Payment Card Industry (PCI)
Software-based PIN Entry on COTS (SPoC)™

Security Requirements

Version 1.1

June 2020

Document Changes

Date	Version	Description
January 2018	1.0	Initial Release
June 2020	1.1	Updated to align with publication of PTS POI v6.0.

Table of Contents

Introduction

Purpose

The purpose of this document is to provide a set of principles, requirements and an evaluation methodology for a mobile payment-acceptance solution where the PIN Cardholder Verification Method (CVM) entry is performed on a Commercial Off-The-Shelf (COTS) device (e.g., smartphone, tablet) in a merchant attended environment.

The security requirements described in this document provide a security risk framework to protect the confidentiality and integrity of sensitive payment information captured and processed on an PIN CVM solution "the solution" operating in a production environment.

Please note: *This standard does not supersede the PCI standards, nor do these requirements constitute a recommendation from the Council or obligate merchants, service providers, or financial institutions to purchase or deploy such solutions. As with all other PCI standards, any mandates, regulations, or rules regarding these requirements are provided by the participating payment brands.*

Audience

The security requirements outlined in this document apply to entities developing PIN CVM applications, evaluator labs, assessors and organizations managing and deploying the solutions.

A separate document, *Software-based PIN Entry on COTS Test Requirements,* is available to provide more granularity and visibility into the testing processes performed by software-based PIN Entry on COTS evaluation laboratories. The security requirements and testing requirements have been developed for specific audiences; therefore, it should be noted that there is not a one-to-one mapping between the documents. The two should be read in combination to fully understand the requirements and the methods for evaluation.

Usage Conventions

This document has been prepared with certain conventions. Within this document, the following terms have a specific meaning when used:

- MUST: Defines a mandatory requirement.
- SHOULD: Defines a recommendation.

Glossary

Term	Definition
AES	Abbreviation for "Advanced Encryption Standard." Block cipher used in symmetric key cryptography adopted by NIST in November 2001 as *FIPS PUB 197* (or *FIPS 197*).
Ahead of Time (AoT) compilation	Compiling of code at some arbitrary time prior to the need to execute the code.
Asymmetric encryption	Also known as public key cryptography. A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can be an encipherment system, a signature system, a combined encipherment and signature system or a key-agreement system. With asymmetric cryptographic techniques, there are four elementary transformations: sign and verify for signature systems, and encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exist asymmetric cryptosystems (e.g., RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and, where used, the four elementary transformations and the corresponding keys should be kept separate.
Attestation	The act of attestation in this standard is the interaction between a verifier (possibly server-based) and a prover (possibly client-based) to determine the current security state/behavior of the prover based on predefined measurements and thresholds provided by the prover.
Attestation system	The set of components that perform attestation processing for the PIN CVM solution. Its components include the PIN CVM application attestation component and the back-end attestation component—the latter works in close association with the back-end monitoring system.
Attestation component	An element of the PIN CVM solution that performs attestation processing.
Authentication	The process for unambiguously establishing the identity of an entity, process, organization or person.
Account data	Account data consists of cardholder data and/or sensitive authentication data.

Term	Definition
Back-end systems	The set of systems providing the server-side functionality of the PIN CVM solution. These functionalities include monitoring, attestation, and transaction processing. In addition, the back-end systems include the IT environments necessary to support the functionalities of the PIN CVM solution.
Cardholder	Customer to whom a payment card or card proxy is issued, or any individual authorized to use a payment card or card proxy.
Cardholder data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See *sensitive authentication data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Cardholder Verification Method (CVM)	A method of authenticating a cardholder during a transaction. Common CVMs include signature, PIN and biometrics.
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data .
Clear text	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as plaintext.
Commercial Off-The-Shelf (COTS) device	A mobile device (e.g., smartphone or tablet) that is designed for mass-market distribution.
Consumer	Individual purchasing goods, services, or both.
Compiling	Translation of computer code from one format into another format. Usually used to take human-readable "source" code and transform this into a format that can be executed by a specific platform or execution environment.
Correlatable data	In the context of this standard, this is data that would facilitate the correlation of a PIN with a separate transaction or database that contains cardholder data such that interception of this data and the entered PIN could reasonably lead to the association of the PIN with its PAN. Examples might include time and date stamps, device identifying information and loyalty program identifiers.
COTS platform	The hardware of the COTS device.
Deterministic Random Number Generator (DRNG)	A deterministic algorithm that generates a sequence of numbers with little or no discernible pattern in the numbers, except for broad statistical properties, which uses a seed value provided by a non-deterministic random number generator.

Term	Definition
Dual control	A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Each entity is equally responsible for the physical protection of materials involved in vulnerable processes. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage and retrieval, dual control requires split knowledge of the key among the entities. No single person can gain control of a protected item or process. Also see *split knowledge*.
ECC	Acronym for "Elliptic Curve Cryptography." Approach to public-key cryptography based on elliptic curves over finite fields.
EMV®	A payment standard that implements cryptographic authentication, published by EMVCo.
EMVCo	A privately owned corporation. The current members of EMVCo are JCB International, American Express, Mastercard, China UnionPay, Discover Financial and Visa Inc.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
Environment	The IT environment supporting one or more functionalities of the PIN CVM solution—such as the IT environment hosting the back-end monitoring system.
Execution environment	The set of hardware and software on which a program is executed. This may be provided through hardware alone, include a combination of hardware and software elements, or be virtualized and implemented in software such that the execution environment can be similarly executed on different hardware platforms.
Full screen mode	Where the PIN CVM application that is currently executing is in control of the primary display and input mechanism(s) of the COTS device. A full screen mode may still include display features that are controlled and/or managed by the COTS OS, but may not include any display from other applications. It is assumed by this standard that full screen mode mitigates the use of any separately controlled or managed displays or input mechanisms to display prompts for data entry, or capture such data entry.
Graphical User Interface (GUI)	A user interface that is provided through images and text.

Term	Definition
Hash	A (mathematical) function that is a non-secret algorithm, which takes any arbitrary-length message as input and produces a fixed-length hash result. Approved hash functions satisfy the following properties: a) One-way – It is computationally infeasible to find any input that maps to any pre-specified output. b) Collision-resistant – It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output. It may be used to reduce a potentially long message into a "hash value" or "message digest" that is sufficiently compact to be input into a digital-signature algorithm. A "good" hash is such that the results of applying the function to a (large) set of values in a given domain will be evenly (and randomly) distributed over a smaller range.
Hash-based Message Authentication Code (HMAC)	A message authentication code that is produced using hash algorithms rather than a symmetric cryptographic algorithm. Defined in FIPS 198-1.
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Just-In-Time (JIT) compilation	Compiling of code immediately prior to the execution of that code.
Key agreement	A key-establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
Key generation	Creation of a cryptographic key either from a random number generator or through a one-way process utilizing another cryptographic key. ***Note:*** *Key variants are not allowed.*
Key installation	Loading of a key that is protected with white-box cryptography, usually embedded within an application.
Key loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.
Key variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.

