Payment Card Industry (PCI)

PIN Transaction Security (PTS) Point of Interaction (POI)

Modular Evaluation Vendor Questionnaire

Version 4.0

June 2013

Document Changes

Date	Version	Description
April 2010	3.0	Initial public release
September 2011	3.1	Clarifications and errata, updates for Non-PIN POIs
February 2013	4.x	RFC version
June 2013	4.0	Initial public release

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
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ANSI TR-31
Integrated Circuit Card Specification for Payment Systems – Book 2: Security and Key Management, Version 4.3, November 2011	EMV 4.3
Identification Cards – Integrated Circuit Cards	ISO 7816
Personal Identification Number (PIN) Management and Security	ISO 9564
Banking – Key Management (Retail)	ISO 11568
Banking – Secure Cryptographic Devices (Retail)	ISO 13491
Financial services -- Requirements for message authentication using symmetric techniques	ISO 16609
Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers	ISO/IEC 18033-3
Guidelines on Triple DES Modes of Operation.	ISO TR 19038
Guideline for Implementing Cryptography In the Federal Government	NIST SP 800-21
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	NIST SP 800-22
Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	NIST SP 800-67
PCI DSS v2.0	PCI SSC
PCI DSS Wireless Guidelines	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* ↑

A – Core Physical Security Characteristics

Section A1

If the answer to A1 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, including 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, other protection methods that exist to prevent access to sensitive information, or bug insertion.
5	The mechanisms protecting against physical penetration of the device.
6	Why the device implementation is such it is not feasible to penetrate and alter the device to disclose sensitive information or to insert a PIN-disclosing bug without requiring an attack potential of at least 26, with a minimum of 13 for exploitation.
7	The secrets that are erased upon tampering 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, by information on the display or a broken security seal visible to the eye, or otherwise, when the terminal is in regular use.

Section A1 (continued)

10	How the device is constructed, by attaching in Annex B at the end of the Questionnaire an exploded diagram of the device showing how all sub-components are assembled and connected internally.
11	How cardholder PIN entry mechanism(s) are implemented (if applicable), including the path taken by the signals that connect the PIN entry mechanisms to the security processor, and any components (including passive components), connectors, or other items connected to the path.
12	For each PCB that carries customer PIN signals, what tamper-detection mechanisms protect these signals from being accessed.
13	Any volume-encapsulation methods used by the device that are designed to make penetration or reverse engineering difficult.
14	Any methods such as soldering, elastomeric strips or adhesives, plastic/metal walls, or others, that are used as part of the security features of the device.
15	How the security processor drives tamper-detection features.
16	Via attachment of a schematic diagram in Annex B at the end of the Questionnaire, the connections to all tamper-detection features, including switches and tamper grids of all device tamper circuits.
17	How passive components, connectors, or other items that carry tamper signals are protected against access.
18	How the device (if used for PIN entry) is protected against placement of an external overlay—i.e., a secondary keypad on top of the existing keypad.
19	How the device (if used for PIN entry) is protected against placement of an internal overlay between the keypad buttons and the keypad footings.

Section A1 (continued)

20	How the device is protected from: ▪ Each side of the device ▪ The back of the device ▪ The front of the device

Comments:

Section A2

If the answer to A2 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 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	The temperature ranges for all components included in the tamper-detection circuits. This shall include mechanical switches and active elements (but not passive elements such as resistors and capacitors).
3	Any glitch detection or prevention features used.
4	Why the security of the device is not compromised by operational and environmental conditions.
5	The tests performed to ensure the security on the changing operational and environmental conditions. Provide test reports, for example by including this information in Annex B at the end of the Questionnaire.
6	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, including both long term and temporary storage locations, and any external memory used.	
3	How sensitive information and functions dealing with sensitive information are protected from modification.	
4	Why the measures are sufficient and effective that it is not feasible to modify sensitive information or functions dealing with sensitive information without requiring 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.	
7	Whether signatures are used as a protection method. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ The algorithms and key lengths used for the signatures.	
	▪ Any padding schemes used for the signatures, and how this prevents padding oracle attacks.	
	▪ How modification of the sensitive information is prevented after signature validation	

Section A4 (continued)

