Cipherithm LLC

PCI PTS V3.x to V4.0 Gap Analysis, But WTF

A Cipherithm White Paper

Document Version 1.00

Publish date: September 1, 2013

DISCLAIMER

This publication is proprietary and confidential to Cipherithm LLC and may not be used for any purpose other than communicating said information for the benefit of Cipherithm LLC its vendors, customers and to further its business interests.

NOTICE

Cipherithm LLC reserves the right to make changes at any time and without notice. The information furnished by Cipherithm LLC in this publication is believed to be accurate and reliable; however, no responsibility is assumed by Cipherithm LLC for its use.

Contents

Revision Control

Version	Date	Editor	Change Description
1.00	Sept 1, 2013	SS	White paper release

Introduction

The purpose of this white paper is to provide a gap analysis between the newly published PCI PTS POI security requirements version 4 to the previous version 3.1. This gap analysis is done from the PED manufacturer's point of view.

This white paper is meant to be an easy to read comparison between PCI PTS version 3.1 and the newly published PCI PTS version 4. Each requirement is listed side by side with our analysis. If you have heard the reports that there are few security changes between the two versions then this white paper will be of interest to you, Despite the fact that the text of each of the security requirement is mostly unchanged, there are modest changes, additions guidance to the corresponding vendor questionnaire and derived test requirements (DTRs).

This white paper points out the number of additional questionnaire questions and documentation that must be provided by a secure vendor to the lab. In some cases, there are a significant number of new tests that the lab is required to review.

Feel free to submit comments, questions, and editorial suggests to info@cipheritm.com

Please note the details of the DTR gap is not provided in this publically available white paper because the DTRs are provided under NDA. If you are interested in the detailed DTR differences please contact Cipheritm.

If you are reading this you must be interested in PTS security requirement. You are expected to review the details that follow. If you give up on the details, be sure to read the summary at the end.

Considerations

For those vendors that have been told that the change from version 3.1 to version 4 is minor you should do a complete review of your version 3.x approved product against the PTS version 4 requirements, including the impact of the DTRs. There are some areas that we believe will required hardware design modifications for most devices. Keep in mind that increasing security on any given design is very difficult, in some cases not possible without significant changes to the electronics and mechanical design. Then the question of making changes to the current design or creation of a new product line needs to be addressed.

We remember when PCI version 1 was first announced to replace the Visa PED approval program. This predates the founding of the PCI SSC as we know it today. The initiative was driven by MasterCard and Visa, an attempt to align the PED security requirements. The vendors at the time applauded the coordination of the two brands that relied on PIN security. However, in the initial meeting it was announced that since there was no major changes to the requirements, that six months after the announcement, all new products would be tested under the PCI version 1 requirements. The first PCI approved product was listed about 14 months after the initial announcement. The reason is took so long is that the new details of the questionnaire and DTRs required new security product design to meet the new security standard. Since that time we have been a bit more skeptical when we hear from the brands and PCI that new security requirements are minor, which is why we have published this white paper.

Keep in mind that to obtain a PCI PTS approval a 100% compliance report is needed. Even the smallest non-compliance issue can sabotage a product approval.

This page was not intentionally left blank. Instead, Microsoft Word spacing left this page blank

Side by Side V3.1 / V4 Comparison

Evaluation Module 1: Core Requirements

A – Core Physical Security Requirements

Requirement Alignment Table

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Security Requirement		
A1.1 *The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader; and* *Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario.*	A1 *The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader; and* *Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours attack time for exploitation.*	The A requirement is no longer two parts, A1.1 and A1.2. The same requirements are now A1 and A2 respectively. The ten hour minimum for exploitation is finally included as a specific requirement. This has been a requirement for scoring the attack potential, but one would have to refer to the Technical FAQ.

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Evaluation Vendor Questionnaire Total Questions: 9 **Modular Derived Test Requirements** Total Tests: 6	Total Questions: 20	There are significant number questions that must be answered. Most are details of the design and require additional details be provided to the lab. There are two areas of concern based on PED designs. *Q18 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.* *Q20 How the device is protected from:* • *Each side of the device* • *The back of the device* • *The front of the device* Significant change identified
Modular Security Requirement **A1.2** *Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.* **Modular Evaluation Vendor Questionnaire** Total Questions: 4 **Modular Derived Test Requirements** Total Tests: 3	A2 *Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.* Total Questions: 4	A1.2 is now A2. There are no additional questions for this requirement. New guidance provided