Term	Definition
Key Check Value (KCV)	A value used to identify a key without revealing any bits of the actual key itself. Check values are computed by encrypting an all-zero block using the key or component as the encryption key, using the leftmost n-bits of the result; where n is at most 24 bits (6 hexadecimal digits/3 bytes TDEA and 5 bytes AES). This method may be used for TDEA. TDEA may optionally use, and AES uses, a technique where the KCV is calculated by MACing an all-zero block using the CMAC algorithm as specified in *ISO 9797-1* (see also *NIST SP 800-38B*). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MAC'd using the TDEA block cipher, while a 128-bit AES key or component will be MAC'd using the AES-128 block cipher. Also known as Key verification check (KVC).
Key wrapping	A format for storage and transmission of symmetric cryptographic keys that embeds metadata about the key type and use, as well as providing cryptographic authentication across the encrypted key and this metadata to ensure that the key and its purpose cannot be altered.
Man-In-The-Middle (MITM) attack	An attack method where a malicious third party interposes between two other communicating parties and modifies the data sent between them.
Mandatory access control	Access control by which the operating system constrains the ability of a process or thread to access or perform an operation on objects or targets such as files, directories, TCP/UDP ports, shared memory segments, IO devices, etc., though an authorization rule enforced by the operating system kernel.
Manual key loading	Loading of a cryptographic key using two or more full-length components or use m of n shares, entered directly through a secure physical mechanism.
MAC	In cryptography, an acronym for "message authentication code." A small piece of information used to authenticate a message.
Mobile device	In the context of this standard, see COTS device.
M of N	An m-of-n scheme is a component or share allocation scheme where m is the number of shares or components necessary to form the key, and n is the number of the total set of shares or components related to the key. Management of the shares or components must be sufficient to ensure that no one person can gain access to enough of the item to form the key alone.
Monitor	In this standard, the "monitor" is an implementation that may be shared across different execution environments, which provides a level of validation and assurance of the execution environment in which the PIN CVM application executes, providing a level of software-based tamper detection and response. The monitor must be capable of being regularly updated to detect and respond to new threats.

Term	Definition
Non-deterministic Random Number Generator (NRNG)	A random number generator that has access to an entropy source and (when working properly) produces output numbers (or bit strings) that have full entropy. Sometimes called a true random number (or bit) generator. Contrast with a deterministic random number generator.
Obfuscation	Protection applied to a process or data through increasing the complexity of interpreting that data. For the purposes of this standard, "obfuscation" refers to "code obfuscation," where computational processes have been applied to increase the complexity of a code set to reduce the ability to reverse-engineer that code.
Offline payment transaction	In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized. Offline transactions are used when terminals do not have online connectivity—e.g., at a ticket kiosk—or in countries where telecommunications costs are high.
Offline PIN verification	A method of PIN verification that sends the PIN entered by the cardholder to the EMV chip on the card.
Online PIN verification	A process used to verify the cardholder's PIN by sending an encrypted PIN value to the issuer or its agent for validation in an authorization request.
Operating System (OS)	System software that manages the underlying hardware and software resources and provides common services for programs. Common operating systems in a COTS environment include, but are not limited to, Android and iOS.
OS store	A digital distribution service operated by the COTS OS vendor or by the COTS device manufacturer.
PCI DSS	The Data Security Standard published and maintained by the Payment Card Industry Security Standards Council. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.
PCI PIN	A PCI standard that contains a complete set of requirements for the secure management, processing and transmission of Personal Identification Number data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.
Personal Identification Number (PIN)	A numeric personal identification code that authenticates a cardholder. A PIN consists only of decimal digits.
PIN CVM application	All parts of the code, regardless of execution environment, that are installed and executed on the merchant COTS device for the purposes of accepting and processing the cardholder's PIN The client-side monitor and/or a payment application may be incorporated into the PIN CVM application or may be a separate application.

Term	Definition
PIN CVM solution ("the solution")	The set of components and processes that support the entry of PIN data into a COTS device. At a minimum, the solution includes SCRP, PIN CVM application, and the back-end systems and environments that perform attestation, monitoring, and payment and online PIN processing.
Physical Unclonable Function (PUF)	An intrinsic value or transformation that can be provided by a system that is a function of some physical process, such that it cannot be replicated or altered.
PIN block	Defined formats used for offline and online PIN processing and transmission, as defined in ISO 9564 Part 1.
Private key	A cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.
Public key	A cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and may be made public. In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to all members of a pre-specified group.
Public key cryptography	See *asymmetric encryption*.
Random Number Generator (RNG)	The process of generating values with a high level of entropy and that satisfy various qualifications, using cryptographic and hardware-based "noise" mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
Replay attack	A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
RSA	An asymmetric encryption algorithm that was defined by the cryptographers Rivest, Shamir, and Aldeman.
Secure boot	See *trusted boot.*
Secure Card Reader – PIN (SCRP)	A physical card reader that has been assessed compliant to the PCI PTS SCRP Approval Class and is listed on the PTS approval website.
Secure channel	A cryptographically protected connection between two processing elements.

Term	Definition
Secure Cryptographic Device (SCD)	A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms. Examples include ANSI X9.24 part 1 or ISO 13491.
Secure Reading and Exchange of Data (SRED)	Requirements contained in the PCI PTS POI Standard, detailing the security controls for devices that protect account data.
Sensitive authentication data	Security-related information—including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN blocks—used to authenticate cardholders and/or authorize payment card transactions.
Sensitive data	For the purposes of this standard, sensitive data is cryptographic materials—e.g., keys, certificates, cardholder PINs or cardholder data.
Sensitive services	Those functions that affect underlying processes that support the protection of sensitive data—e.g., cryptographic keys, PINs and cardholder data.
Split knowledge	A condition under which two or more entities separately have key components or key shares that individually convey no knowledge of the resultant cryptographic key. The information needed to perform a process such as key formation is split among two or more people. No individual has enough information to gain knowledge of any part of the actual key that is formed.
Software protection mechanisms	Methods and implementations used to prevent the reverse engineering and modification of software. See *obfuscation* and *white-box cryptography* as examples of commonly used software protection mechanisms.
Solution provider	An entity that develops, manages and/or deploys PIN CVM solutions.
Supported platform	The current operating system supported by the operating system vendor.
Symmetric encryption	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption. Also known as “secret key.”
Tamper-detection	The automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module.
Tamper-responsive	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
TDES	An algorithm specified in *ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. (PIN)*