8	Whether physical protections are used as a protection method (for example when plaintext information exists in external memory. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ Whether the physical protections cover all memory traces, vias, passive elements, or other areas of access.	
	▪ How the memory packages are protected, including access to BGA balls and traces on internal chip carriers of packages.	
9	Whether encryption is used as a protection method. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ The algorithms and key lengths used.	
	▪ What modes of operation are used for the encryption.	
	▪ How this prevents the re-location of memory from one area to another.	
	▪ How the method of encryption prevents the exposure of sensitive information through building of a "dictionary" (i.e., look-up table) of possible encrypted values.	
	▪ If a key stream mode of encryption is used (e.g. OFB), how the encryption of different data with the same key is prevented.	
10	For each integrated circuit element that may be programmed or configured in some way:	
	▪ The different ways in which the element may be programmed or configured	
	▪ Any in-circuit testing or debugging features provided by these elements	
	▪ The methods implemented to disable the programming/testing features	
11	Whether applications and/or firmware are executed on the same processor that stores or operates on plaintext passwords, PINs, or public keys. Yes ☐ No ☐ If **"YES,"** describe:	
	What mechanisms are implemented to prevent these applications from modifying this information.	

Comments:

Section A5

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

1	The device protections that guard against PIN digits being determined by monitoring sounds emitted when any key is pressed (this does not refer to audible tones addressed in Section A12).
2	The device's protections against monitoring electro-magnetic emissions.
3	Any electro-magnetic emissions testing that has been performed. Provide data and results for the tests performed, for example by placing this information in Annex B at the end of the Questionnaire.
4	The device's protections against monitoring power consumption. Provide data for tests performed.
5	Any other external characteristics considered. If applicable, provide data and results for the tests performed, for example by placing this information in Annex B at the end of the Questionnaire.
6	Why it is not feasible to determine the entered PIN by monitoring sound, electro-magnetic emissions, or power consumption without requiring an attack potential of at least 26, with a minimum of 13 for exploitation.

Comments:

Section A6

If the answer to A6 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 different cryptographic operations implemented with the device, whether they are implemented in software and/or hardware, and what side-channel analysis protections are implemented for each.
3	The protections the cryptographic processing elements implement to protect against attacks to force cryptographic errors, such as glitch attacks, and to protect against chip-level attacks to extract the cryptographic keys.
4	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components' design.
5	Whether the device includes any tamper-detection and response mechanisms in these components. Yes ☐ No ☐
	If **"YES,"** provide responses to Section A1.
6	Whether the device includes any tamper-resistance mechanisms in these components. Yes ☐ No ☐
	If **"YES,"** provide responses to Section A1.
7	Why the device implementation is such that it is not feasible to determine 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)—without requiring an attack cost potential of at least 35, with a minimum of 15 for exploitation.
8	Why the programming or in-circuit testing features of the processing elements of the POI cannot be re-enabled (either temporarily or permanently).

9	Any assistance and/or materials that will be provided to the evaluating test house to facilitate robust and efficient testing.

Comments:

Section A7

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

1	What are the protections against the alteration of prompts for non-PIN data? This includes access to the display itself as well the path from the display to the controlling processing element.
2	What is the response of the device to an attempt to alter prompts for non-PIN data?
3	Where prompts for non-PIN data entry are stored within the device and the protections implemented for those prompts.
4	Why it is not feasible to conduct unauthorized alteration of prompts for non-PIN data entry into the device such that PINs are compromised, without requiring an attack potential of at least 18 per device with a minimum of 9 for initial exploitation.

Comments:

Section A8

If the answer to A8 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.
3	Via attachment of the user (acquirer/merchant) instructions, the implementation criteria. Where visual observation deterrence is not an integral part of the device, include drawings and descriptions to illustrate how visual observation is deterred.

Comments:

Section A9

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

1	The mechanisms, including any necessary APIs, used by the device to capture data from magnetic-stripe payment cards.
2	The mechanisms used to prevent skimming attacks against the device. If logical (e.g., encryption) protections are used describe: ▪ The integrated circuit used to provide the encryption and any physical protections provided ▪ The algorithm, mode of operation, and key management used ▪ How the cryptographic keys are loaded and, if keys can be updated, how this occurs ▪ The method used to generate these keys and how this achieves unique key(s) per device
3	Describe any physical protections that are implemented to protect the path from the read head to the security processor, including all intervening elements.
4	The mechanisms ensuring 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.
5	If the mechanism causes the device to be locked as part of the action taken, describe how the unlocking takes place.
6	Why 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 without requiring an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation.