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Security Requirement **A2** *If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose sensitive data. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of sensitive data.* **Modular Evaluation Vendor Questionnaire** Total Questions: 6 **Modular Derived Test Requirements** Total Tests: 8	 Total Questions: 0	This requirement was removed because it was redundant with other tests.
Modular Security Requirement **A3** *The security of the device is not compromised by altering:* • *Environmental conditions* • *Operational conditions* *(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)* **Modular Evaluation Vendor Questionnaire** Total Questions: 3 **Modular Derived Test Requirements** Total Tests: 4	 A3 *The security of the device is not compromised by altering:* • *Environmental conditions* • *Operational conditions* *(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)* Total Questions: 6 Total Tests: 10	 Additional questions concerning the temperature detection and “glitch” detection and prevention. New guidance provided

PCI PTS Version 3.1		PCI PTS Version 4		Notes
	Modular Security Requirement			
A4	*Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation*	A4	*Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 6		Total Questions: 11	Additional questions about the device design
	Modular Derived Test Requirements			
	Total Tests: 4			New guidance provided
	Modular Security Requirement			
A5	*If PIN entry is accompanied by audible tones, then the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit*	A11	*If PIN entry is accompanied by audible tones, the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit*	No reason given for moving this requirement.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 3		Total Questions: 3	
	Modular Derived Test Requirements			
	Total Tests: 3			Possible side channel
	Modular Security Requirement			
A6	*There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring—even with the cooperation of the device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation*	A5	*There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring—even with the cooperation of the device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 6		Total Questions: 6	Minor change to Q3 requiring more specific tests and results.

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Derived Test Requirements Total Tests: 5		 Identified as a possible red flag
Modular Security Requirement **A7** *Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation* **Modular Evaluation Vendor Questionnaire** Total Questions: 5 **Modular Derived Test Requirements** Total Tests: 3	A6 *Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation* Total Questions: 9	Additional information for the cryptographic processor is required for side channel attacks and how it is not possible to re-enable the programming and in-circuit testing features on a product device. New guidance provided

PCI PTS Version 3.1		PCI PTS Version 4		Notes
	Modular Security Requirement			
A8	***Note:*** *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A8, B16.1, B16.2, or E3.4.* *(Statements A8 and B16.1 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement B16.2 is an option that allows third parties to control the means of authorization. E3.4 is for all other unattended POI devices not meeting one of the aforementioned.)* *The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation*	A7	*Note: If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.* • *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.* • *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.* • *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation*	The note here indicates the change made to requirement B16.
	Modular Evaluation Vendor Questionnaire Total Questions: 3		Total Questions: 4	Additional guidance in Q1 states that access to the display is in scope of this requirement and where prompts and what protections are there.
	Modular Derived Test Requirements Total Tests: 3			 Identified as a possible red flag
	Modular Security Requirement			
A9	*The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.*	A8	*The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 2		Total Questions: 3	Additional documentation is required to be supplied to the lab.

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Derived Test Requirements Total Tests: 4		
Modular Security Requirement **A10** *It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation* **Modular Evaluation Vendor Questionnaire** Total Questions: 4 **Modular Derived Test Requirements** Total Tests: 5	**Modular Security Requirement** A9 *It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation* Total Questions: 6	Additional questions added to the questionnaire about the API used to collect the MSR data and how the device prevents skimming attacks including the path clear text MSR data travels inside the device.  Identified as a possible red flag
Modular Security Requirement **A11** *Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation* **Modular Evaluation Vendor Questionnaire** Total Questions: 7 **Modular Derived Test Requirements** Total Tests: 6	**Modular Security Requirement** A10 *Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation* Total Questions: 8	One new question about the use of cryptography to secure modular components and how replay and man-in-the-middle attacks are prevented. Important changes for UPT vendors