Term	Definition
Test Requirements (TR)	Requirements that dictate the set of tests that must be performed to confirm compliance with a specific standard.
The solution	See *PIN CVM solution*.
Third-party app stores	App stores that are not supported by the COTS OS vendor and are not pre-installed by the device manufacturer.
True Random Number Generator (TRNG)	A device that generates random numbers from a physical process, such as a PUF, rather than a deterministic algorithm.
Trusted boot	A cryptographic process where the bootloader verifies the integrity of all components (e.g., kernel objects) loaded during operating system start-up process, before loading. Also known as Verified Boot and secure boot (e.g., Google or Apple).
Trusted Execution Environment (TEE)	A Trusted Execution Environment provides security features such as isolated execution environment for trusted applications ("Trustlets"). It protects security assets from general software attacks, defines safeguards as to data and functions that a program can access and resists a set of defined threats.
User Interface (UI)	The set of the human-machine interfaces that allows for interaction between a person and a computerized system.
White-box cryptography	A method used to obfuscate a cryptographic algorithm and key with the intent that the determination of the key value is computationally complex.

Publications and References

PCI SSC Standards https://www.pcisecuritystandards.org/document_library	
DSS	Data Security Standard
DESV	Designated Entities Supplemental Validation (Appendix A3 in PCI DSS v3.2)
HSM	PIN Transaction Security (PTS) Hardware Security Module Security Requirements
PA-DSS	Payment Application Data Security Standard
PIN	PIN Security Requirements
POI	PTS Point of Interaction Modular Security Requirements

Other Industry Security References	
CERTSECCODE	SEI CERT Coding Standards – https://www.securecoding.cert.org
OWASPMOB10	*OWASP Mobile Security Project – Top Ten Mobile Risks* https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
OWASPMOB2015	OWASP Mobile Security Project – 2015 Scratchpad https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-2015_Scratchpad
SCSECSWDEV	The Ten Best Practices for Secure Software Development https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/ Certification Programs/CSSLP/ISC2_WPIV.pdf
ANSI X9.24	Retail Financial Services Key Management
FIPS 140-2	Federal Information Processing Standard, Security Requirements for Cryptographic Modules
FIPS 186-4	Federal Information Processing Standard, Digital Signature Standard (DSS)
FIPS 198-1	Federal Information Processing Standard, The Keyed-Hash Message Authentication Code, (HMAC)

Other Industry Security References	
FIPS PUB 197 (or "FIPS 197")	Federal Information Processing Standards Publication 197 ADVANCED ENCRYPTION STANDARD (AES)
ISECOM	Institute for Security and Open Methodologies
ISSEA SSE-CMM	International Systems Security Engineering Association Systems Security Engineering Capability Maturity Model
ISO 11568	Financial Services, Key Management
ISO 13491	Financial Services, Secure Cryptographic Devices
ISO 16609	Banking Requirements for message authentication using symmetric techniques
ISO 9564-2	Financial services -- Personal Identification Number (PIN) management and security -- Part 2: Approved algorithms for PIN encipherment
ISO 9564-1	Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems
ISO/IEC 11770	Information technology -- Security techniques -- Key management
ISO/IEC 18031	Information technology -- Security techniques -- Random bit generation
ISO/IEC 18033-3	Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers
ISO/IEC 21827	Federal Information Processing Standard, Advanced Encryption Standard
MITRE's Common Vulnerabilities and Exposures list	MITRE Common Vulnerabilities and Exposures database
NIST SP 800-38B	National Institute of Standards and Technology, Special Report on Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication
NIST SP 800-52	National Institute of Standards and Technology, Special Report on Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST SP 800-57	National Institute of Standards and Technology, Special Report on Recommendation for Key Management, Part 1: General (Revision 3)
NIST SP 800-22	National Institute of Standards and Technology, Special Report on A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Other Industry Security References	
NIST Special Publication 800-90A	National Institute of Standards and Technology, Special Report on Recommendation for Random Number Generation Using Deterministic Random Bit Generators
NIST Special Publication 800-130	National Institute of Standards and Technology, Special Report on Framework for Designing Cryptographic Key Management Systems
NIST's National Vulnerability Database	National Institute of Standards and Technology National Vulnerability Database
Open Source Security Testing Methodology Manual (OSSTMM)	http://www.isecom.org/research/osstmm.html
U.S. Department of Homeland Security's US-CERT	United States Computer Emergency Readiness Team

Scope of Requirements

These security requirements apply to the individual components and processes that make up the production Software-based PIN CVM solution, referred to as "the solution," that allows a cardholder to enter their PIN into a COTS device for authorization of contact or contactless EMV card payment transactions presented to the SCRP.

Software-based PIN entry (online or offline PIN) is only permitted for contact and contactless EMV chip transactions processed online. Offline payment transactions are prohibited, e.g., EMV offline transaction authorization or batch authorizations.

Solutions may optionally include magnetic-stripe readers that meet the security and testing requirements detailed in Payment Card Industry (PCI) Software-based PIN Entry on COTS Magnetic Stripe Readers Annex. Software-based PIN entry is not permitted for magnetic stripe read transactions.

Overview

Background

In traditional merchant payment PIN entry scenarios, cardholder authentication data—e.g., a PIN—is entered into a device specifically designed for the protection of PIN data—e.g., a PIN entry device (PED). The payment industry recognizes PEDs that have been independently tested and comply with detailed security requirements developed by PCI to ensure the confidentiality, integrity and availability of the PIN data. Traditional PEDs rely on hardware protections as the primary mechanisms to ensure the security of PIN data within the device. Merchants use traditional PEDs to support cardholder PIN acceptance.

Mobile payment acceptance enables the processing of payment transactions, e.g., using a smartphone or tablet, that performs the functions of an electronic point-of-sale terminal. Software-based PIN entry solutions allow for the processing of mobile payment-acceptance transactions with a cardholder's PIN.

Software-based cardholder authentication provides an alternative for chip and PIN markets by providing a software application interface on a merchant's COTS device to capture and process a cardholder's PIN. These solutions rely on a combination of mechanisms and security controls including but not limited to device hardware, application software and independent management and oversight of the entire process to ensure the security of the transaction and PIN data.