Comments:

Section A10

If the answer to A10 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, including how dual control is enforced.
6	If cryptographic mechanisms are used, how replay and man-in-the-middle attacks are prevented.
7	If passwords or other secret data are used for the mechanism, describe the initialization and use.
8	Why the component implementation is such that it is not feasible to disable the tamper mechanisms without requiring an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation.

Comments:

Section A11

If the answer to A11 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:

B – 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, including validation of any register settings relied upon for the security of the device.
3	How initial machine code is loaded and executed by the processing elements, and how any subsequent firmware modules are loaded and executed, up to and including software modules used for PIN entry functions.
4	The algorithms and key sizes used to perform self-test functions, and how the keying material integrity is maintained subsequent to loading.
5	Any self-test functions implemented by the built-in functions of the security processing elements and what sources of information and testing have been used to validate that these processes are in place.
6	The response of the device to a self-test failure for each type of component.
7	The types of events that initiate self-tests for each type of test.
8	The types of events that initiate a device reset, including elapsed time.

Comments:

Section B2

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

1	All logical and physical interfaces provided by the POI and how each of the above interfaces is configured to accept commands.
2	The languages the device's source code is written in and the type and configuration of the operating system(s) used for each of the security processing elements.
3	All command interpreters within the software, including but not limited to SQL commands and OS commands.
4	Which commands are accepted by the affected device components.
5	How the commands are linked to the device modes.
6	What type of parameter- and data-checking is performed.
7	Why the functionality is not influenced by logical anomalies.
8	Any tests that have been performed to ensure the functionality is not influenced by logical anomalies. Provide a rationale explaining why the test coverage is sufficient.
9	How sensitive information or the PIN is prevented from being outputted in clear-text.
10	Whether the POI is designed to allow for non-firmware applications to be executed, and what firmware functions on which such non-firmware applications would execute (e.g., PIN processing, cryptographic key operations, prompt control, etc.) are provided by the processor.

Comments:

Section B3

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

1	The documented software-development process that details how firmware must be written, reviewed, and tested to ensure the software is free from security vulnerabilities.
2	The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.
3	The compiler settings used in order to maximize the mitigation of known vulnerabilities.
4	Any mitigation techniques such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Harvard architecture and stack canaries used to help prevent common exploits, including how the test lab may place reliance upon these techniques in connection with B2 and other relevant requirements.

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 methods used for initial firmware loading and, if different, the methods used for updates.
3	The mechanisms used and the device components affected by the firmware/software update.
4	What cryptographic algorithms and key sizes are used for firmware/software authentication.
5	How any public or private secret keys are loaded into the device during manufacturing.
6	The device's response when firmware/software to be updated cannot be authenticated.
7	How the firmware/software is deleted if rejected.

Comments:

Section B4.1

If the answer to B4.1 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	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.
7	The cryptographic algorithms and key sizes used for software application/configuration authentication.
8	The device's response if software application/configuration to be updated cannot be authenticated.
9	How the software application/configuration update 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 and through which interfaces.
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 device 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 plaintext form in any location after encryption.
3	The maximum time a plaintext 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 item 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 descriptions of the following:	
	▪ 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.	
11	All methods used to load cryptographic keys into device.	

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 taken 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, including any seed values used, hardware systems, and software-based, deterministic pseudo random number generators (DPRNG).	
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.	
4	The random number generator used by any open protocols used by the device.	
	Protocol Name	Reference

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	The process used for erasure.	
10	The circumstances under which keys are erased. Describe this 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 keys and whether the keys are loaded encrypted, or in plaintext, or as encrypted or plaintext 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 regarding this key-distribution technique:	
	▪ The technique 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 ☐

B11, continued

15	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 ☐
	▪ If RSA is used, is the key length at least 2048 bit?	Yes ☐ No ☐
16	The hashing algorithm(s) that are used.	
	The purpose of their usage(s).	
17	Whether single component keys can be loaded and the algorithm used to encrypt them during key entry.	
18	All storage and usage locations for each key ever present in, or used by, the device.	
19	Each combination of key-exchange technique and key-storage mechanism supported by the device (e.g., ANSI TR-31).	
20	How keys stored or used by the device are generated.	
21	Whether the device uses any key-derivation method. Yes ☐ No ☐	
	If **"YES,"** describe the method.	
22	Whether any keys are calculated as a variant of another key. Yes ☐ No ☐	
	If **"YES,"** 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.
3	All methods that the POI supports for external PIN transfer to other network nodes or devices or other subcomponents outside the area validated to requirement A1.