B – Core Logical Security Requirements

Requirement Alignment Table

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
B1	*The device performs a self-test, which includes integrity and authenticity tests as addressed in B4, upon start-up and at least once per day to check firmware, security mechanisms for signs of tampering, and whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner.*	B1	*The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.*	It is not clear what memory needs to be reinitialized or how this may be done. This almost appears to require a reboot.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 4		Total Questions: 8	Additional information about the boot code and loading of firmware is required for lab review and evaluation. Seems there is a move to make a distinction of the security module performing self test versus vendor code and segmentation for meeting the same requirement.
	Modular Derived Test Requirements			
	Total Tests: 4			New guidance provided
	Modular Security Requirement			
B2	*The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting the clear-text PIN or other sensitive data.*	B2	*The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting the clear-text PIN or other sensitive data.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 6		Total Questions: 10	The additional questions require more details about the logic used to process the API and what programming languages are used.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 4			New guidance provided
	Modular Security Requirement			
B3	*The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.*	B3	*The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 2		Total Questions: 4	Additional documentation for software design, testing and release is required for the device evaluation.
	Modular Derived Test Requirements Total Tests: 4			New guidance provided
	Modular Security Requirement			
B4	*If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.*	B4	*If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 5		Total Questions: 7	Additional questions about firmware loading and public/private key loading.
	Modular Derived Test Requirements Total Tests: 7			New guidance provided
	Modular Security Requirement			
		B4.1	*The firmware must support the authentication of applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.*	The additional B4.1 requirement was a SRED requirement and moved to a core requirement. Previously the PED only had to authenticate and test the integrity of firmware, now applications must also be authenticated and integrity tested.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Total Questions: 0		Total Questions: 9	The questions for this requirement are meant to identify all components that have "firmware" that are required to meet the PCI PTS requirements. The device must also perform authentication for applications as well as the previous requirement to authentication firmware.
	Modular Derived Test Requirements			
	Total Tests: 0			New tests for application authentication
	Modular Security Requirement			
B5	*The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.*	B5	*The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 2		Total Questions: 2	No new questions
	Modular Derived Test Requirements			
	Total Tests: 4			
	Modular Security Requirement			
B6	*Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button.* *The device must automatically clear its internal buffers when either:* • *The transaction is completed, or* • *The device has timed out waiting for the response from the cardholder or merchant.*	B6	*Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button.* *The device must automatically clear its internal buffers when either:* • *The transaction is completed, or* • *The device has timed out waiting for the response from the cardholder or merchant.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 10		Total Questions: 10	No new questions

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 4			
	Modular Security Requirement			
B7	*Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.*	B7	*Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 10		Total Questions: 11	The one additional questions requires all methods to load keys into the device be identified.
	Modular Derived Test Requirements Total Tests: 8			Modest impact
	Modular Security Requirement			
B8	*To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode.*	B8	*To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 8		Total Questions: 8	No new questions.
	Modular Derived Test Requirements Total Tests: 6			Modest Impact
	Modular Security Requirement			
B9	*If random numbers are generated by the device in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.*	B9	*If random numbers are generated by the device in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.*	

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 3 **Modular Derived Test Requirements** Total Tests: 5		Total Questions: 4	The additional questions are related to the random number generator and the seed for pseudo random number generator. Also, the applicability to open protocols. New guidance provided
	Modular Security Requirement			
B10	*The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.* **Modular Evaluation Vendor Questionnaire** Total Questions: 2 **Modular Derived Test Requirements** Total Tests: 3	B10	*The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.* Total Questions: 2	No new questions
	Modular Security Requirement			
B11	*The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.* **Modular Evaluation Vendor Questionnaire** Total Questions: 21 **Modular Derived Test Requirements** Total Tests: 10	B11	*The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.* Total Questions: 22	The V3.1 questions were numbered incorrectly so there were two #14 questions. So there were 21 in all. The one new question requires information about how the keys that are stored in the device are generated New guidance provided

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
B12	*The PIN-encryption technique implemented in the device is a technique included in ISO 9564.*	B12	*The PIN-encryption technique implemented in the device is a technique included in ISO 9564.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 2		Total Questions: 3	One new question: *Q3* *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.* Seems redundant with A1.
	Modular Derived Test Requirements			
	Total Tests: 3			
	Modular Security Requirement			
B13	*It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the device.* *The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.*	B13	*It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the device.* *The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 8		Total Questions: 9	The additional question requires specifics on the implementation if the device supports data decryption.
	Modular Derived Test Requirements			
	Total Tests: 4			
	Modular Security Requirement			
B14	*There is no mechanism in the device that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.*	B14	*There is no mechanism in the device that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.*	

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 4 **Modular Derived Test Requirements** Total Tests: 4		Total Questions: 4	No new questions
	Modular Security Requirement			
B15	*The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations.* **Modular Evaluation Vendor Questionnaire** Total Questions: 3 **Modular Derived Test Requirements** Total Tests: 3	B15	*The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations.* Total Questions: 3	No new questions.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
B16	***Note:*** *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A8, B16.1, B16.2, or E3.4.* *(Statements A8 and B16.1 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement B16.2 is an option that allows third parties to control the means of authorization. E3.4 is for all other unattended POI devices not meeting one of the aforementioned.)*	B16	*Note: If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.* *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.* *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.* *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation4 to circumvent. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.*	The overall requirement is the same. B16.1 and B16.2 was combined as they were redundant. Devices that allowed the changing of prompts operated in the same mode whether or not the acquirer or the vendor controlled the prompts.
B16.1	*All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation to circumvent. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.*			