The following figure highlights the security model differences (and reliance on controls) between a traditional PED implementation (hardware PIN) and a software-based PIN entry solution (software PIN) for the protection of PIN data.

Security Model – Traditional Hardware-based PIN Entry vs. Software-based PIN Entry

In a hardware-based PIN entry security model, the protection of the PIN is primarily the responsibility of the specialized PED hardware and software (including the firmware). Some hardware-based solutions may utilize back-end systems to supplement their security posture; however, traditional hardware PIN entry devices have all protections within the device itself. Detection mechanisms that identify when security controls are not in an approved state operate within the PED, and the response for the hardware security model is to disable the PED from processing PIN-based transactions and to clear all sensitive data from the device. All PIN security protections are performed within the PED itself.

In a software-based PIN entry security model, the device where the PIN is entered and initially protected remains an important component. In addition, mechanisms that support attestation (to ensure the security mechanisms are intact and operational), detection (to notify when anomalies are present) and response (controls to alert and take action), play an equally significant role in the overall software-based PIN entry solution security model. Furthermore, having the device connected online provides opportunities to extend these capabilities to back-end monitoring systems.

There are, however, individual components of a software solution where there is limited control—for example, the underlying mobile device hardware platform and OS. Given that these are COTS devices, there is an assumption that these components (e.g., COTS OS, configuration of hardware components of a phone, etc.) are unknown or untrusted.

It must be assumed that an attacker has full access to the software that executes on any unknown or untrusted platform (where that "software" may be a binary executable, interpreted bytecode, etc., as it is loaded onto the platform). Therefore, it is considered important for the software to provide inherent protections that complicate reverse engineering and tampering of the code execution flow. This may include, but is not limited to, protections using "obfuscation" of the code, internal integrity checks for code and processing flows and encryption of code segments, etc.

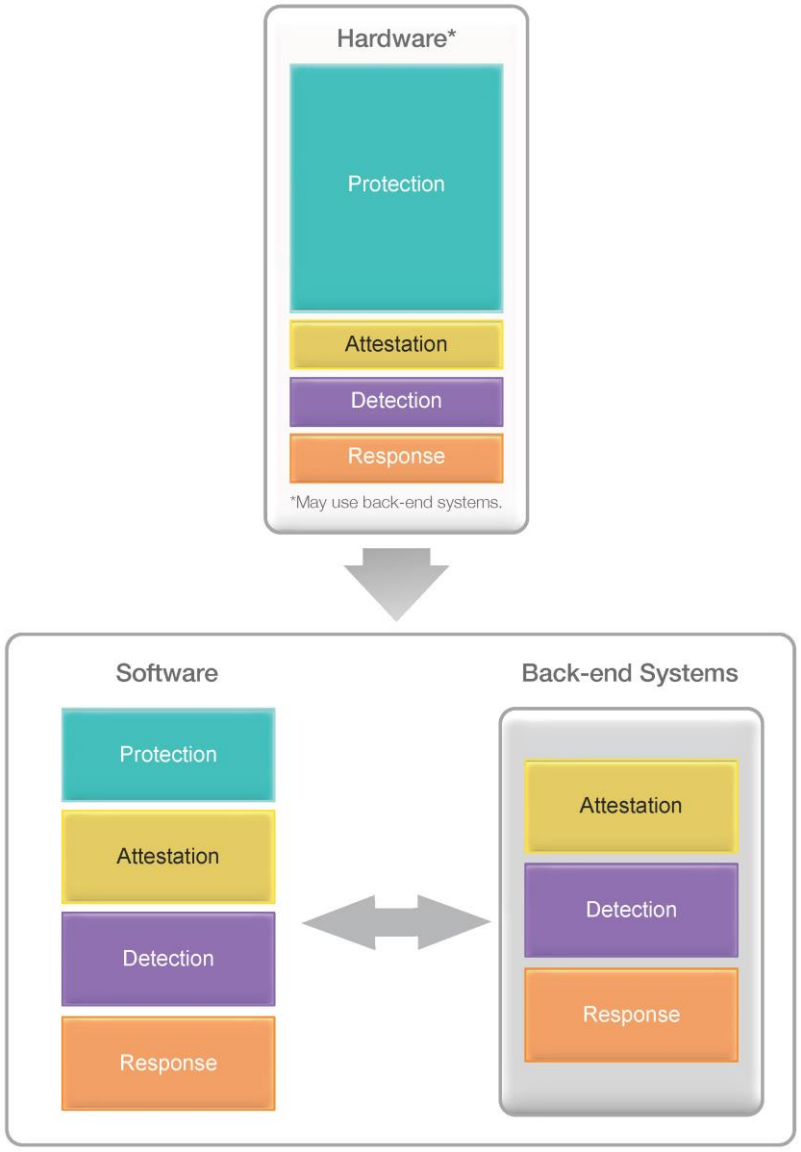


Figure 1: Hardware-based and Software-based PIN Entry

Software-based PIN entry architecture relies upon the following components that combine to provide for protection, attestation, detection and response controls:

1. An SCRP device that supports the solution. The SCRP is SRED-enabled and connected to the COTS device. The SCRP provides:
   a. Protection of cardholder data sourced from the payment instrument
   b. Decryption of encrypted PIN data received from the PIN CVM application
   c. Translation of PIN data into required PIN-block format (This would only apply to online PIN verification processing.)
   d. Re-encryption of PIN data
2. A PIN CVM application that resides on the COTS device and:
   a. Provides a secure UI for PIN entry
   b. Performs initial encryption of the PIN
   c. Passes attestation health-check data about the SCRP, COTS platform, and PIN CVM application to the monitoring environment
   d. Contains software protection mechanisms to maintain its own integrity against attack
   e. Delivers the encrypted PIN to the SCRP to be decrypted/re-encrypted in order for it to be passed to the back-end monitoring and attestation systems
3. A COTS device that is operated by the merchant to run the PIN CVM application as well as the SCRP. The COTS may have a TEE built in but it is not a requirement.
4. A set of back-end systems that perform functions for the The solution such as:
   - Attestation
     Processes attestation health-check data from the PIN CVM application and enforces pre-established security policies
   - Monitoring
     Monitors and provisions security controls to detect, alert and mitigate suspected or actual threats and attacks against the SCRP, PIN CVM application, and the COTS device
   - Processing
     Processing environment that receives encrypted cardholder and PIN data (for online PIN) from the SCRP