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 plaintext PIN data is distinguished from any other data that might be entered into a device.
3	Whether the device supports data decryption, and what methods are implemented to prevent the use of this function to decrypt PINs.
4	How encrypted PIN data is distinguished from all other data encrypted or plaintext.
5	All key-encrypting keys.
6	What data can be encrypted using key-encrypting keys.
7	How this data is distinguished from all other data.
8	How encrypted keys are distinguished from all other data.
9	How the device enforces that data keys, key-encipherment keys, and PIN-encipherment keys have different values—specifically, that no one key can take the same value as any other key within the POI.

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 plaintext secret or private cryptographic keys or plaintext PINs or other sensitive data. Yes ☐ No ☐
	If **"YES,"** describe the mechanism.
2	How the outputting of plaintext keys and plaintext PINs is prevented.
3	In what locations within the device cryptographic keys may exist in plaintext.
4	Under what circumstances a plaintext 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 are 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 entry are separate operations.

Comments:

Section B16

If the answer to B16 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 implemented cryptographic algorithms/mechanisms/protocols that protect the control of the device's display and device usage.
4	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.
5	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.
6	Which effective key length(s) is/are utilized for all the cryptographic algorithm(s) implemented.
	Is the chosen key length appropriate for the algorithm and its protection purpose? Yes ☐ No ☐
	If **"YES,"** state why this is the case.

Section B16 (continued)

7	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.
8	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.
	▪ Describe how the separation between applications with security impact from those without security impacts is enforced.
2	For each security relevant application, list by groups the data objects and their location.
3	What mechanisms exist within the POI that allow for the execution of non-ROM based configuration or program data (e.g., processors, micro-controllers, FPGAs, etc.).
4	Whether the device relies upon the use of different processors to provide for the separation between the firmware and any applications and, if so, the method of communications provided between these processors, including any physical interface and API(s).
5	Which mechanism(s) ensure that code and data objects of different applications/firmware are kept separate.
6	The mechanisms provided to prevent the execution of memory used to hold data objects.

Comments:

Section B18

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

1	Whether the device implements a commercial operating system, custom operating system, function executive, or other mechanism. If the device uses a commercial operating system, note the name and version of this system.
2	The method to ensure that the operating system contains only the components and the services necessary for the intended operation.
3	The procedures used for maintenance and updates of the operating system.
4	The rationale for why the method used to enforce least privilege is effective.
5	The rationale for why all the components and services listed in the configuration list are necessary.
6	The API functionality and commands that exist and are identified as either required to support specific functionality or disabled/removed.

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:

Section B20

If the answer to B20 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How changes to the security policy document are controlled.
2	How the device is configured to comply with the security policy.

Comments:

C – Online Security Characteristics

Section C1

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

1	Whether:	
	▪ The device provides for a single master key for all hierarchies into which a PIN key may be loaded,	Yes ☐ No ☐
	▪ This master key is the only key which can be loaded into the POI in plain text, and	Yes ☐ No ☐
	▪ The device provides for only one PIN key.	Yes ☐ No ☐
	If the answers to each of the above are **"YES,"** the rest of this section is N/A.	
2	Any means available to a cardholder or merchant to issue commands that result in the selection of keys by the device (for example, buttons that can be pressed to select between acquirers).	
3	How the device prohibits unauthorized key replacement and key misuse.	
4	Whether the device supports multiple key hierarchies. Yes ☐ No ☐	
	If **"YES,"** describe how the device authenticates key selection or uses commands for the PIN key or any PIN KEKs and implements dual control or cryptographic mechanisms to do so.	

Comments:

D – Offline Security Characteristics

Section D1

If the answer to D1 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.