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
B16.2	*Cryptographically based controls are utilized to control the device display and device usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the device. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key-management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.*			
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 9 (total)		Total Questions: 8	No new questions
	Modular Derived Test Requirements			
	Total Tests: 15 (total)			New guidance provided
	Modular Security Requirement			
B17	*If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the device, including modifying data objects belonging to another application.*	B17	*If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the device including, but not limited to, modifying data objects belonging to another application or the OS.*	Same overall requirement with additional guidance.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 3		Total Questions: 5	The additional questions are details about the application separation.
	Modular Derived Test Requirements			
	Total Tests: 4			Significant new guidance provided
	Modular Security Requirement			
B18	*The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.*	B18	*The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 4		Total Questions: 6	Additional questions about the operating system (commercial or custom) and the support of default API and functions.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 5			
	Modular Security Requirement			
B19	*The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.*	B19	*The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 2		Total Questions: 2	No new questions.
	Modular Derived Test Requirements Total Tests: 4			
	Modular Security Requirement			
		B20	*A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.*	This is a new requirement that requires the vendor to provide complete documentation on the secure use of the product. This will have to be provided to the evaluation lab to be marked "Yes"
	Modular Evaluation Vendor Questionnaire Total Questions: 0		Total Questions: 2	Questions on how the security policy is documented and how the device complies with the policy.
	Modular Derived Test Requirements Total Tests: 0			New guidance provided

C – Online Security Requirements

Requirement Alignment Table

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
C1	*If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the device prohibits unauthorized key replacement and key misuse.*	C1	*If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the device prohibits unauthorized key replacement and key misuse.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 3		Total Questions: 4	Additional questions providing information about the key hierarchies.
	Modular Derived Test Requirements			
	Total Tests: 2			

D – Offline Security Requirements

Requirement Alignment Table

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
D1	*It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, nor is it possible for both an ICC card and any other foreign object to reside within the card insertion slot.* *Note: The card reader may consist of areas of different protection levels, e.g., the areas of the ICC card interface itself, and the area holding retracted cards.*	D1	*It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, nor is it possible for both an ICC card and any other foreign object to reside within the card insertion slot.* ***Note:** All attacks shall include a minimum of ten hours' attack time for exploitation.*	The ten hour minimum for exploitation is finally included as a specific requirement. This has been a requirement for scoring the attack potential, but one would have to refer to the Technical FAQ.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 3		Total Questions: 19	The majority of the questions added to D1 are actually from the V3.1 D2 questionnaire. There is no explanation why they were moved.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 8			
	Modular Security Requirement			
D2	*The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.*	D2	*The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 11		Total Questions: 1	The missing questions from V4 were moved to D1. There is no explanation why they were moved.
	Modular Derived Test Requirements Total Tests: 2			
	Modular Security Requirement			
D3	*The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.*	D3	*The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 2		Total Questions: 2	No new questions.
	Modular Derived Test Requirements Total Tests: 2			
	Modular Security Requirement			
D4	*PIN protection during transmission between the device encrypting the PIN and the ICC Reader (at least two must apply):*	D4	*PIN protection during transmission between the device encrypting the PIN and the ICC reader (at least **two** must apply):* *If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be:* • *An enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.* • *A plaintext PIN, the PIN block shall be enciphered*	Overall the same requirement, D4.1 to D4.4 consolidated to one requirement.

PCI PTS Version 3.1	PCI PTS Version 4	Notes
	from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564. *If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be:* • *An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.* • *A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.*	
D4.1 *If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be an enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564* D4.2 *If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be a plain-text PIN, the PIN block shall be enciphered from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plain-text to the IC card) in accordance with ISO 9564* D4,3 *If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be an enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.* D4.4 *If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be a plain-text PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plain-text PIN is transmitted to the ICC reader through an unprotected environment, then the PIN block shall be*		

PCI PTS Version 3.1	PCI PTS Version 4	Notes
enciphered in accordance with ISO 9564. **Modular Evaluation Vendor Questionnaire** Total Questions: 5 **Modular Derived Test Requirements** Total Tests: 9 (total)	Total Questions: 4	No new questions.

Evaluation Module 2: POS Terminal Integration

E – POS Terminal Integration Security Requirements

No significant changes.

Evaluation Module 3: Open Protocols

F – POS Terminal Integration Security Requirements

There are no changes to these requirements, they have just be re-aligned.

