Payment Card Industry (PCI)

Software-based PIN Entry on COTS™ Magnetic Stripe Readers Annex

Security and Test Requirements

May 2019

Document Changes

Date	Version	Description
May 2019	1.0	Initial publication.

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this optional Software-based PIN Entry on COTS™ (SPoC™) Magnetic Stripe Readers Annex (*SPoC Annex*) is to provide additional security and testing requirements for Software-based PIN Entry on COTS™ (SPoC™) Solutions ("SPoC Solution") to support magnetic stripe readers (MSR) that are used with an SPoC PIN Cardholder Verification Method (CVM) Application for payment acceptance.

The security and testing requirements described in *SPoC Annex* provide a framework for protecting the confidentiality and integrity of Account data[1] captured and processed on a standalone MSR. The MSR works in combination with the existing elements of an SPoC Solution. Adding optional support to process magnetic stripe transactions allows merchants to use a single solution to accept payments.

1.2 Background

SPoC Solutions enable cardholders to enter their PIN into a PIN CVM Application running on a commercial off-the shelf (COTS) Device for authorization of contact or contactless EMV® card payment transactions. Software-based PIN entry (online or offline PIN) is permitted only for contact and contactless chip-based transactions that are processed online. To support the reading of chip enabled cards or devices, chip-only validated PCI PIN Transaction Security (PTS) Secure Carder Reader PIN (SCRP) readers must be used.

To support and process transactions from the reading of magnetic-stripe cards, SPoC Solutions may support standalone MSRs, as long as the PIN is not allowed for such transactions. The MSR is an accessory to the SPoC Solution for payment acceptance, and not a substitute for the SCRP as it relates to producing surrogate PAN values or random seeds used by the PIN CVM Application.

[1] Refer to *PCI PTS POI Technical Evaluation FAQs*, Section K1 Question 3.