Section D1 (continued)

10	The rationale as to why the ICC reader prevents or otherwise detects 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 the successful implant of a sensitive-data-disclosing bug aiming at capturing offline PIN and IC card information.
12	Whether the device implements any active detection mechanisms that the ICC acceptor utilizes to prevent a “shim” from being left in the slot. Yes ☐ No ☐
13	If the answer to 12 above is “YES,” describe:
	▪ The protections used to prevent penetration of the device for the purpose of determining or modifying sensitive data.
	▪ For each PCB that carries the customer ICC I/O signal, the tamper-detection mechanisms to protect these signals from being accessed (such as tamper grids).
	▪ The specialized skills and equipment that would be necessary to penetrate the device in order to determine or modify sensitive data.
16	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	How the construction of the device is such that the entire slot opening is in full view of the cardholder prior to card insertion such that any objects within the slot would be clearly visible.

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 **"YES,"** 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 plaintext methods of ICC user authentication. Yes ☐ No ☐
2	How the PIN is enciphered between the devices and the PIN block format(s) used, 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 plaintext PIN (or PIN block) may transit outside of the device encrypting the PIN or ICC reader.

Comments:

E – 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	Why the implementation is such that it is not feasible to place an overlay with a PIN-disclosing bug without requiring 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	Why it is not feasible to alter the correspondence between the display messages and the operating state without requiring 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	Why the implementation is such that it is not feasible to disable the tamper mechanisms without requiring 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:

F–J – 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

F – Discovery

Section F1

If the answer to F1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	All logical and physical interfaces that use a public domain protocol.	
	Interface Name	Reference
2	Each protocol and service available for each of the listed interfaces above	
	Protocol Name	Reference
3	How each of the above interfaces is configured to accept commands	
4	For each of the above interfaces which component implements the protocol, if it is a security protocol, and the location from which the software was derived.	

Comments:

G – Vulnerability Assessment

Section G1

If the answer to G1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The reference and provided documentation for the vendor vulnerability procedures.
2	The vendor's procedures for detection of vulnerabilities in all interfaces.
3	How the vendor's vulnerability-assessment procedures outline the process for classification and detection of vulnerabilities and include a correct description, a level of criticality, and mitigation measures.
4	The vendor's procedures for on-going, timely detection of new vulnerabilities and verify that the process creates an auditable record.

Comments:

Section G2

If the answer to G2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The reference and documentation for all the protocols and services available on the platform.
2	How the vulnerability assessment of all the protocols and services was executed, and why this leads to the assertion that they do not contain exploitable vulnerabilities.
3	The vulnerability-assessment documentation, vulnerability-survey evidence, and test evidence.

Comments:

Section G3

If the answer to G3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The referenced and provided documentation for the vulnerability disclosure measures, supporting the response to G3 of the *PCI PTS POI Security Requirements.*
2	The vendor's timely creation of mitigation measures for newly found vulnerabilities and that procedures exist to continually update and document all vulnerabilities.

Comments:

H – Vendor Guidance

Section H1

If the answer to H1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The referenced and provided vendor security guidance for how each logical and physical interface must be securely used.
2	The referenced and provided vendor security guidance for how each protocol and service must be securely used.

Comments:

Section H2

If the answer to H2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The referenced and provided vendor security guidance for the default configuration for each logical and physical interface.

Comments:

Section H3

If the answer to H3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The referenced and provided vendor security guidance for how keys and certificates must be used.

Comments:

I – Operational Testing

Section I1

If the answer to I1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The public domain security protocols supporting the response to I1 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section I2

If the answer to I2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The encryption mechanism of the security protocol used to provide data confidentiality supporting the response to I2 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section I3

If the answer to I3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanism of the security protocol used to provide data integrity supporting the response to I3 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section I4

If the answer to I4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanism of the security protocol used to provide server authentication supporting the response to I4 in the PCI PTS POI Security Requirements.	
	Protocol Name	Reference

Comments:

Section I5

If the answer to I5 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	Reference and provide documentation describing the mechanism of the security protocol, used to provide exception handling and replay detection supporting the response to I5 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference

Comments:

Section I7

If the answer to I7 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The mechanism of the security protocol, used to provide session management supporting the response to I7 in the *PCI PTS POI Security Requirements.*	
	Protocol Name	Reference
2	The device's session-management features to ensure that connections are not left open for longer than necessary.	
3	The device's session-management features to ensure that the device limits the amount of concurrent connections that the device can maintain.	

Comments:

J – Maintenance

Section J1

If the answer to J1 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The vendor's procedures for configuration management.

Comments:

Section J2

If the answer to J2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The vendor's maintenance procedures.

Comments:

Section J3

If the answer to J3 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The vendor's update procedures including both software and firmware updates.