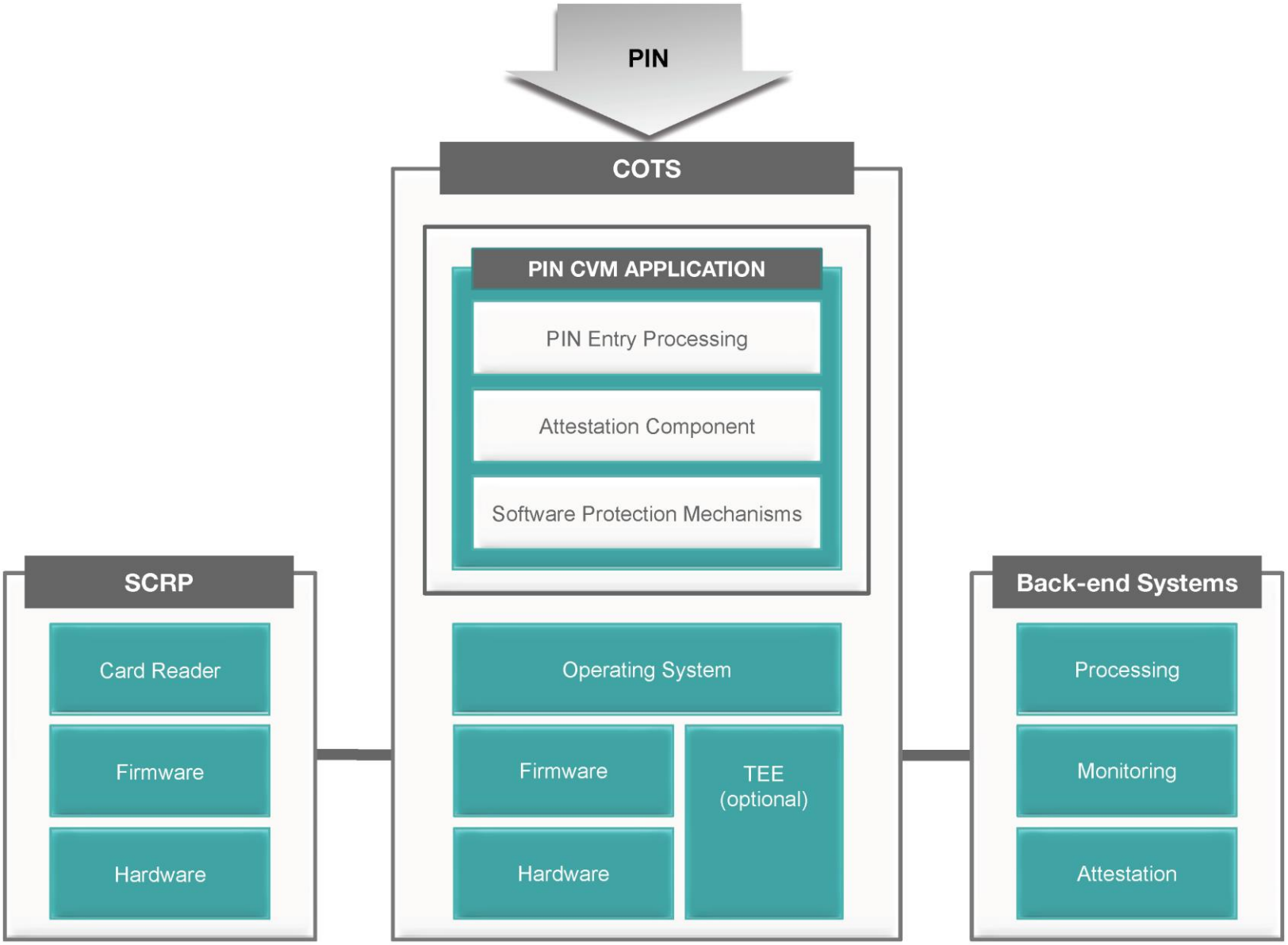


Figure 2: Example of PIN CVM Solution Architecture

Software-based PIN Entry Solution Overview

The following diagram illustrates the flow of a PIN transaction in a software-based PIN entry solution. Steps 1-7 are detailed on the following page.