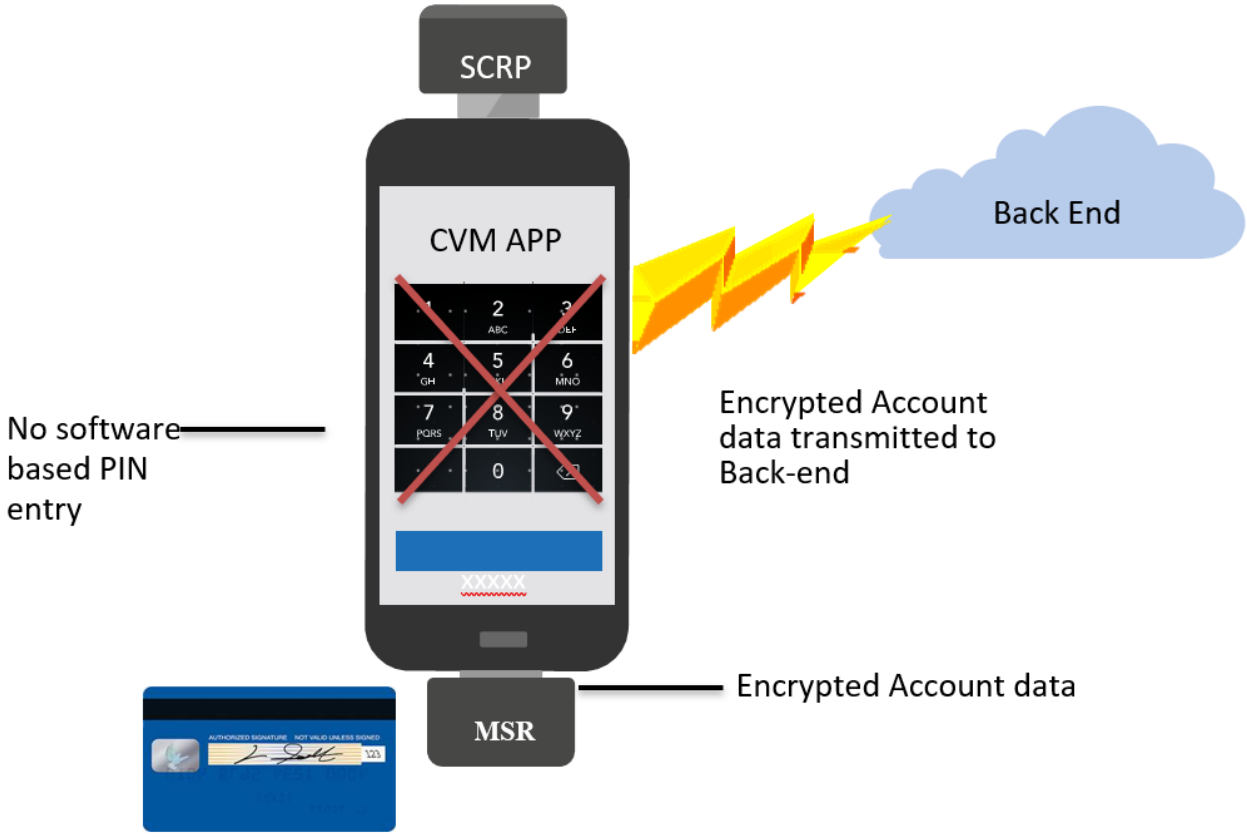

Figure 1: Example of PIN CVM Solution Architecture with Optional MSR Support

An MSR in an SPoC Solution has the following characteristics:

- The MSR supports only magnetic-stripe transactions.
- The MSR produces only encrypted Account data according to the requirements outlined in this document.
- The MSR connects and communicates securely with the PIN CVM Application.
- The MSR undergoes a security evaluation and approval, and it is referenced as part of the SPoC Solution.

1.3 Introduction to the Use of MSRs

To protect the Account data that is read from magnetic-stripe cards and the encrypted output that is delivered to the back-end payment processing systems, the MSR must conform to one of the following:

- *PCI PTS POI Modular Security Requirements*

Note: The MSR must be an approved PCI PTS device that is listed on the PCI SSC Approved Device website with an SCR Approval Class and supports only contact magnetic stripe.

OR

- The security requirements identified in this document

Note: A SPoC Lab must validate the MSR against specific requirements in Section 4, *Non-PTS Approved MSR Security Requirements and Derived Test Requirements*, which focuses on encryption of Account data on the device.

When MSRs are used in SPoC Solutions, only the MSR devices included in the SPoC Solution listing can be used.

When the Account data is read through an MSR, the PIN CVM Application will not allow software-based PIN entry.

To maintain the integrity of the SPoC Solution, the SCRP, which is a mandatory element of the SPoC Solution, must always be in position to communicate with the PIN CVM Application, even during the processing of data read by an MSR. All chip-based contact and contactless payment transactions must originate from the SCRP.

Table 1 summarizes the options and the applicability of PCI SSC standards/programs to the supported MSRs allowed in an SPoC Solution.

Table 1: Applicability of PCI SSC Standards/Programs to MSR

	Listed PCI PTS SCR		Non-PTS Approved MSR
Security Requirements	*PCI PTS POI Security Requirements*, SRED Module 4		Security and test requirements listed in Section 4, *Non-PTS Approved MSR Security Requirements and Derived Test Requirements*
Test Requirements	*PCI PTS POI Modular Derived Test Requirements*		
MSR Evaluation, Device Approval and Device Listing Process	*PCI PTS, Device Testing and Approval Program Guide*	**OR**	Evaluation and Device Approval Process as in *SPoC Program Guide* and *SPoC Annex*[2]
SPoC Solution Listing Process	Evaluation and Device Approval Process as in *SPoC Program Guide* and *SPoC Annex*		

1.4 Audience

The security and test requirements outlined in this document apply to entities who are developing SPoC Solutions that incorporate MSR functions and to PCI-recognized SPoC Laboratories.

1.5 Usage Conventions

This document uses the following terms with specific meanings:

- **Must** defines a mandatory requirement.
- **Should** defines a recommendation.

1.6 References

PCI PTS POI Requirements and Derived Test Requirements V5.1

PCI PTS Device Testing and Approval Program Guide V1.8

[2] Refer to Validating, Listing and Maintaining SPoC Solutions with MSRs for guidance on specific conflicts between the *SPoC Annex* and the *SPoC Security Requirements* and *SPoC Test Requirements*.

1.7 Glossary

In addition to terms defined in the *PCI DSS Glossary, Abbreviations and Acronyms*[3], *Software-based PIN Entry on COTS (SPoC) Security Requirements*, the terms/acronyms listed in Table 2 are used throughout this document.

Table 2: Glossary of Terms

Term	Definition
SCR	Abbreviation for Secure Card Reader. A physical card reader that has been assessed compliant to the PCI PTS POI device in SCR Approval Class and is listed on the PTS approval Website.
MSR	Abbreviation for Magnetic Stripe Reader. Magnetic Stripe Reader permitted in an SPoC Solution that either is listed as an approved PCI PTS POI device on the PCI SSC Approved Device website with a SCR Approval Class or is validated in accordance with the security requirements identified in this document and listed as part of The Solution. Also referred to as "Permitted MSR".
Firmware	Any code present in an MSR or an SCRP approval-class device is considered firmware and must be assessed and listed as part of the device approval.