Evaluation Module 4: Secure Reading and Exchange of Data (SRED)

Account Data Protection

Requirement Alignment Table

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
K1	*All account data is either encrypted immediately upon entry or entered in clear-text into a secure device and processed within the secure controller of the device.*	K1	*All account data is either encrypted immediately upon entry or entered in clear-text into a secure device and processed within the secure controller of the device.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 4		Total Questions: 4	No new questions

PCI PTS Version 3.1	PCI PTS Version 4	Notes
Modular Derived Test Requirements Total Tests: 3		
Modular Security Requirement K1.1 *The device protects all account data upon entry (consistent with A10 for magnetic stripe data and D1 for Chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation*	K1.1 *The device protects all account data upon entry (consistent with A10 for magnetic stripe data and D1 for Chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation* ***Note:*** *MSRs and ICCRs must meet the attack potentials stipulated in DTRs A10 and D1 respectively.*	There is a discrepancy here, K1.1 provides a specific attack potential that must be met. However the note indicates that the attack potentials are to be consistent with A10 and D1. A10 is the requirement for the magnetic stripe reader: • Attack potential is 18 points, minimum of 9 points for exploitation. D1 is the requirement for the contact chip card reader: • Attack potential is 20 points, minimum of 10 points for exploitation.
Modular Evaluation Vendor Questionnaire Total Questions: 22 (total)	Total Questions: 34 (total)	For devices that are PEDs these questions are consistent with various requirements in sections A-D. The duplication of the questions are for the devices that those devices that are not PIN Entry Devices and seek SRED approval.
Modular Derived Test Requirements Total Tests: 5		
Modular Security Requirement	K1.2 *Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.*	This is language consistent with A2 (A1.2 in version 3). This is potentially a major issue to meet SRED depending on the implementation that will require a reader redesign. In the key pad requirement, this meant that there was more than one active security mechanism that had

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
				to be defeated. Many reader implementation cannot meet this at this time, especially those used in modular POI devices. In the case of an encrypting heads, there is only one security mechanism in that the firmware and key are injected at the time of manufacturing and are typically a onetime event. These devices do not typically have battery backed RAM to store secrets. At this time the requirement is incomplete due to a lack of a version 4 technical FAQ.
	Modular Evaluation Vendor Questionnaire Total Questions: 0 **Modular Derived Test Requirements** Total Tests:		Total Questions: 4	New guidance provided
	Modular Security Requirement			
K2	*The logical and physical integration of an approved secure card reader into a PIN entry POI terminal does not create new attack paths to the account data. The account data is protected (consistent with A2) from the input component to the secure controller of the device.*	K2	*The logical and physical integration of an approved secure card reader into a PIN entry POI terminal does not create new attack paths to the account data. The account data is protected (consistent with A2) from the input component to the secure controller of the device.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 8 **Modular Derived Test Requirements** Total Tests: 4		Total Questions: 8	No new questions New guidance provided
	Modular Security Requirement			
K3	*Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation*	K3	*Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation.*	

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 5 **Modular Derived Test Requirements** Total Tests: 3		Total Questions: 7	See A7. New guidance provided
	Modular Security Requirement			
K3.1	*Public keys must be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorized modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation* **Modular Evaluation Vendor Questionnaire** Total Questions: 3 **Modular Derived Test Requirements** Total Tests: 3	K3.1	*Public keys must be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorized modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation* Total Questions: 3	No new tests
	Modular Security Requirement			
K4	*All account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (e.g., AES, TDES) and should use ANSI X9 or ISO-approved modes of operation.* **Modular Evaluation Vendor Questionnaire** Total Questions: 7 **Modular Derived Test Requirements** Total Tests: 6	K4	*All account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (e.g., AES, TDES) and should use ANSI X9 or ISO-approved modes of operation.* Total Questions: 7	No new questions
	Modular Security Requirement			
K5	*If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.* **Modular Evaluation Vendor Questionnaire** Total Questions: 5	K5	*If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.* Total Questions: 5	No new questions

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 4			
	Modular Security Requirement			
K6	*The device supports data origin authentication of encrypted messages.*	K6	*The device supports data origin authentication of encrypted messages.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 1		Total Questions: 1	No new questions
	Modular Derived Test Requirements Total Tests: 2			
	Modular Security Requirement			
K7	*Secret and private keys which reside within the device to support account data encryption are unique per device.*	K7	*Secret and private keys that reside within the device to support account data encryption are unique per device.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 1		Total Questions: 1	No new questions
	Modular Derived Test Requirements Total Tests: 3			
	Modular Security Requirement			
K8	*Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted.* *The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.*	K8	*Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted.* *The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 8		Total Questions: 8	No new questions, minor change to question 8 about unique keys.
	Modular Derived Test Requirements Total Tests: 4			New guidance provided

