycle.
3	The procedures that exist for the integration documentation to be shipped or otherwise made available to integrators

Comments:

Section E4.3

If the answer to E4.3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how to implement the protection system(s) against unauthorized removal for each embedded device.
2	The documented review process and release cycle of updates for the integration documentation and the relationship of the release cycle to the design/manufacturing cycle.
3	The procedures that exist for the integration documentation to be shipped or otherwise made available to integrators.

Comments:

Open Protocols

Platform Description

1	Describe, or refer to a description of, the different models that currently use the platform. Provide information about the differences between the different models. Indicate for each model all the communication channels, possible peripherals, intended use.
2	Describe, or refer to a description of, the hardware referenced by the hardware version number. Provide information about the general architecture, processor, and communication modules. Clearly indicate the hardware boundaries of the approved platform.
3	Describe, or refer to a description of, the firmware referenced by the firmware version number. Provide detailed information about the operating system and communication libraries (e.g., suppliers, product names and versions). Clearly indicate the firmware boundaries of the approved platform.
4	Describe, or refer to a description of, the application referenced by the application version number. Provide detailed application information (e.g., suppliers, product names and versions). Clearly indicate the application boundaries of the approved platform.
5	Describe, or refer to a description of, the intended use of the protocols and services listed in the *Open Protocols Module – Protocol Declaration Form*. Make clear which are intended for financial applications and terminal management.
6	Describe, or refer to a description of, the intended use of the devices based on the platform: set-up, possible applications, and users.
7	Indicate, or refer to documentation, if devices based on the platform can be used for other (non-financial) applications. List and describe these applications.

Comments:

Protocols and Services

Section F: IP and Link Layer

This table must be completed considering the IP and link layer **in their entirety.**

1	Reference and provide documentation that describes the link layer options that are available on the platform.
2	Describe how the vulnerability assessment of the IP and link layer was executed, and why this leads to the assertion that it does not contain exploitable vulnerabilities. Reference and provide vulnerability assessment documentation, vulnerability survey evidence, and test evidence.
3	Reference and provide the security guidance that describes how the IP and link layer must be securely used.
4	Describe, or refer to a description of, the default configuration of the IP and link layer. Provide documentation supporting the statement.

Comments:

Section G: IP Protocols

This table must be completed considering the IP protocols **in their entirety**.

1	Reference and provide documentation that describes the IP protocols that are available on the platform.
2	Describe how the vulnerability assessment of the IP protocols was executed, and why this leads to the assertion that they do not contain exploitable vulnerabilities. Reference and provide vulnerability assessment documentation, vulnerability survey evidence, and test evidence.
3	Reference and provide the security guidance that describes how the IP protocols must be securely used.
4	Describe, or refer to a description of, the default configuration of the IP protocols. Provide documentation supporting the statement.

Comments:

Section H: Security Protocols

Table H-1 below must be completed considering the Security protocols **in their entirety**.

Table H-1: Security Protocols in their Entirety

1	Reference and provide documentation that describes the security protocols that are available on the platform.
2	Describe how the vulnerability assessment of the security protocols was executed, and why this leads to the assertion that they do not contain exploitable vulnerabilities. Reference and provide vulnerability assessment documentation, vulnerability survey evidence, and test evidence.
3	Reference and provide the security guidance that describes how the security protocols must be securely used.
4	Describe, or refer to a description of, the default configuration of the security protocols. Provide documentation supporting the statement.

Comments:

Table H-2 **must be completed for each of the security protocols** that might be used for financial applications or platform management.

Table H-2: Specified Security Protocol

5	Reference and provide the security guidance supporting the response to H5 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference
6	Reference and provide documentation describing the encryption mechanism of the security protocol, supporting the response to H6 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Table H-2 (continued)

7	Reference and provide documentation describing the integrity mechanism of the security protocol, supporting the response to H7 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference
8	Reference and provide documentation describing the server authentication mechanism of the security protocol, supporting the response to H8 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference
9	Reference and provide documentation describing the replay protection used by the security protocol, supporting the response to H9 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference
10	Reference and provide documentation describing the random generator used by the security protocol, supporting the response to H10 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section I: IP Services

Table I-1 below must be completed considering the IP Services **in their entirety.**

Table I-1: IP Services in their Entirety

1	Reference and provide documentation that describes the IP services that are available on the platform.
2	Describe how the vulnerability assessment of the IP services was executed, and why this leads to the assertion that they do not contain exploitable vulnerabilities. Reference and provide vulnerability assessment documentation, vulnerability survey evidence, and test evidence.
3	Reference and provide the security guidance that describes how the IP services must be securely used.
4	Describe, or refer to a description of, the default configuration of the IP services. Provide documentation supporting the statement.
5	Reference and provide documentation describing how the platform supports session management, supporting the response to I5 in the *PCI PTS POI Security Requirements*.