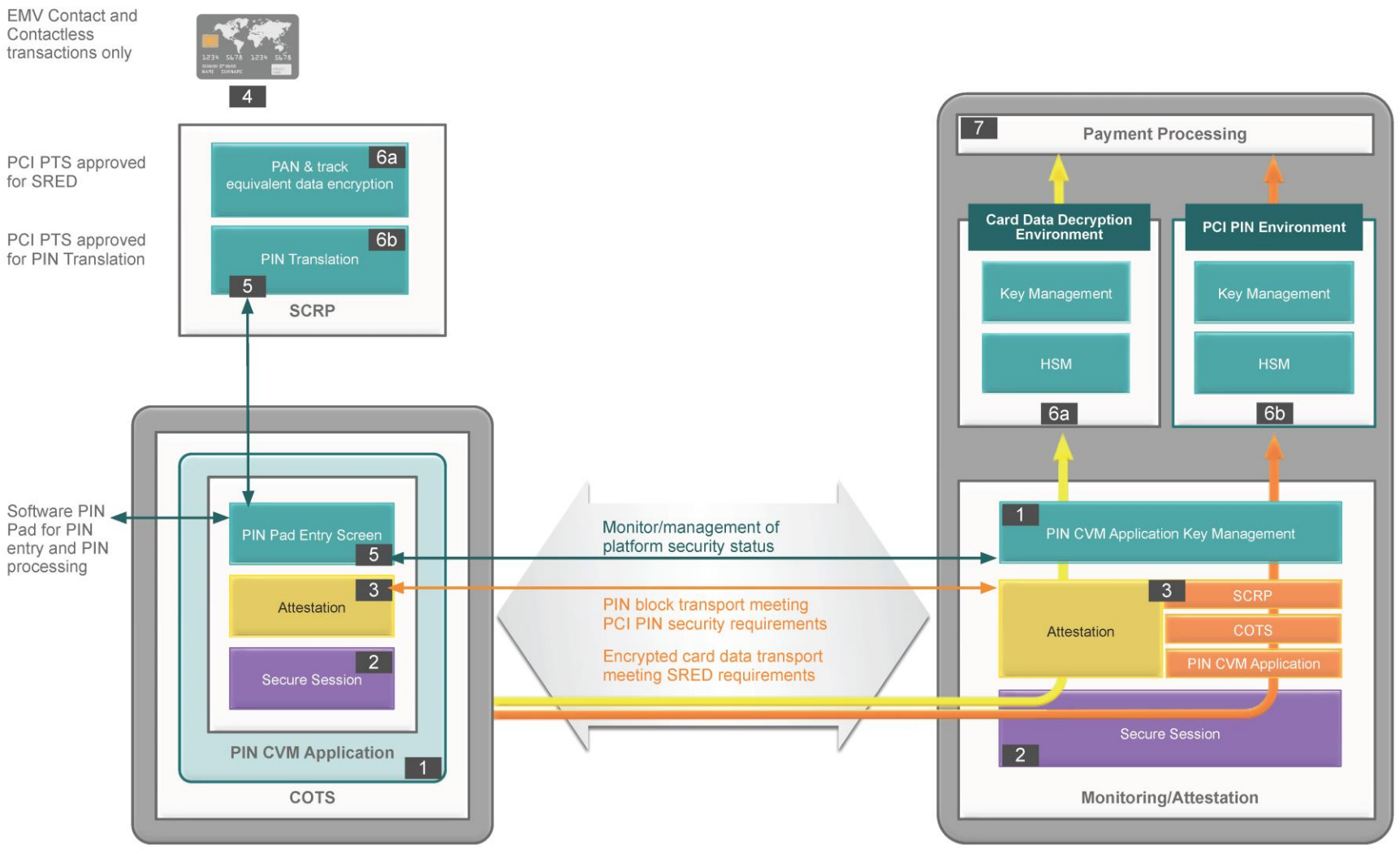


Figure 3: Software-based PIN Entry Solution

1. PIN CVM application and SCRP are initialized with their financial keys (this may be asynchronous with the transaction).
2. A secure communication channel between the PIN CVM application and the back-end monitoring system is established.
3. The back-end monitoring system determines the security status of the mobile payment-acceptance platform (SCRP, COTS platform, and PIN CVM application) using the attestation component.
4. An EMV card, contact or contactless, or an NFC-enabled mobile EMV payment device is presented to the SCRP.
5. The PIN CVM application PIN entry component renders a PIN entry screen on the COTS platform and the cardholder enters their PIN using the rendered PIN pad from the PIN CVM application. The resulting information is enciphered and sent to the SCRP by the PIN CVM application.
6. The SRED component of the SCRP enciphers the account data using preloaded data-encryption keys according to either Figure 4 (online PIN verification) or Figure 5 (offline PIN verification) below.
7. The payment transaction is processed.

Figure 4: Online PIN Verification

– An enciphered PIN block is generated by the SCRP component (online PIN processing, contact and contactless EMV) using preloaded PIN-encryption keys.

– The SRED data and enciphered PIN block (online PIN processing only) are transmitted to an HSM within the back-end payment processing system.

– OR –

(See following page)

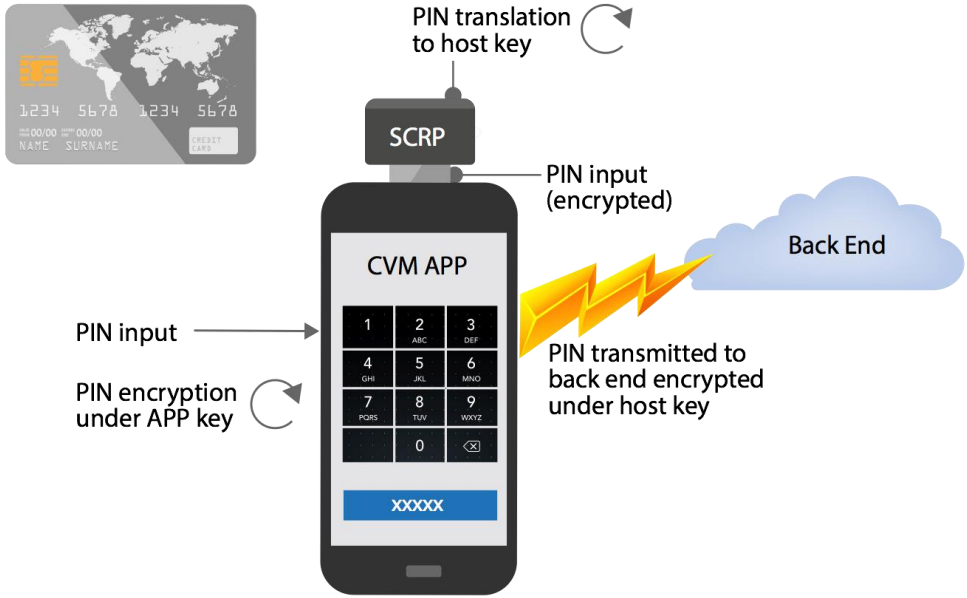
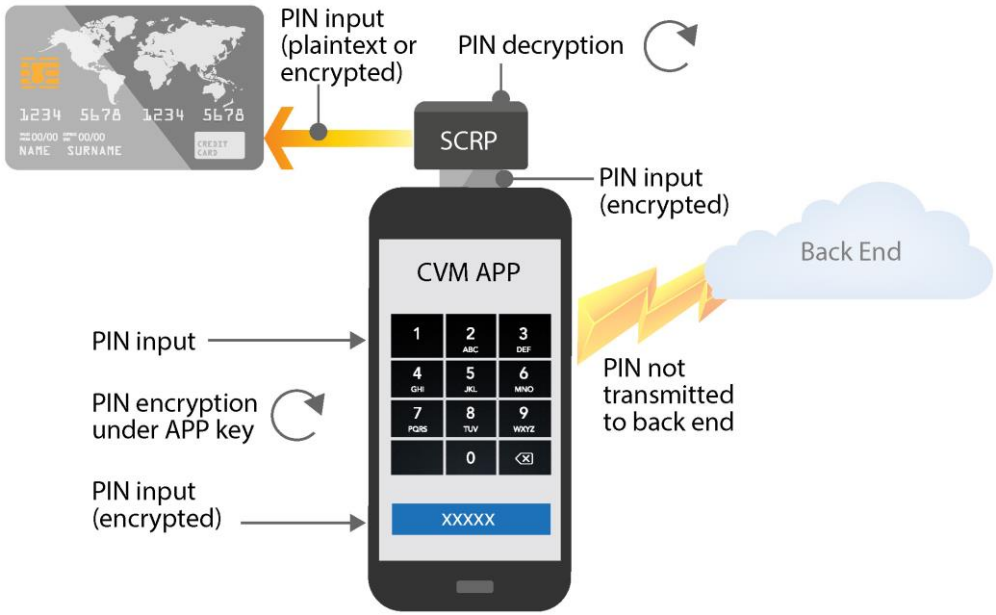


Figure 5: Offline PIN Verification

- The SCRP performs offline PIN verification (contact EMV only).
- The SRED data is transmitted to an HSM within the back-end payment processing system.