[3] https://www.pcisecuritystandards.org/pci_security/glossary

2 Domain 1: MSR Use in an SPoC Solution

Security Requirements	Test Requirements	Guidance
1.1 All MSR devices must encrypt Account data when a card is read (card swipe).	**1.1.a** The tester must verify that the MSR meets one of the following conditions: • Approved PCI PTS device (approval class SCR) • Evaluated as part of the *SPoC MSR Annex*.	MSRs should encrypt Account data to prevent exposure within the PIN CVM Application and to ensure that Account data is securely transmitted to the back-end processing environment. The security of the encryption process within the MSR is expected to satisfy the encryption requirements in Section 4, *Non-PTS Approved MSR Security Requirements and Derived Test Requirements*..
	1.1.b For all approved PCI PTS devices, the tester must list and provide the PCI PTS approval number for each device and verify that the device is designed to operate in a single state, encrypting all Account data. ***Note:*** Report as required in *SPoC Test Requirement* TF1.1.	
	1.1.c For MSR devices that are not PCI PTS approved, the tester must verify that the MSRs meet the security requirements listed in Section 4, *Non-PTS Approved MSR Security Requirements and Derived Test Requirements*.	
	1.1.d The tester must verify that the MSR devices under review support only magnetic-stripe reading mechanisms.	
1.2 MSRs must not output Account data in clear text.	**1.2.a** The tester must verify that the Account data is not available (or required for processing) in clear text outside the MSR. ***Note:*** Report as required in *SPoC Test Requirement* TB 3.1.	To protect the confidentiality of the Account data, the MSR is required to output only encrypted Account data.

3 Domain 2: PIN CVM Application and Back-end Monitoring Systems

Security Requirements	Test Requirements	Guidance
2.1 PIN CVM Application must ensure SCRP is connected, secured, and operational at all times. **2.1.1** If the SCRP is unavailable, MSR-based transactions may optionally be processed under the following conditions: • Back-end Monitoring System must be able to detect the absence of an SCRP. • The Solution Provider must have a documented policy and a set of risk-based parameters to allow processing of MSR transactions to continue in the absence of an SCRP.	**2.1.a** The tester must verify that the PIN CVM Application does not process payment transactions from an MSR when the SCRP triggers tamper-response mechanisms documented in *SPoC Test Requirements* TC2.3 and TC2.4.	SCRPs support the reading of chip-based cards and payment devices, and provide security for the PIN CVM Application (seeding RNG, message signing). SCRPs are mandatory in the SPoC Solution. When an SCRP is unavailable, the Solution may optionally support MSR transaction processing. However, the Solution is required to detect that an SCRP is unavailable, and the Solution Provider should have a documented policy and a set of risk-based parameters to allow MSR transaction processing to continue in the absence of an SCRP. Risk parameters may include, but are not limited to: • Time period the SCRP is unavailable • Number of transactions allowed without an SCRP being connected • Other mitigating controls implemented in the Back-end Monitoring Systems
	2.1.b The tester must verify that the SPoC Solution allows for the physical connection or pairing of MSR devices in addition to and in conjunction with an SCRP.	
	2.1.c The tester must verify that the Back-end Monitoring System can detect when an SCRP is unavailable.	
	2.1.d When an SCRP is unavailable, the tester must verify that the Solution Provider has a documented policy and a set of risk-based parameters under which magnetic-stripe-read transactions are permitted.	
2.2 PINs must not be prompted for or allowed to be entered into the PIN CVM Application when an MSR is used.	**2.2.a** The tester must verify that the PIN CVM Application does not allow software-based PIN entry when an MSR is used.	The software-based PIN entry process should be protected from manipulation or subversion. Software-based PIN entry is allowed only for chip-based contact or contactless transactions and should not be entered when a magnetic stripe is read by an MSR that is permitted by the SPoC Solution.
	2.2.b The tester must note any other transaction types supported by the PIN CVM Application, and for each type that does not involve a chip-based transaction, confirm that the software-based PIN entry is not supported or able to be performed. ***Note:*** Report as required in *SPoC Test Requirement* TB10.2.	