Comments:

Table I-2 **must be completed for each of the IP Services** that might be used for financial applications or platform management.

Table I-2: Specified IP Service

6	Reference and provide documentation describing how the IP Service ensures confidentiality, integrity, authentication and protection against replay by using an appropriate security protocol, supporting the response to I6 of the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section J: Security Management

1	Reference and provide the security guidance, supporting the response to J1 of the *PCI PTS POI Security Requirements.*
2	Reference and provide the documentation describing the security maintenance measures, supporting the response to J2 of the *PCI PTS POI Security Requirements.*
3	Reference and provide the documentation describing the vulnerability disclosure measures, supporting the response to J3 of the *PCI PTS POI Security Requirements.*
4	Reference and provide the documentation describing the update mechanisms and the security guidance, supporting the response to J4 of the *PCI PTS POI Security Requirements.*

Comments:

Account Data Encryption

Section K1

If the answer to K1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The component(s) that implement an account-data encryption function.
1.1	For each identified component, when and how account data is encrypted.
2	What processes besides encryption can be performed within the secure controller.
2.1	For each identified process, why this process does not impact the security of the encryption function.

Comments:

Section K1.1

If the answer to K1.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

For ICC-Based Entry

1	The protections used to prevent penetration of the device for the purpose of determining or modifying account data.
2	The specialized skills and equipment that would be necessary to penetrate the device in order to determine or modify account data.
3	Why it is not feasible to penetrate the ICC reader to modify the ICC reader hardware or software in order to determine or modify account data without requiring an attack potential of at least 16, with a minimum of 8 for exploitation.

Comments:

For Magnetic-Stripe Entry

1	The mechanisms used to prevent skimming attacks against the device.
2	The mechanisms such that it is not feasible to modify or penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader or the device's hardware or software, in order to determine or modify account data.
3	If the mechanism causes the device to be locked as part of the action taken, describe how the unlocking takes place.
4	The rationale for why modification or penetration of the device to make any additions, substitutions, or modifications to the Magnetic-stripe Reader or the device's hardware or software, in order to determine or modify account data requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation.

Comments:

Section K1.1 (continued)

For Manual PAN Key Entry

1	The protections used to prevent penetration of the device for the purpose of determining or modifying account data.
2	The specialized skills and equipment that would be necessary to penetrate the device in order to determine or modify account data.
3	Why it is not feasible to penetrate the input device's hardware or software in order to determine or modify account data without requiring an attack potential of at least 16, with a minimum of 8 for exploitation.

Comments:

Section K1.1 (continued)

Tamper-Detection Mechanisms

1	The mechanisms protecting against tampering.
2	The tamper action(s) that trigger(s) the mechanisms.
3	The response of the device to tamper detection. (This should include a written description of how the tamper mechanisms work and how erasure of secret information and/or inoperability is accomplished.)
4	In addition to tamper detection, the protection methods that exist to prevent access to account data, or bug insertion.
5	The mechanisms protecting against physical penetration of the device.
6	The rationale for why the device implementation is such that penetrating and altering the device to disclose sensitive information or to insert an account data-disclosing bug requires an attack potential of at least 16, with a minimum of 8 for exploitation.
7	The secrets that are erased and the mechanisms used to accomplish this.
8	How any secret information that is not erased is protected.

Comments:

Section K1.1 (continued)

Independent Security Mechanisms

1	The combinations of tamper detection and/or tamper evidence.
2	How the security mechanisms work.
3	How the security mechanisms are independent.
4	Why the security mechanisms do not rely upon insecure services and characteristics.

Comments:

Section K2

If the answer to K2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Any design documentation references, such as assembly drawings, schematics, housing/frame, or data sheets that provide information on how the logical and physical integration of an approved component into a PIN entry POI terminal does not create new attack paths to the account data.
2	How the integration of approved component(s) has been performed strictly according to the component manufacturer's recommendations.
3	Why the failure of a component does not create new attack paths to the account data.
4	Whether the relevant device components permit access to internal areas for maintenance or service. Yes ☐ No ☐
5	If the answer 4 above is "YES," how access to account data is prevented by the design of the internal areas.
6	If the answer 4 above is "YES," the mechanism that causes immediate erasure of account data.
7	How the mechanism is triggered.
8	The erasure method.