Security Objective and Assets

Security Objective

The objective of these security requirements is to provide reasonable assurance that Software-based the solutions provide adequate security mechanisms, controls and mitigations to protect the consumer's cardholder data, PIN, and other assets—e.g., cryptographic keys, correlatable data, etc.—from unauthorized disclosure, modification or misuse by providing an attack surface that may be perceived as uneconomic for an attacker to penetrate.

It is recognized that an attacker may have other objectives—e.g., self-promotion, nation-state attack, etc.—and may expend more resources to circumvent established controls than is warranted by the direct financial fraud payback.

For the COTS components, the objective of these security requirements is to provide reasonable assurance that these components have been kept up to date and have not been modified from what had been deployed by the COTS provider.

Security Assets

There are a number of assets to be protected within the payment ecosystem—for example PIN, PAN, and full-track-equivalent data. The Payment Card Industry Security Standards Council (PCI SSC) defines security requirements for the protection of this data as well as the protection of other sensitive assets, such as cryptographic keys used to protect cardholder data and PIN data. There may be additional assets that require protection as determined by national or regional regulations—e.g., personally identifiable information (PII). Protection of these additional assets is out of scope of these requirements.

Assets are categorized as requiring one or more security services: confidentiality (C), integrity (I), and integrity with the addition of auditability/authentication (I+). The solution provider may identify other security services, for example confidentiality of binaries. The following are assets to be protected by the solution. The solution provider may implement additional controls for other assets not referenced in this list.

Security Assets	Security Services
Account data	C and I
Attestation data	C and I+
Cryptographic keys and related parameters (static and ephemeral) used for communications processing and to secure transport to/from the COTS device.	C and I+
PIN CVM application	C and I+
PIN data	C and I
Private and secret keys or session keys and related parameters (static and ephemeral) used during PIN processing and cardholder data encryption.	C and I

Security Requirements and Guidance

The following security requirements have been defined to address attack scenarios known at time of publication.

As detailed in the requirements, solution providers have ongoing responsibility to proactively perform risk assessments to identify potential flaws or gaps that may be introduced into software-based PIN entry scenarios that may be associated with changes in technology or identification of new threats and vulnerabilities.

A guidance column is provided to describe the intent or security objective behind each of the security requirements. This column contains guidance only and is intended to assist with understanding the intent of each requirement. The guidance in this column does not replace, limit or extend the actual security requirement.

The requirements defined in this standard have been grouped into modules (see table below) to align with major components that support the security of the overall solution and to support security evaluations if components are the responsibility of different organizations.

Module	Title	Description
1.	Core Requirements	General requirements that define security controls applicable to the overall solution. The solution provider is responsible to ensure these requirements are in place.
2.	PIN CVM Application	The PIN CVM application requirements apply to the software application(s) that reside on the COTS device and communicate with the SCRP and the back-end attestation component and back-end monitoring systems. The PIN CVM application is responsible for displaying the PIN entry screen, masking entered PIN values in the display, initial encryption of the entered PIN, collecting and reporting attestation information.
3.	Back-end Systems – Monitoring/Attestation	The back-end monitoring system supports the management of the solution. It interacts with the PIN CVM application on the COTS device and facilitates detecting anomalous and potentially fraudulent activity, including suspicious transactions. The back-end attestation ensures that the required security controls and mitigation mechanisms on the COTS device, SCRP, and functions within the PIN CVM application that are necessary to protect cardholder and PIN data are intact and functioning as intended. The back-end attestation component requires integration with the PIN CVM application to send the attestation data to it.
4.	Solution Integration Requirements	Overall oversight, governance and responsibility of the solution is necessary to ensure all security controls are in place and functioning as intended. The solution provider is responsible for ensuring these requirements are implemented.
5.	Back-end Systems – Processing	The back-end payment processing systems are the processes/environments that perform and complete PIN and payment processing.

Module 1: Core Requirements

Control Objective: *All solution security requirements must work in concert to protect the cardholder's PIN and support a secure mobile payment-acceptance transaction.*

If applicable, all parties involved in the solution are required to adhere to stated requirements in this section. The solution providers are ultimately responsible for ensuring the stated requirements are met.

All components of the solution must meet the requirements in Core Requirements module.

1.1 Protection of Sensitive Services

Requirements	Guidance
Sensitive services are those functions that affect underlying processes that support the protection of sensitive data—e.g., cryptographic keys, PINs and cardholder data. All sensitive services ***must be identified and support the confidentiality, integrity, and availability of the solution****. Entering or exiting sensitive services must not reveal or otherwise affect sensitive data.*	
1. Documentation detailing all sensitive services implemented by the components and solution must exist and be updated as necessary, or at least annually. At a minimum, this must include key loading (for all in-scope areas), signing of applications and SCRP firmware and signing of updates to the monitor services or configuration.	*Proper identification of processes and functions that are fundamental to the security of the solution is necessary to ensure common understanding and assist with identifying roles and responsibilities for proper management and security of these processes and/or functions. Without this information, implementation of security controls may be overlooked which could lead to unauthorized disclosure or compromise of the solution.*
2. A dual-control process must exist for the generation of cryptographic keys used for digital signatures to verify the authenticity and integrity of security assets.	*Use of COTS devices introduces additional risks as it relates to privacy, unauthorized disclosure and exposure to vulnerabilities. Therefore, it is imperative that trust is established through the use of digital signatures to ensure the solution components know which other components are authentic and the data exchange to and from components is intact and has not been altered. Use of dual control and cryptographic keys further enhances the trust of digital signatures by ensuring the processes to create the digital signatures conform to industry acceptable practices. Refer to Appendix C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms for more information.*