Security Requirements	Test Requirements	Guidance
2.3 PIN CVM Application must ensure that the PIN has been cleared securely from memory.	**2.3.a** The tester must verify that the PIN CVM Application securely clears its internal buffers when one of the following occurs: • The transaction terminates for any reason (success or failure) • The PIN CVM Application has timed out waiting for a response from the cardholder or merchant • Transaction fall-back from SCRP to MSR • The monitoring system has signalled a tamper-detection event; or the PIN CVM Application is halted, loses focus, or otherwise is moved to background processing. ***Note:*** Report as required in *SPoC Test Requirement* TB7.	• To prevent correlation of the PIN entered on the COTS Device and Account data from the MSR, the PIN CVM Application should automatically clear its internal buffers (memory it controls). See additional guidance in SPoC Test Requirements TB7.
2.4 PIN CVM Application must not have access to clear text Account data originating from an MSR.	**2.4.a** The tester must verify that the PIN CVM Application cannot modify or decrypt the Account data received from an MSR. ***Note:*** Report as required in *SPoC Test Requirements* TB3.4.	The PIN CVM Application should not be able to decrypt the Account data encrypted by the MSR. Decryption of Account data can occur only in the PCI DSS-compliant back-end processing environment. See the *SPoC Security Requirement 5.1* for additional guidance.
	2.4.b The tester must verify that PIN CVM Application cannot disable encryption of the Account data. ***Note:*** Report as required in *SPoC Test Requirements* B5 and D2.	
	2.4.c The tester must verify that MSR encryption keys are never available to the PIN CVM Application.	
2.5 Only permitted MSRs can be used in the SPoC Solution for the purpose of magnetic-stripe payment acceptance.	**2.5.a** The tester must verify that the SPoC Solution supports only permitted MSRs. ***Note:*** Report as required in *SPoC Test Requirement* TR F1.	Permitted MSRs provide a security baseline to protect Account data. The SPoC Solution supports MSRs that meet either of the following conditions: • Listed as an approved PCI PTS device on the PCI SSC Approved Device Website with an SCR Approval Class • Evaluated by an SPoC Lab to meet the security requirements listed in Section 4, *Non-PTS Approved MSR Security Requirements and Derived Test Requirements*.

Security Requirements	Test Requirements	Guidance
2.6 The Back-end Monitoring System or PIN CVM Application must identify the MSR. **2.6.1** Transactions originating from unrecognized MSRs that are not associated with the SPoC Solution must be managed in accordance with established risk-based policies.	**2.6.a** The tester must verify that mechanisms exist to uniquely identify the MSR. ***Note:*** Report as required in *SPoC Test Requirement* TD1.1-1.2.	Identification of the MSR can contribute to confirming the security status of the SPoC Solution when preparing to process a payment transaction. The physically connected or securely paired MSR should be uniquely identified by the Back-end Monitoring System or PIN CVM Application. For example, the PIN CVM Application or the Back-end Monitoring System could identify the connected MSR by determining a unique, verifiable identifier. MSR identification ensures that all communications come from a recognized MSR associated with the SPoC Solution, and that risks associated with transactions originating from unrecognized MSRs are managed in accordance with established risk policies. MSR identification should be performed before accepting encrypted Account data when the MSR supports bi-directional communication. In cases where the MSR cannot be queried because the MSR outputs only encrypted Account data, the identifier is usually supplied with the encrypted Account data. The identifier can be used to verify the MSR with the back-end monitoring or payment processing systems, and confirm that the firmware on the device is acceptable.
	2.6.b The tester must detail these identification mechanisms and the criteria used to validate their use. ***Note:*** Report as required in *SPoC Test Requirements* TC2.2-TC2.4.	
	2.6.c The tester must verify that the Solution Provider has implemented risk-based policies to manage unrecognized MSRs.	
	2.6.d The tester must attempt to connect an unrecognized MSR and confirm that it is detected and managed in accordance with established risk-based policy.	

4 Non-PTS Approved MSR Security Requirements and Derived Test Requirements

MSRs used in an SPoC Solution must encrypt Account data to prevent exposure within the PIN CVM Application and to ensure that Account data is securely transmitted to the back-end processing environment. Applicable requirements were adopted from *PCI PTS POI v5.1* with a primary focus on Account data encryption.

The following sections provide instructions to the SPoC Lab about how to apply the PTS evaluation method for non-PTS-listed MSRs.

4.1 MSR K—Secure Reading and Exchange of Data

4.1.1 MSR K1—Account Data Processing

Security Requirements	Test Requirements	Guidance
All Account data is encrypted immediately upon entry.	Evaluate and report as required in *PCI PTS POI* DTR K1.	This requirement ensures that all Account data is handled in a secure manner. The requirement allows for the encryption of Account data directly at the read head, or for Account data to be submitted to the controller of the MSR in clear text. This data is then communicated to the MSR controller where it is processed. The term “processed” includes, but is not limited to, Account data encryption and the selective disclosure of clear text Account data by the secure controller to authenticated applications (per *PTS POI* K15.1). An MSR intended for use with a COTS device in an SPoC Solution should never release Account data in the clear.