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
K9	*If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.*	K9	*If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 7		Total Questions: 7	No new questions
	Modular Derived Test Requirements			
	Total Tests: 9			
	Modular Security Requirement			
K10	*The firmware, and any changes thereafter, have been inspected and reviewed consistent with B3.*	K10	*The firmware, and any changes thereafter, have been inspected and reviewed consistent with B3.*	
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 2		Total Questions: 4	See B3 above
	Modular Derived Test Requirements			
	Total Tests: 4			New guidance provided
	Modular Security Requirement			
K11	*The device performs self-tests consistent with B1.*			Removed since K11.1 and K11.2 specify the requirements they must be consistent with.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 8		Total Questions: 0	
	Modular Derived Test Requirements			
	Total Tests: 4			
	Modular Security Requirement			
K11.1	*The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4.*	K11.1	*The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4.*	

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 9 (3 of which were unnumbered) **Modular Derived Test Requirements** Total Tests: 7		Total Questions: 9	No new questions.
	Modular Security Requirement			
K11.2	*The vendor must provide clear security guidance consistent with B2 and B6 to all application developers to ensure:* • *That it is not possible for applications to be influenced by logical anomalies which could result in clear text data being outputted whilst the terminal is in encrypting mode.* • *That account data is not retained any longer, or used more often, than strictly necessary.*	K11.2	*The vendor must provide clear security guidance consistent with B2 and B6 to all application developers to ensure:* • *That it is not possible for applications to be influenced by logical anomalies which could result in clear text data being outputted whilst the terminal is in encrypting mode.* • *That account data is not retained any longer, or used more often, than strictly necessary.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 1 **Modular Derived Test Requirements** Total Tests: 3		Total Questions: 1	No new questions
	Modular Security Requirement			
K12	*If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.*	K12	*If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.*	
	Modular Evaluation Vendor Questionnaire Total Questions: 5 **Modular Derived Test Requirements** Total Tests: 7		Total Questions: 7	See B4 above.
	Modular Security Requirement			
K13	*The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying*	K13	*The device's functionality shall not be influenced by logical anomalies consistent with B2.*	

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	wrong parameters or data which could result in the device outputting clear-text account data. **Modular Evaluation Vendor Questionnaire** Total Questions: 6 **Modular Derived Test Requirements** Total Tests: 4		Total Questions: 10	See B2 above New guidance provided
	Modular Security Requirement			
K14	*The security requirements specified in sections H and J of the Open Protocols module have been met.* **Modular Evaluation Vendor Questionnaire** Total Questions: 1 **Modular Derived Test Requirements** Total Tests: 2	K14	*If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), then requirements specified in DTR Module 3: Open Protocols Requirements have been met.* Total Questions: 1	Based on the change to open protocols module, K14 and K15 have been combined to one requirement No new questions.
	Modular Security Requirement			
K15	*If the device is capable of communicating over an IP network, the security requirements specified in sections F, G, and I of the Open Protocols module have been met.* **Modular Evaluation Vendor Questionnaire** Total Questions: 1 **Modular Derived Test Requirements** Total Tests: 2		Total Questions: 0	
	Modular Security Requirement			
K16	*When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.*	K15	*When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.*	Same requirement, different requirement reference.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 8 **Modular Derived Test Requirements** Total Tests: 8		Total Questions: 8	No new questions New guidance provided
	Modular Security Requirement			
K16.1	*When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device.*	K15.1	*When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire Total Questions: 2 **Modular Derived Test Requirements** Total Tests: 3		Total Questions: 2	No new tests
	Modular Security Requirement			
K16.2	*Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*	K15.2	*Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire Total Questions: 9 **Modular Derived Test Requirements** Total Tests: 4		Total Questions: 9	No new tests
	Modular Security Requirement			
K17	*If the device is capable of generating surrogate PAN values to be outputted outside of the device, it is not possible to determine the original PAN knowing only the surrogate value.*	K16	*If the device is capable of generating surrogate PAN values to be outputted outside of the device, it is not possible to determine the original PAN knowing only the surrogate value.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire Total Questions: 2 **Modular Derived Test Requirements** Total Tests: 3		Total Questions: 2	No new tests