Comments:

Section J4

If the answer to J4 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	The vendor's authentication and security procedures including both configuration and software updates. Describe the mechanism for confidentiality, integrity, server authentication and protection against replay.
2	The procedure if the authenticity is not confirmed.

Comments:

K – 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 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 detects the successful implant of a sensitive-data-disclosing bug aiming at capturing offline PIN and IC card information

Section K1.1 (continued)

For ICC-Based Entry (continued)

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.
12	Whether the device implements any active detection mechanisms that the ICC acceptor utilizes to prevent a “shim” from being left in the slot. Yes ☐ No ☐ If **“YES,”** describe:
13	The protections used to prevent penetration of the device for the purpose of determining or modifying account data.
14	For each PCB that carries the customer ICC I/O signal, the tamper-detection mechanisms (such as tamper grids) to preclude these signals from being accessed.
15	The specialized skills and equipment that would be necessary to penetrate the device in order to determine or modify account data.
16	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:

Section K1.1 (continued)

For Magnetic-Stripe Entry

1	The mechanisms used by the device to capture data from magnetic-stripe payment cards, including any necessary APIs.
2	The mechanisms used to prevent skimming attacks against the device. If logical (e.g., encryption) protections are used, describe: ▪ The integrated circuit used to provide the encryption and any physical protections provided ▪ The algorithm, mode of operation, and key management used ▪ How the cryptographic keys are loaded and, if keys can be updated, how this occurs ▪ The method used to generate these keys and how this achieves a unique key(s) per device Describe any physical protections that are implemented to protect the path from the read head to the security processor, including all intervening elements.
3	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.
4	If the mechanism causes the device to be locked as part of the action taken, describe how the unlocking takes place.
5	Why 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 without requiring 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:

For Contactless

1	The mechanisms used to protect the path for contactless data from the point of digitization of the 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	Why the device implementation is such that it is not feasible to penetrate and alter 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 K1.2

If the answer to K1.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

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 to 4 above is **"YES,"** how access to account data is prevented by the design of the internal areas.
6	If the answer to 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 different cryptographic operations implemented with the device, whether they are implemented in software and hardware, and what side-channel analysis protections are implemented for each.
3	The protections the cryptographic processing elements implement to protect against glitch attacks to force cryptographic errors and to protect against chip-level attacks to extract the cryptographic keys.
4	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components' design.
5	Whether the device includes any tamper-detection and response mechanisms in these components. Yes ☐ No ☐
	If **"YES,"** provide responses to Section K1.1.
6	Whether the device includes any tamper-resistance mechanisms in these components. Yes ☐ No ☐
	If **"YES,"** provide responses to Section K1.1.
7	Why the device implementation is such that it is not feasible to determine 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)—without requiring an attack cost 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	Why the device implementation is such that it is not feasible to modify any public key resident in the device and used for account data protection purposes without requiring 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 plaintext 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 plaintext data.
4	All account data key-encrypting keys.
5	The account data that 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—specifically, that no one key can take the same value as any other key within the POI.

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 software development process that details how firmware must be written, reviewed and tested to ensure the software is free from security vulnerabilities. •
2	The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.
3	The compiler settings used in order to maximize the mitigation of known vulnerabilities.
4	Any mitigation techniques such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Harvard architecture and stack canaries used to help prevent common exploits, including how the test lab may place reliance upon these techniques in connection with B2 and other relevant requirements.

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.
7	The cryptographic algorithms and key sizes are used for software application/configuration authentication.
8	The device's response if software application/configuration to be updated cannot be authenticated.
9	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	The components of the device that allow updates of firmware and/or software.
2	The methods used for initial firmware loading, and if different, the methods used for updates.
2	The mechanisms used and the device components affected by the firmware/software update.
4	The cryptographic algorithms and key sizes used for firmware/software authentication.
5	How any public or private secret keys are loaded into the device during manufacturing.
6	The device's response if firmware/software to be updated cannot be authenticated.
7	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	All logical and physical interfaces provided by the POI and how each of the above interfaces is configured to accept commands.
2	The languages the device's source code is written in and the type and configuration of the operating system(s) used for each of the security processing elements.
3	All command interpreters within the software, including but not limited to SQL commands and OS commands.
4	Which commands are accepted by the affected device components?
5	How the commands are linked to the device modes.
6	What type of parameter- and data-checking is performed.
7	Why the functionality is not influenced by logical anomalies.
8	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.
9	How account data is prevented from being outputted in clear-text.