4.1.2 MSR K4 Encryption Mechanisms

Security Requirements	Test Requirements	Guidance
Account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (such as, AES, TDES) and must use ANSI X9 or ISO-approved modes of operation.	Evaluate and report as required in *PCI PTS POI* DTR K4.	All Account data should be encrypted using only ANSI X9 or ISO-approved encryption algorithms (such as, AES, TDES). The encryption algorithm should use a mode of operation described in *ISO/IEC 10116:2006* (or equivalent), and follow secure padding guidelines. Any text encryption method that relies on non-standard modes of operation (such as, format-preserving Feistel-based Encryption Mode [FFX]) should be approved by at least one independent security evaluation organization or standards body. Such encryption methods should be subjected to independent expert review and implemented following all guidelines rising from the evaluation and peer review, including any recommendations for associated key management. The independent expert should be qualified through a combination of education, training, and experience in cryptology to provide objective technical evaluations that are independent of any ties to vendors and special interests. Independent expert qualifications are further defined in the *PCI PTS POI Glossary*. Double-length TDES keys can be used only in unique-key-per-transaction implementations as defined *in ISO 11568* for key derivation or transformation, such as DUKPT. Double-length TDES keys are not permitted in master/session or fixed key implementations.

4.1.3 MSR K5 Remote Key Distribution

Security Requirements	Test Requirements	Guidance
If remote key distribution is used, the MSR must support mutual authentication between the sending key-distribution host and receiving device.	Evaluate and report as required in *PCI PTS POI* DTR K5.	It should not be possible to subvert the key distribution process to expose cryptographic keys. Only legitimate peers may engage in key distribution. Legitimacy may be established, for example, through a demonstration of knowledge (proof of possession) of a shared secret. If an identity-based scheme is used, pair-wise keys may be "exchanged" using a non-interactive process.

4.1.4 MSR K6 Data Origin Authentication

Security Requirements	Test Requirements	Guidance
If the MSR supports bi-directional communication and provides access to Sensitive Services or functions, the MSR must support data-origin authentication of encrypted messages.	Evaluate and report as required in *PCI PTS POI* DTR K6.	To prevent an adversary from posing as a legitimate sender to send falsified messages and to allow the tracing of particular actions to a specific device, the MSR should support data origin authentication on all encrypted messages.

4.1.5 MSR K7 Unique Secret and Private Keys Per MSR Device

Security Requirements	Test Requirements	Guidance
Secret and private key(s) that reside within the MSR to support Account data encryption are unique for each MSR device.	Evaluate and report as required in *PCI PTS POI* DTR K7.	The use of a single secret key deployed to numerous MSR devices introduces unacceptable vulnerabilities into the payment chain. Should a single MSR be compromised, all data encrypted from MSR devices that share a common key may be decrypted.

4.1.6 MSR K9 Remote Access

Security Requirements	Test Requirements	Guidance
If the MSR can be accessed remotely for administration purposes, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access must be denied.	Evaluate and report as required in *PCI PTS POI* DTR K9.	Authentication should not be performed by a component of lesser protection strength than the one for which the access is intended; or the authentication should be performed by the target component. MSR K11.1 and MSR K12 address application loads, firmware updates, application updates, and configuration updates. MSR K9 addresses other administration activities. A secure session should be established for these communications, unless there is no impact, when for example, the load itself is cryptographically authenticated at the target.

4.1.7 MSR K10 Firmware Certification

Security Requirements	Test Requirements	Guidance
The firmware and any subsequent updates have been inspected and reviewed consistent with *PCI PTS POI* B3.	Evaluate and report as required in *PCI PTS POI* DTR K10.	The vendor should indicate the compiler settings to maximize the mitigation of known vulnerabilities. The vendor should implement measures to help prevent common exploits of "buffer overflow" and similar vulnerabilities. Programming strategies to address these vulnerabilities include: • Avoid them by design. For example, use a programming language that prevents buffer overflow. • Find vulnerabilities through adequate testing. For example, use static-code analysis or comprehensive fuzz testing. • Mitigate vulnerabilities with techniques such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Harvard Architecture and Stack Canaries. The vendor should document where labs may place reliance upon measures to help prevent common exploits and vulnerabilities in connection with *PCI PTS POI* K13 and other relevant requirements.

4.1.8 MSR K 11.1 Software Authenticity

Security Requirements	Test Requirements	Guidance
If the MSR allows firmware and/or configuration updates, the MSR cryptographically authenticates all updates consistent with *PCI PTS POI* B4.	Evaluate and report as required in *PCI PTS POI DTR* K11.1.	Firmware is any code that can be loaded onto the MSR.