Comments:

Section K3

If the answer to K3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The device components that store or use cryptographic keys related to the operations under the scope of the device requirements.
2	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components' design.
3	Whether the device includes any tamper-detection and response mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section K1.1.
4	Whether the device includes any tamper-resistance mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section K1.1.
5	The rationale for why the device implementation is such that the cost of determining any account-data encryption related cryptographic key resident in the device—either by penetration of the device or by monitoring emanations from the device (including power fluctuations)—exceeds an attack potential of at least 26, with a minimum of 13 for exploitation.

Comments:

Section K3.1

If the answer to K3.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How the integrity of the public key is ensured.
2	How the authenticity of the public key is ensured.
3	The rationale for why the device implementation is such that the cost of or modifying any public key used for account data protection purposes which is resident in the device exceeds an attack potential of at least 26, with a minimum of 13 for exploitation.

Comments:

Section K4

If the answer to K4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The encryption algorithm being used.
2	The padding mechanism being used.
3	The mode of operation being used.
4	The key size being used.
5	Any relevant documentation, such as security evaluation reports, schematics, data sheets, vendor test procedures and test reports about the encryption algorithm, padding mechanism and mode of operation being used.
6a	The credentials of the expert reviewer that assessed the security of the mode of operation used by the encryption algorithm (if a non-standardized mode of operation is in use).
6b	How the expert reviewer is independent to the vendor.

Comments:

Section K5

If the answer to K5 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How the device supports mutual authentication.
2	The protocol used to provide mutual authentication.
3	How freshness and liveness of messages exchanged during mutual authentication is provided.

Comments:

Section K6

If the answer to K6 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanism used to support data origin authentication.

Comments:

Section K7

If the answer to K7 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The process by which only unique keys will be used by device.

Comments:

Section K8

If the answer to K8 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	For every key used for account data protection resident within the device, indicate what type of data can be encrypted, decrypted, signed and verified.
2	How plain-text account data is distinguished from any other data that might be entered into a device.
3	How encrypted account data is distinguished from all other encrypted or plain-text data.
4	All account data key-encrypting keys.
5	What account data can be encrypted using key-encrypting keys.
6	How this account data is distinguished from all other data.
7	How account data encrypting keys are distinguished from all other data.
8	How the device enforces that account data-encipherment keys, key-encipherment keys, and PIN-encipherment keys are different values.

Comments:

Section K9

If the answer to K9 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which components of the device allow remote connections.
2	The mechanisms used and the device components affected by the remote connection.
3	How accountability for the entity initiating the access attempt is ensured.
4	How freshness and liveness of the access attempt is ensured.
5	What cryptographic algorithms (including padding mechanisms and modes of operation), protocols and key sizes are used for remote connections.
6	The device's response if remote access request cannot be authenticated.
7	How the connection is dropped if rejected.

Comments:

Section K10

If the answer to K10 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The documented firmware review process and frequency.
2	The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.

Comments:

Section K11

If the answer to K11 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The set of relevant device components.
2	All self-tests performed by the relevant device components.
3	The response of the device to a self-test failure for each type of component.
4	The types of events that initiate self-tests for each type of test.
7	What cryptographic algorithms and key sizes are used for firmware/software authentication?
8	What is the device's response if firmware/software cannot be authenticated?

Comments:

Section K11.1

If the answer to K11.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which components of the device allow applications to be loaded?
2	What cryptographic algorithms and key sizes are used for application authentication?
3	What is the device's response if the application cannot be authenticated?
4	How the application is deleted if rejected.
5	Which components of the device allow software application/configuration updates.
6	The mechanisms used and the device components affected by the updates.
	What cryptographic algorithms and key sizes are used for software application/configuration authentication?
	What is the device's response if software application/configuration to be updated cannot be authenticated?
	How the software application/configuration update is deleted if rejected.

Comments:

Section K11.2

If the answer to K11.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The guidance that is provided to application developers.

Comments:

Section K12

If the answer to K12 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which components of the device allow updates of firmware and/or software?
2	The mechanisms used and the device components affected by the firmware/software update.
3	What cryptographic algorithms and key sizes are used for firmware/software authentication?
4	What is the device's response if firmware/software to be updated cannot be authenticated?
5	How the firmware/software is deleted if rejected.

Comments:

Section K13

If the answer to K13 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Which commands are accepted by the affected device components?
2	How the commands are linked to the device modes.
3	What type of parameter- and data-checking is performed?
4	Why the functionality is not influenced by logical anomalies.
5	Any tests that have been performed to ensure the functionality is not influenced by logical anomalies. Provide a rationale why the test coverage is sufficient.
6	How account data is prevented from being outputted in clear-text.

Comments:

Section K14

If the answer to K14 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How the security requirements specified in sections H and J of the Open Protocols Module have been met.