Section K13, continued

10	Whether the POI is designed to allow for non-firmware applications to be executed. Yes ☐ No ☐
	The firmware functions provided by the processor on which such non-firmware applications would execute (e.g. PIN processing, cryptographic key operations, prompt control, etc.)

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 F, G, H, I 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	Whether there is are mechanism(s) that will allow the outputting of plaintext 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 plaintext 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 K15.1

If the answer to K15.1 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 K15.2

If the answer to K15.2 in the *PCI PTS POI Security Requirements* was "YES," describe:

1	How it is ensured that the account data does not remain in plaintext form in any location after encryption.
2	The maximum time a plaintext 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 K16

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 K16.1

If the answer to K16.1 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 K16.2

If the answer to K16.2 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 K17

If the answer to K17 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 this is 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	The keys that may be erased.	
9	The process used for erasure.	
10	The circumstances under which keys are erased. Describe for all device states (power-on, power-off, sleep mode).	

K17, continued

11	Other data that is erased.	
	The circumstances under which other data is erased.	
12	The keys that 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 plaintext or as encrypted or plaintext 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 ☐
15	How the authenticity of origin is ensured—e.g., is the signature of the exchange message tested?	
	▪ The reaction of the device if an authenticity test fails.	
	▪ The effective key length(s) utilized for all the cryptographic algorithm(s) in question.	
	▪ Whether the chosen key length is appropriate for the algorithm and its protection purpose.	Yes ☐ No ☐
	▪ In case RSA is used, whether the key length is at least 2048 bit.	Yes ☐ No ☐

K17, continued

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

Comments:

Section K18

If the answer to K18 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 K19

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

1	The operational and environmental conditions for which the device was designed.
2	The temperature ranges for all components included in the tamper-detection circuits.
3	Any glitch-detection or prevention features used.
4	Why the security of the device is not compromised by operational and environmental conditions.
5	The tests performed to ensure the security on the changing operational and environmental conditions. Provide test reports, for example by placing this information in Annex B at the end of the Questionnaire.
6	Why the measures are sufficient and effective.

Comments:

Section K20

If the answer to K20 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.
	▪ Describe how the separation between applications with security impact from those without security impact is enforced.
2	For each security-relevant application, list by groups the data objects and their location.
3	What mechanisms exist within the POI that allow for the execution of non-ROM based configuration or program data (e.g., processors, micro-controllers, FPGAs, etc.).
4	Whether the device relies upon the use of different processors to provide for the separation between the firmware and any applications. Yes ☐ No ☐
	If **"YES,"** describe the method of communications provided between these processors, including any physical interface and API(s).
5	Which mechanisms ensure that code and data objects of different applications/firmware are kept separate.
6	The mechanisms provided to prevent the execution of memory used to hold data objects.

Comments:

Section K21

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

1	Whether the device implements a commercial operating system, custom operating system, function executive, or other mechanism. Yes ☐ No ☐
	If the device uses a commercial operating system, note the name and version of this system.
2	The method to ensure that the operating system contains only the components and the services necessary for the intended operation.
3	The procedures used for maintenance and updates of the operating system.
4	The rationale for why the method used to enforce least privilege is effective.
5	The rationale for why all the components and services listed in the configuration list are necessary.
6	Describe the security policy enforced by the device to not allow unauthorized or unnecessary functions.
7	The rationale for why it is infeasible to remove API functionality and commands that are not necessary to support specific functionality.

Comments:

Section K22

If the answer to K22 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.

K22, 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.	
11	All methods used to load cryptographic keys into device.	

Comments:

Section K23

If the answer to K23 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 taken by the device once the maximum time is reached.

Comments:

Annex A: DTR Templates

DTR TA1.7

Enumerate each of the circuit boards indicated in the POI in the table below, providing, at a minimum:

PCB Designator	PCB Version	PCB purpose	Picture reference	Sensitive signals	Tamper-Detection Mechanisms

DTR TA1.10

Using vendor documentation for each tamper grid that is implemented, complete the details indicated in the table below, describing, at a minimum:

Tamper Grid Location	Physical Implementation	Size of Traces and Distance between Traces, Signals, or Layers	Number of Tamper-detecting Signals	Method of Connection	Adjacent Signals?