4.1.9 MSR K12 Firmware Updates

Security Requirements	Test Requirements	Guidance
If the MSR allows firmware updates, the MSR must cryptographically authenticate the firmware, and if the authenticity is not confirmed, the firmware update is rejected and deleted.	Evaluate and report as required in *PCI PTS POI* DTR K12.	Firmware is considered to be any code within the MSR. The evaluating lab may require copies of source code and assistance from the vendor to make a systematic review of relevant security functions. The authentication should not be performed by a component of lesser protection strength than the one for which the firmware/software is intended, or the authentication performed by the target component of the firmware. The MSR should have the ability to accept firmware updates from a remote host, such as a terminal management system using polling or similar techniques. If the firmware updates are done between physically and logically disparate components, the update mechanism should use a secure channel as follows: • Each secure channel should provide mutual authentication to uniquely identify each component before exchanging Sensitive Data. The secure channel should also protect against man-in-the-middle (MITM) and replay attacks. • Mutual authentication between the communicating components should be based on cryptography that aligns with *PCI PTS POI Appendix E*, *"Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms."* • Cryptographic keys used to establish secure channels between components and for data encryption should be unique, except by chance.

4.1.10 MSR K13 Logical Anomalies

Security Requirements	Testing Requirements	Guidance
The MSR's functionality must not be influenced by logical anomalies and be consistent with *PCI PTS POI* B2.	Evaluate and report as required in *PCI PTS POI* DTR K13.	Functionality is considered as any operation, via any internal or external interface, that could impact the security of all of the MSR's relevant components. Vendors should provide software-design rules and specifications to support their claims that the MSR operations are not influenced by logical anomalies. All interfaces and associated communication methods of the MSR should be assessed. The interfaces should be documented and assessed regardless of whether they are used for or have access to Account data. Sufficient evidence should be provided to demonstrate the validity of laboratory assessments. The *PCI PTS POI* Open Protocols Module should be used to assess any communication method that uses a wireless, local, or wide-area network to transport data. This includes, but is not limited to, Bluetooth, Wi-Fi, Cellular (GPRS, CDMA), or Ethernet. A serial point-to-point connection would not need to be assessed unless that connection is wireless or through a hub, switch, or other multiport device. In addition, any communication that uses a public domain protocol or security protocol would be assessed with the Open Protocols Module.

4.1.11 MSR K14 Open Protocols and Services

Security Requirements	Test Requirements	Guidance
If the MSR 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 *PCI PTS POI* DTR Module 3: *Open Protocols Requirements* and any applicable FAQs must be met. All security requirements and corresponding testing requirements specified in *PCI PTS POI* Sections F, G, H, and I of DTR Module 3: *Open Protocols Requirements* must be met.	Evaluate and report as required in PCI *PTS POI* DTR K14.	Weak implementations of IP stacks, and/or ancillary IP services can act as attack vectors into an MSR device.

4.1.12 MSR K15 Clearing of Internal Buffers

Security Requirements	Test Requirements	Guidance
Account data must not be retained longer, or used more often, than strictly necessary.	Evaluate and report as required in PCI *PTS POI* DTR K15.2.	The MSR should automatically ensure that full Account data is cleared when either of the following occur: • The transaction is completed. • The MSR has timed out waiting for the response from the cardholder or merchant.

4.1.13 MSR K16 Surrogate PAN Values

Security Requirements	Test Requirements	Guidance
If the MSR is capable of generating surrogate PAN values to be output outside of the MSR device, it must not be possible to determine the original PAN knowing only the surrogate value.	Evaluate and report as required in PCI *PTS POI* DTR K16.	To support the ancillary business process, surrogate PAN values may be generated by the MSR. The probability of determining the original PAN knowing only the surrogate value should be no better than a random guess.

4.1.14 MSR K16.1 Salt Generation

Security Requirements	Test Requirements	Guidance
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.	Evaluate and report as required in PCI *PTS POI* DTR K16.1.	A cryptographic salt comprises random bits that can be input into a cryptographic function. Random bits should be generated such that the probability of the same random bits being output is statistically insignificant. A known salt value may compromise the effectiveness of the cryptographic function. The salt may be unique per transaction, unique per a group of transactions, unique per MSR, or unique per merchant. Salts that are unique per transaction or otherwise unique per MSR, should be generated by the transaction MSR device. Salts that are unique per merchant are generated outside the transaction MSR device and require loading to each merchant MSR. The vendor should supply documentation to the merchant/acquirer processor about how to securely load the salt values and how this loading is treated as a Sensitive Service in accordance with *PCI PTS POI* K22.