Comments:

Section K15

If the answer to K15 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How the security requirements specified in sections F, G, and I of the Open Protocols Module have been met.

Comments:

Section K16

If the answer to K16 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether there is are mechanism(s) that will allow the outputting of plain-text account data. Yes ☐ No ☐
	If yes, describe these mechanisms.
2	The mechanism that allows the device to switch between encrypting and non-encrypting mode.
3	How the outputting of plain-text account data is prevented.
4	Which components of the device allow encryption to be enabled/disabled.
5	How accountability for the entity initiating the enablement/disablement attempt is ensured.
6	How freshness and liveness of the enablement/disablement attempt is ensured.
7	What cryptographic algorithms (including padding mechanisms and modes of operation), protocols and key sizes are used for remote enablement/disablement.
8	The mechanism that provides protection against attacks designed to determine the valid, full PANs knowing only the truncated output (the mechanism should yield equivalence to determining a 16-digit PAN knowing only the first 6 and last four digits).

Comments:

Section K16.1

If the answer to K16.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The process of how applications are loaded onto the device.
2	How access to account data from other applications residing on the device is prevented.

Comments:

Section K16.2

If the answer to K16.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How it is ensured that the account data does not remain in plain-text form in any location after encryption.
2	The maximum time a plain-text account data can exist after completion of a transaction.
3	Which sensitive information (account data/keys) is used by which component in the course of a transaction?
4	How the end of a transaction is defined.
5	The data that is automatically cleared from the device's internal buffers when a transaction is completed.
6	The location of all buffers that are cleared.
7	The process used to clear the buffers.
8	What is the time-out period for a device waiting for the response from the cardholder or background system?
9	The action taken by the device upon time-out.

Comments:

Section K17

If the answer to K17 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How surrogate PANs are generated.
2	The tests performed to demonstrate that the probability of determining the original PAN knowing only the surrogate value should be no better than a random guess.

Comments:

Section K17.1

If the answer to K17.1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The length of the salt that is used.
2	The method of generating salt, including how random numbers are generated.

Comments:

Section K17.2

If the answer to K17.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Why it is not feasible to penetrate the device's hardware or software in order to determine or modify a salt value without requiring an attack potential of at least 16, with a minimum of 8 for exploitation.

Comments:

Section K18

If the answer to K18 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The Fixed Key, Master Key/Session Key, or Unique Key Per Transaction (UKPT) PIN protection technique.	
2	Whether each key is used for only one cryptographic purpose. Yes ☐ No ☐	
	How is this enforced?	
3	How keys are protected during key storage against unauthorized disclosure and substitution.	
4	How key separation is ensured during key storage.	
5	All cryptographic algorithms implemented by the device.	
6	For all cryptographic keys that reside within an operational device, indicate the following:	
	▪ Name	
	▪ Key size	
	▪ Associated cryptographic algorithm	
	▪ The data that may be encrypted under the key	
	▪ The number of instances or registers for that key type	
	▪ How the key is identified by the device so that it is used only as intended	
7	Whether the device has the ability to erase cryptographic keys. Yes ☐ No ☐	
8	What keys may be erased?	
9	What process is used for erasure?	
10	Under what circumstances are keys erased? Describe for all device states (power-on, power-off, sleep mode).	

K18, continued

11	What other data are erased?	
	Under what circumstances?	
12	What keys are not erased?	
13	How all keys present or otherwise used in the device are loaded, including who (e.g., acquirer or manufacturer) generates and whether the keys are loaded encrypted or as plain-text or as encrypted or plain-text components/secret shares.	
14	Whether there is a key-distribution technique present that uses an asymmetric algorithm with a public key for the exchange of symmetric secret keys and address each of the following points.	
	▪ Utilizes a random/pseudo-random key-generation process such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others?	Yes ☐ No ☐ N/A ☐
	Is the random source tested in a suitable manner before key generation?	Yes ☐ No ☐
	▪ How is the authenticity of public keys ensured?	
	Is there a certificate hierarchy?	Yes ☐ No ☐
	How are certificates (signed public keys of the key-exchange partners) generated, i.e., who signs?	
	▪ Is there mutual device authentication?	Yes ☐ No ☐
	If certificates are used, how are they tested and accepted or rejected?	
	▪ Is there a secure formatting and padding of the message used containing the symmetric secret key?	Yes ☐ No ☐
	Is the correctness of the message structure tested by the receiver?	Yes ☐ No ☐
14	How the authenticity of origin is ensured—e.g., is the signature of the exchange message tested?	
	▪ What is the reaction of the device if an authenticity test fails?	
	▪ Which effective key length(s) is/are utilized for all the cryptographic algorithm(s) in question?	
	▪ Is the chosen key length appropriate for the algorithm and its protection purpose?	Yes ☐ No ☐
	▪ In case RSA is used, is the key length at least 2048 bit?	Yes ☐ No ☐