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Security Requirement			
K17.1	*If using a hash function to generate surrogate PAN values, input to the hash function must use a salt with minimum length of 64-bits.*	K16.1	*If using a hash function to generate surrogate PAN values, input to the hash function must use a salt with minimum length of 64-bits.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 2		Total Questions: 2	No new questions
	Modular Derived Test Requirements			
	Total Tests: 4			
	Modular Security Requirement			
K17.2	*If using a hash function to generate surrogate PAN values, the salt is kept secret and appropriately protected. Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per device for identification and initial exploitation with a minimum of 8 for exploitation*	K16.2	*If using a hash function to generate surrogate PAN values, the salt is kept secret and appropriately protected. Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per device for identification and initial exploitation with a minimum of 8 for exploitation*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 1		Total Questions: 1	No new questions
	Modular Derived Test Requirements			
	Total Tests: 3			
	Modular Security Requirement			
K18	*The key-management techniques implemented in the device are consistent with B11.*	K17	*The key-management techniques implemented in the device are consistent with B11.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire			
	Total Questions: 20		Total Questions: 22	See A6 above
	Modular Derived Test Requirements			
	Total Tests: 10			
	Modular Security Requirement			
K19	*The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.*	K18	*The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.*	Same requirement, different requirement reference.

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Evaluation Vendor Questionnaire Total Questions: 1 **Modular Derived Test Requirements** Total Tests: 3		Total Questions: 1	No new questions
	Modular Security Requirement			
K20	*If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose any secret or private keys or account data. Immediate access to secret or private keys or account data is either prevented by the design of the internal areas (e.g., by enclosing components with such data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of secret and private keys and account data.*			This requirement was removed because it was redundant with other tests.
	Modular Evaluation Vendor Questionnaire Total Questions: 6 **Modular Derived Test Requirements** Total Tests: 8		Total Questions: 0	
	Modular Security Requirement			
K21	*Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data.* *(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)*	K19	*Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data.* *(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire Total Questions: 4 **Modular Derived Test Requirements** Total Tests: 4		Total Questions: 6	See A3 above
	Modular Security Requirement			
K22	*If the device supports multiple applications, it must enforce the separation between applications consistent*	K20	*If the device supports multiple applications, it must enforce the separation between applications consistent*	Same requirement, different requirement

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	with B17. **Modular Evaluation Vendor Questionnaire** Total Questions: 3 **Modular Derived Test Requirements** Total Tests: 4		*with B17* Total Questions: 5	reference. Additional information about application security and separation.
K23	**Modular Security Requirement** *The following features of the device's operating system must be in place:* • *The operating system of the device must contain only the software (components and services) necessary for the intended operation.* • *The operating system must be configured securely and run with least privilege.* • *The security policy enforced by the device must not allow unauthorized or unnecessary functions.* • *API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed).* **Modular Evaluation Vendor Questionnaire** Total Questions: 6 **Modular Derived Test Requirements** Total Tests: 7	K21	*The following features of the device's operating system must be in place:* • *The operating system of the device must contain only the software (components and services) necessary for the intended operation.* • *The operating system must be configured securely and run with least privilege.* • *The security policy enforced by the device must not allow unauthorized or unnecessary functions.* • *API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed).* Total Questions: 7	Same requirement, different requirement reference. See B18 above
K24	**Modular Security Requirement** *Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.* **Modular Evaluation Vendor Questionnaire** Total Questions: 10	K22	*Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.* Total Questions: 11	Same requirement, different requirement reference. See B7 above

	PCI PTS Version 3.1		PCI PTS Version 4	Notes
	Modular Derived Test Requirements Total Tests: 6			
	Modular Security Requirement			
K25	*Sensitive services are protected from unauthorized use consistent with B8.*	K23	*Sensitive services are protected from unauthorized use consistent with B8.*	Same requirement, different requirement reference.
	Modular Evaluation Vendor Questionnaire Total Questions: 8		Total Questions: 8	See B8 above
	Modular Derived Test Requirements Total Tests: 6			

Summary of Additional Questions and Test

A – Core Physical Security Requirements

	Questionnaires			DTR Tests		
V4 Requirement	**V3**	**V4**	**% Increase**	**V3**	**V4**	**% Increase**
A1	9	20	122%	6	32	433%
A2	4	4	0%	3	4	33%
A3	3	5	67%	4	10	150%
A4	6	11	83%	4	13	225%
A5	3	3	0%	3	4	33%
A6	6	6	0%	5	10	100%
A7	5	6	20%	3	15	400%
A8	3	4	33%	3	7	133%
A9	2	3	50%	4	12	200%
A10	4	6	50%	5	9	80%
A11	7	8	14%	6	12	100%
	52	76	46%	46	128	178%