4.1.15 MSR K16.2 Salt Storage

Security Requirements	Test Requirements	Guidance
If using a hash function to generate surrogate PAN values, the salt is kept secret and protected appropriately. Disclosure of the salt cannot occur without an attack potential of at least 16 per MSR for identification and initial exploitation, and a minimum of 8 for exploitation, as defined in *PCI PTS POI* Appendix B.	Evaluate and report as required in *PCI PTS POI* DTR K16.2.	This requirement protects the salt from reverse engineering attacks.

4.1.16 MSR K17 Key Management

Security Requirements	Test Requirements	Guidance
The key-management techniques implemented in the MSR must be consistent with *PCI PTS POI* B11.	Evaluate and report as required in *PCI PTS POI* DTR K17	TDES key components should be combined by either XORing of full-length key components or through implementation of a recognized secret-sharing scheme, such as Shamir. Private key components should be combined using a recognized secret-sharing scheme. Generating a check value for a key or key component should be done by a cryptographic process such that all portions of the key or key component are involved in generating the check value. Clear keys or clear-key parts should not be loaded using the service module. An MSR may include more than one compliant key exchange and storage scheme. This does not imply that the MSR should enforce *ANSI X9 TR-31* or an equivalent scheme, but it should be able to implement such a scheme as a configuration option. *ANSI X9 TR-31* support or equivalent should use a key-derivation method. In addition, the MSR may optionally support the key-calculation method. MSR devices should support *ANSI X9 TR-31* or an equivalent method for key loading whenever a symmetric key (AES or TDES) is loaded encrypted by another symmetric key. This applies whether symmetric keys are loaded manually (through the keypad), using a key-injection device, or from a remote host. It does not apply when clear text symmetric keys or their components are loaded using standard dual-control techniques. The MSR also optionally supports *ANSI X9 TR-31* or an equivalent method for the storage of keys encrypted under a symmetric key. Any equivalent method should include the cryptographic binding of the key-usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key should take place within the secure cryptographic boundary of the MSR.

Security Requirements	Test Requirements	Guidance
		(Continued) For all TDEA modes of operation, the three cryptographic keys (K1, K2, K3) define a TDEA key bundle (see X9.24). The bundle and the individual keys should: • Be secret; • Be generated randomly or pseudo-randomly; • Have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source; • Be used in the appropriate order as specified by the particular mode; • Be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged; • Cannot be unbundled for any purpose. Documentation should be provided demonstrating how the method meets these criteria. The evaluating lab may require copies of source code and assistance from the vendor to make a systematic review of relevant security functions. Encryption keys should be used only for their unique purpose: data encryption keys should only be used to encrypt Account data; key-encrypting keys (KEK) should be used only to encrypt keys. Any key calculated as a variant of another key should be protected in a manner equivalent to or greater in security as the original key. AES keys can only be: • Loaded using asymmetric keys of equivalent or greater strength • Encrypted by another AES key of equal or greater strength • Manually loaded using Dual Control techniques • Internally generated using a Random Number Generator compliant with *PCI PTS POI* B9. Remote key distribution using asymmetric techniques should employ mechanisms to protect against MITM attacks.

4.1.16.1 MSR K19 Robustness under Changing Environmental or Operational Conditions

Security Requirements	Test Requirements	Guidance
Changes in environmental or operational conditions must not compromise the security of the MSR, or cause the MSR to output clear text Account data.	Evaluate and report as required in *PCI PTS POI* DTR K19.	To test this security requirements, the MSR could be subjected to temperatures or operating voltages outside the stated operating ranges. The vendor should either provide substantive data to support the product security functions outside of the normal operating conditions; or show that the product uses sensors that will trigger a tamper response under such conditions. The objective is not to replicate vendor testing, but to account for shortcomings in the testing. The tester may rely upon vendor testing as appropriate to fulfill the testing requirements.

4.1.17 MSR K22 Protection of Sensitive Services

Security Requirements	Test Requirements	Guidance
If the MSR supports bi-directional communication and provides access to Sensitive Services or functions, the access to Sensitive Services and sensitive functions must require authentication. Entering or exiting Sensitive Services must not reveal or otherwise affect Sensitive Data.	Evaluate and report as required in *PCI PTS POI* DTR K22.	Sensitive Services provide access to the underlying sensitive functions. Sensitive functions are those functions that process Sensitive Data, such as cryptographic keys, Account data, passwords, and authentication codes. Authentication should require Dual Control techniques when entering Sensitive Data through a secure user interface, or cryptographic techniques when entering electronic data. The use of other techniques to access Sensitive Services prevents the MSR from using existing keying material. A Sensitive Service (state) allows the execution of functions that are not available during normal use. These functions include: • Loading a master key • Deleting stored transactions • Altering the MSR configuration Key components entered manually are considered Sensitive Data during entry. The MSR should not reveal, aurally or visually, the entry of different values.