K18, continued

15	The hashing algorithm(s) that are used.
	The purpose of the usage(s).
16	Whether single component keys can be loaded and the algorithm used to encrypt them during key entry.
17	All storage and usage locations for each key ever present in or used by the device.
18	Each combination of key-exchange technique and key-storage mechanism supported by the device (e.g., ANSI TR-31).
19	Whether the device uses any key-derivation method. Yes ☐ No ☐
	If so, describe the method.
20	Whether any keys are calculated as a variant of another key. Yes ☐ No ☐
	If so, describe how the variant(s) are protected at an equivalent or greater level of security as the original key(s).

Comments:

Section K19

If the answer to K19 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The characteristics that prevent or significantly deter the use of a stolen device for exhaustive PAN determination.

Comments:

Section K20

If the answer to K20 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the relevant device components permit access to internal areas for maintenance or service. Yes ☐ No ☐
2	If the answer to 1 above is "YES," how access to sensitive data such as account or cryptographic data is prevented by the design of the internal areas.
3	If the answer to 1 above is "YES," the mechanism that causes immediate erasure of account and cryptographic data.
4	How the mechanism is triggered.
5	What data is erased?
6	The erasure method.

Comments:

Section K21

If the answer to K21 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The operational and environmental conditions for which the device was designed.
2	Why the security of the device is not compromised by operational and environmental conditions.
3	The tests performed to ensure the security on the changing operational and environmental conditions. (Provide test reports.)
4	Why the measures are sufficient and effective.

Comments:

Section K22

If the answer to K22 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Whether the device supports multiple applications. Yes ☐ No ☐
	If yes, provide a list of these applications, and identify those with security impact.
	If yes, how is the separation between applications with security impact from those without security impact enforced?
2	For each security-relevant application, list by groups the data objects and their location.
3	Which mechanism prevents applications from accessing data objects not belonging to it.

Comments:

Section K23

If the answer to K23 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The method to ensure that the operating system contains only the components and the services necessary for the intended operation.
2	The procedures used for maintenance and updates of the operating system.
3	The rationale for why the method used to enforce least privilege is effective.
4	The rationale for why all the components and services listed in the configuration list are necessary.
5	Describe the security policy enforced by the device to not allow unauthorized or unnecessary functions.
6	The rationale for why it is infeasible to remove API functionality and commands that are not necessary to support specific functionality.

Comments:

Section K24

If the answer to K24 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The sensitive functions provided by the device. *Sensitive functions are functions that are not intended to be accessed by end users (cardholders and merchants) that can impact the security of the device. Examples are key loading or the definition and maintenance of user roles.*
2	How the device controls the access and use of sensitive functions.
3	The authentication method used to access sensitive services.
4	The measures that ensure that entering or exiting sensitive services does not reveal or otherwise affect sensitive information.
5	The interface used to authenticate access to sensitive services.
6	Whether an external device is used to authenticate access to sensitive services.
7	How the authentication data used to access sensitive services in the device is protected, as it is input/output via the interface.
8	Which of the following is true for the data referred to in 7 above: ☐ Data inputs cannot be discerned from any displayed characters. ☐ Data inputs cannot be discerned by monitoring audible or electro-magnetic emissions. ☐ Sensitive data is cleared from internal buffers upon exiting a secure mode.

K24, continued

9	The management of any data used for authentication. *Examples of authentication data are passwords, cryptographic keys, and hardware tokens*. Include:	
	▪ The number of devices that share the same keys or passwords	
	▪ Cryptographic algorithms used for authentication, if applicable	
	▪ Data size (key or password length)	
	▪ How authentication data is distributed to legitimate users	
	▪ How authentication data can be updated	
10	The device's response to false authentication data.	

Comments:

Section K25

If the answer to K25 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	What is the limit on the number of actions that can be performed when using sensitive functions?
2	The rationale for the limit that was chosen.
3	How the chosen limit on the number of actions minimizes the risks from unauthorized use of sensitive services.
4	The device's response once the limit on the number of actions has been reached.
5	The maximum time the device may remain inactive once it has accessed sensitive functions.
6	The action taken by the device once the maximum time for inactivity has been reached.
7	The maximum time before the device returns to normal mode after initially accessing sensitive functions.
8	The action take by the device once the maximum time is reached.

Comments:

Device Diagrams (Optional)

If you wish to include diagrams or other illustrations in support of the relevant device's functionality, please insert them here.