DTR TA1.10

For each tamper switch used in the POI, complete the details indicated in the table below, at a minimum.

Switch Location	Number Used in that Location	Physical Implementation	Size of Switch Contacts	Conductive Ink Protections	Additional Comments

DTR A3.5

Use the table below to detail the environmental protection features implemented by the POI.

	Maximum Value	Minimum Value	Detecting Circuitry	Response
Voltage (Specify type)	Configured Value	Configured Value		
	Tested Value	Tested Value		
Temperature	Configured Value	Configured Value		
	Tested Value	Tested Value		

DTR TA4.4

In the following table, outline the locations of all types of sensitive information and functions, adding to those provided where other types of sensitive information exist within the POI.

Sensitive Information	Storage area	Method of protection
Plaintext PINs		
Passwords		
POI Firmware		
Public keys		

DTR TA8.9

Enter details of the POI into the table below.

Dimension	*Device Measurement*	*Maximum for classification as handheld*
The width at the “5” key		7.62 cm
The height at the “5” key The sum of the width and the height at the “5” key		— 10.16 cm
The keypad length, from the bottom of the “0” key to the top of the “2” key		10.16 cm
The weight of the POI		500grams

DTR TA8.11

If the device provides a privacy shield, complete the table below with angles of observation to the center of the "5" key.

Angle of POI	Angle of observation to "5" key	Minimum angle required by Annex A1.1	Minimum angle required by Annex A1.2
0			
45			
90			
135			
180			
225			
270			
315			

DTR TB1.11

Complete the following table indicating the process used to authenticate the firmware images during each stage of the booting process.

Boot stage	Algorithms and Key Sizes Used for Authentication	Area/Code/Registers Authenticated	Method and Frequency of Re-authentication	Action Performed if Failed

DTRs TB4.8 and TB4.1.8

Complete the following table for each of the processing elements listed in DTR A4.

Processing/ Firmware Element	Elements Used to Perform Authentication	Algorithms and Key Sizes Used for Firmware Authentication	Format of Authentication Block	Process Performed if Authentication Failed

DTR TD.1.16

Where not previously covered in Requirement A1, for each tamper grid that is relied upon for security of the customer ICC I/O signal, complete the table below

Tamper Grid Location	Physical Implementation	Size of Traces and Distance between Traces, Signals, or Layers	Number of Tamper-detecting Signals	Method of Connection	Adjacent Signals?

DTR TF1.4

Complete a table describing all protocols, which component implements the protocol, if it is a security protocol and the location where the software was derived from. Include all exempted protocols and note why they have been exempted from OP requirements. Describe the security protocol implemented for confidentially, integrity, and authenticity.

Protocol Name	Component Handling the Protocol	Source Code Base and Version	Security Protocol	If not in OP scope, why?
IP (General)	Security Processor	Linux (3.7.1)		
TLS	Security Processor	OpenSSL (1.0.1c)		
GPRS	GPRS Modem	Modem vendor		Modem uses a separate processor, which is logically and physically segmented from the security processor.
IP (GPRS)	GPRS Modem	Modem vendor		Modem uses a separate processor, which is logically and physically segmented from the security processor.

Protocol Name	Component Handling the Protocol	Source Code Base and Version	Security Protocol	If not in OP scope, why?

DTRs K11.1.8 and K12.8

Complete the following table for each of the processing elements listed in DTR A4. .

Processing/ Firmware Element	Elements Used to Perform Authentication	Algorithms and Key Sizes Used for Firmware Authentication	Format of Authentication Block	Process Performed if Authentication Failed

DTR K19.5

Use the table below to detail the environmental-protection features implemented by the POI.

	Maximum Value	Minimum Value	Detecting Circuitry	Response
Voltage (Specify type)	Configured Value	Configured Value		
	Tested Value	Tested Value		
Temperature	Configured Value	Configured Value		
	Tested Value	Tested Value		

Annex B: Device Diagrams and Test Reports

(Mandatory where specified in the preceding questions; optional for additional information)

Required Diagrams and Reports

If any of the Sections noted below were completed within the Questionnaire, attach requested diagrams or reports, as appropriate, in the areas designated below.

Section A1, Question 10:

Section A1, Question 16:

Section A3, Question 5:

Section A5, Question 3:

Section A5, Question 5:

Section K19, Question 5:

Optional Diagrams or Illustrations

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