4.1.18 MSR K23 Sensitive Services Limits

Security Requirements	Test Requirements	Guidance
If the MSR support bi-directional communication and provides access to Sensitive Services or functions, the Sensitive Services are protected from unauthorized use consistent with *PCI PTS POI* B8.	Evaluate and report as required in *PCI PTS POI* DTR K23.	This applies to all transitions to the use of Sensitive Services. The evaluating lab may require copies of source code and assistance from the vendor to make a systematic review of relevant security functions.

4.2 MSR L&M—Device Management

4.2.1 MSR L—During Manufacturing

Security Requirements	Test Requirements	Guidance
The SPoC Solution Provider must meet the security requirements for the following areas: • Change control • Certified firmware control • Device component control • Production firmware control • Post-production storage • Secret information • Component control during design and development • Repair and inspection control	Evaluate and report as required in *PCI PTS POI* DTR Module 5 (L–During Manufacturing).	Verify procedure compliance with the following design evidences: • Evidence of existence—procedures exist and have been implemented. For example, the lab has received procedures from the company that implements the requirement. • Evidence of process output—procedures produce output files (e.g., log files) when in use. Over periods of 3, 6, or 12 months, process output files can be collected randomly and validated. For example, for L2, the lab can randomly select a few occasions and ask for the related log belonging to the Dual Control or standardized cryptographic authentication procedure used.

4.2.2 MSR M—Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment

Security Requirements	Test Requirements	Guidance
The SPoC Solution Provider must meet the security requirements for the following areas: • Shipping tamper-protection documentation • Device-accountability transfer procedures • Shipping security procedures • Development-security documentation • Authenticity of POI security-related components • Authenticity of POI security-related Components for key-loading facility • Unique visible identifier • Operational management manual	Evaluate and report as required in *PCI PTS POI* DTR Module 5 (M – Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment).	Verify procedure compliance with the following design evidences: • Evidence of existence—procedures exist and have been implemented. For example, the lab has received procedures from the company that implements the requirement. • Evidence of process output—procedures produce output files (e.g., log files) when in use. Over periods of 3, 6, or 12 months, process output files can be collected randomly and validated. For example, for L2, the lab can randomly select a few occasions and ask for the related log belonging to the Dual Control or standardized cryptographic authentication procedure used.

5 Validating, Listing and Maintaining SPoC Solutions with MSRs

5.1 Evaluation and Validation

Evaluation of SPoC Solutions that include MSRs as an optional element, should become familiar with identified conflicts between the *SPoC MSR Annex* and the published *SPoC Security and Testing Requirements*. These conflicts include:

- *SR 3.3 Type 1 Attestation and TR B5 Online Processing*. While SCRPs must continue not to support magnetic-stripe read function, the *SPoC Annex* allows for the use of MSRs that meet the Annex requirements. One or more MSRs that meet the *SPoC Annex* requirements are allowed to be physically connected or paired and used with the PIN CVM Application. Other MSRs that are not approved as components of the SPoC Solution continue to be prohibited from physically connecting or pairing with the PIN CVM Application.
- *TB 5.2*—One or more MSRs that meet the *SPoC Annex* requirements are allowed to be paired and used with the PIN CVM Application.
- *TF 1.1 Secure Card Reader*—MSRs that meet the *SPoC Annex* requirements are a permitted method of entry for the Account data.
- *Target of Evaluation*—Allows for the addition of one or more MSRs to the assets under this standard.

While some SPoC Solution testing and validation procedures differ between MSRs and SCRPs (as described in this Annex), an SPoC Solution that includes an MSR uses the same process and program requirements as SPoC Solutions that use SCRPs exclusively. The program requirements and processes are described in sections 3, 4 and 6 of the *SPoC Program Guide.*

5.2 Maintaining a Validated SPoC Solution Listing

Maintaining an SPoC Solution with MSRs will follow the same process and program requirements as maintaining SPoC Solutions with SCRPs, as described in section 5 of the *SPoC Program Guide.*

Validated SPoC Solutions and MSR devices supported by the Solution will be listed on PCI Security Standards Council website. The *List of Validated SPoC Solutions* and its various elements are described in Appendix B of the *SPoC Program Guide*. The **MSRs Supported** field identifies any PTS-listed or non-PTS-listed MSR that has been validated for use with the respective SPoC Solution, and the MSRs approval expiry date, as applicable. An expiry

date that is in the past is denoted by a color change. PTS-listed MSRs include a link to the associated entry on the *List of Approved PTS Devices* on the Website.