B – Core Logical Security Requirements

	Questionnaires			DTR Tests		
V4 Requirement	V3	V4	% Increase	V3	V4	% Increase
B1	4	8	100%	4	14	250%
B2	6	10	67%	4	11	175%
B3	2	4	100%	4	19	375%
B4	5	7	40%	7	14	100%
B4.1		9			14	
B5	2	2	0%	4	8	100%
B6	10	10	0%	4	8	100%
B7	10	11	10%	8	18	125%
B8	8	8	0%	6	9	50%
B9	3	4	33%	5	6	20%
B10	2	2	0%	3	8	167%
B11	21	22	5%	10	26	160%
B12	2	3	50%	3	9	200%
B13	8	9	13%	4	5	25%
B14	4	4	0%	4	7	75%
B15	3	3	0%	3	4	33%
B16	9	8	-11%	15	13	-13%
B17	3	5	67%	4	14	250%
B18	4	6	50%	5	8	60%
B19	2	2	0%	4	4	0%
B20		2			19	
	108	139	29%	101	238	136%

C – Online Security Requirements

	Questionnaires			DTR Tests		
V4 Requirement	V3	V4	% Increase	V3	V4	% Increase
C1	3	4	33%	2	5	150%
	3	4	33%	2	5	150%

D – Offline Security Requirements

	Questionnaires	DTR Tests

V4 Requirement	V3	V4	% Increase	V3	V4	% Increase
D1	3	19	533%	8	19	138%
D2	11	1	-91%	2	3	50%
D3	2	2	0%	2	6	200%
D4	5	4	-20%	9	11	22%
	21	26	24%	21	39	86%

Account Data Protection

	Questionnaires			DTR Tests		
V4 Requirement	V3	V4	% Increase	V3	V4	% Increase
K1	4	4	0%	3	3	0%
K1.1	22	34	55%	5	5	0%
K1.2		4			4	
K2	8	8	0%	4	4	0%
K3	5	7	40%	3	14	367%
K3.1	3	3	0%	3	3	0%
K4	7	7	0%	6	6	0%
K5	5	5	0%	4	4	0%
K6	1	1	0%	2	2	0%
K7	1	1	0%	3	4	33%
K8	8	8	0%	4	4	0%
K9	7	7	0%	9	9	0%
K10	2	4	100%	4	19	375%
K11	8	0	-100%	4	0	-100%
K11.1	9	9	0%	7	14	100%
K11.2	1	1	0%	3	3	0%
K12	5	7	40%	7	14	100%
K13	6	10	67%	4	14	250%
K14	1	1	0%	2	2	0%
K15	1	0	-100%	2	0	-100%
K16	8	8	0%	8	8	0%
K16.1	2	2	0%	3	3	0%
K16.2	9	9	0%	4	8	100%
K17	2	2	0%	3	3	0%
K17.1	2	2	0%	4	4	0%
K17.2	1	1	0%	3	3	0%
K18	20	22	10%	10	25	150%
K19	1	1	0%	3	3	0%
K20	6			8		
K21	4	6	50%	4	10	150%
K22	3	5	67%	4	12	200%
K23	6	7	17%	7	9	29%
K24	10	11	10%	6	16	167%
K25	8	8	0%	6	9	50%

186	205	10%	152	241	59%

Totals

Total

Questionnaires			DTR Tests		
V3	**V4**	**% Increase**	**V3**	**V4**	**% Increase**
370	450	22%	322	651	102%

Summary

This paper is not meant to bash the PCI SSC in anyway. We actually appreciate the program because it sets the security bar and levels the playing field for all secure payment terminal vendors. However, we have a long history with PED security and have watched the evaluation from the Visa PED vendor self attestation to the Visa PED lab evaluation to the introduction of PCI to finally where we are today.

By now you are probably wondering about the title of this white paper *PCI PTS V3.x to V4.0 Gap Analysis, But WTF*. The actual title of this paper is:

*PCI PTS V3.x to V4.0 Gap Analysis, But **W**here's the **T**echnical **F**AQ*.

For those that have been involved with the PCI program for any amount of time know that the true requirements are not in the security requirements, questionnaire or even the DTRs, they are actually refined in the Technical FAQs. And the technical FAQs can be published at any time, and could when published have negatively affected a new product development cycle.

There are also some very vague security requirements hidden in plain sight of the details that may be difficult to address without the infamous technical FAQ.