1.2 Random Numbers

Requirements	Guidance
Random numbers must be generated using a process that ensures sufficient entropy (as defined in NIST SP800-90b) and lack of statistical correlation. *This applies to all components and parts of the solution where random numbers are generated for security functions.*	
1. Documentation to identify all random number generation functions and reliance on random data used in the solution must exist and be maintained.	*Identification of all security functions implemented within the solution that require or rely upon the use of random data is necessary to ensure the process used is sound and cannot be circumvented since cryptography depends on the creation of secret data that is known to only those that have a need to know and unknown and unpredictable to others. random number generation sets the security baseline that other security controls rely upon. This may include the generation of padding data (for example, for use in certificates, key bundles, EMV unpredictable numbers, or offline encrypted PIN blocks), generation of cryptographic keys, randomization of the keypad, etc.* *Random generator attacks used by malicious users seek out weak random number implementations and have been the cause of a number of high profile vulnerabilities, therefore the quality of the random numbers generated by the system is vital.*
2. Any random numbers used on the COTS device for security purposes must be seeded from a value provided from the RNG on the SCRP that has been validated through PCI PTS testing. ***Note:** This excludes the establishment of secure communication protocols where the use of the native OS RNG is out of the control of the PIN CVM application.*	*Sufficient entropy is not assured in COTS devices (e.g., NIST SP800-90b), therefore confirmation that the secret value, e.g., seeded value, is from a trusted and tested source such as the SCRP is necessary and the seed length is at least 256-bits. A PCI PTS SCRP is a hardware security component that has been independently tested to ensure it meets the most stringent of requirements. Combination of the seeds should ensure that entropy of the seeds is maintained. An example of how this might be done is XOR'ing the two seed values. This may be combined with a further seed generated on the COTS platform.* *The random number seed obtained from the SCRP may be used by the white-box DRNG to generate any cryptographic keys or random numbers required by the PIN CVM application. However, each time the PIN CVM application is started, it should be re-seeded from the SCRP. The seed value should never be stored in non-volatile memory.*
3. Random number generation used by the PIN CVM application must utilize a PRNG that was originally seeded by a random seed provided by the SCRP. It must not be possible to replay or reuse the same seed except by chance.	*The secret value (e.g., random seed) used by the PIN CVM application random number generation process is critical to ensure appropriate entropy for the process as well as protect against the ability to obtain the key itself. The PIN CVM application may have limited controls due to the nature of software; therefore, the PIN CVM application relies on obtaining the initial random seed from a SCD that has had trust established. An SCRP provides the required high confidence and trust.*

1.2 Random Numbers

Requirements	Guidance
4. The PIN CVM application must use an assessed RNG where cryptographic algorithms require the use of random numbers.	*RNGs come in two types: DRNG and NRNG. A DRNG depends on an initial seed value, provided by an NRNG, from which it generates pseudo random numbers. In this case, the seed value comes from the SCRP.* *Vendors should avoid implementing their own DRNG and where possible implement well known sources or algorithms as specified in NIST 800-90a.* *The PIN CVM application RNG should be tested for fitness of purpose against a known standard (e.g., NIST 800-22, NIST 800-90a).*
5. Any random numbers used on a back-end system for security purposes must be seeded from a value provided initially from the RNG on at least a FIPS 140-2 Level 3 or PCI-approved HSM. **Note:** *Random numbers that are not directly relied upon for security of the customer PIN, cardholder data, or monitoring/attestation data—e.g., random values used in TLS sessions, where the data being transmitted is otherwise protected using application level cryptography—do not need to meet this requirement.*	*RNG generation performed in a FIPS 140-2 Level 3 (or above) or PCI-approved HSM that has been independently tested ensures the process meets the most stringent of requirements.*

1.3 Acceptable Cryptography

Requirements	Guidance
Cryptography is an important factor to ensure confidentiality and integrity of data and processes that support the solution; therefore, it is important that only industry-recognized standard cryptographic algorithms and implementation methodologies be the basis for any security services used in the solution. *This applies to all components and processes used in the solution.*	
1. Documentation must exist to identify cryptographic processes and operations used by the solution for security services. At a minimum, documentation must include the following: • Cryptographic algorithms used and where • Identification of all keys, the complete key hierarchy, their purposes and crypto periods • Key-generation or key-agreement processes	*Information that identifies cryptographic operations used in the solution assist with ensuring controls are appropriately tested as well as identify areas where cryptography may be beneficial to increase the solution's security assurance. Comprehensive documentation that includes (but is not limited to) cipher suites or other cryptographic algorithms implemented includes transport layer protocols that are used for secure channels.*
2. All security services provided by the solution must adhere to Appendix C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	*Use of recognized cryptographic methods provides assurance that the solution adheres to industry-tested and accepted algorithms, along with appropriate key lengths that provide effective key strength and proper key-management practices. Proprietary or "home-grown" algorithms do not provide this assurance and are not permitted.* *Refer to industry standards and best practices for information on cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).* *The solution should utilize the most robust and current encryption algorithms and key sizes to withstand modern day attacks and ensure support into the future. Legacy algorithms have a shelf life and may lose some of their effectiveness over time.*

1.3 Acceptable Cryptography

Requirements	Guidance
3. Where key-derivation methods are used for creating a unique key, the method must not be reversible (e.g., using XOR operations only) and provide perfect forward secrecy.	*While the Base Derivation Key (BDK) does not provide for forward secrecy, the use of derived unique key per transaction (DUKPT) as a key-management method does provide forward secrecy. The Initial PIN Encryption Key (IPEK) creates a set of keys that are irreversibly derived from it. The actual keys used for PIN encryption are these keys, each of which is only used once. The compromise of any one of these keys does not compromise future or past data encrypted by any other derived key. The BDK is created within and only resides within an HSM. The IPEK is securely loaded into an SCD (in the case of this standard, the SCRP), is unique to the SCD and never leaves the SCD. As long as the BDK and IPEK remain secure, DUKPT as a key-management method meets the requirement for forward secrecy as specified in this standard.*
4. Hash functions must be implemented in accordance with Appendix C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	*Use of hash functions ensures the integrity of data and since hash functions are based on mathematical and cryptographic functions, use of recognized, accepted methods is necessary. This does not preclude the use of other hash types, such as MD5, where collision resistance is not required as a security feature.*
5. Encryption used to protect PIN data or tamper-detection data must be performed using a key that is unique per transaction/communication session and per PIN CVM application instance.	*Requiring unique keys per transaction and communication session ensures that in the event the keys were compromised they could not be used in subsequent transactions.*
6. All messages that are communicated between components in the solution must use a unique key per session.	*Replay attacks occur when a malicious user is able to reuse session keys for multiple messages. Requiring unique keys per session thwarts this type of attack.*
7. Security must not be provided to any key by a key of lesser strength.	*Encryption keys lose their strength when protected by a key of lesser strength, making it easier for malicious users to perform attacks against the weaker key to reveal its content. For example, assume a data-encryption key is created with 256-bit AES security, which is considered a strong key and can with high probability withstand current data attacks. However, if that same data-encryption key was then transported with a key-encryption key (KEK) that was only 128-bit AES key strength, the data-encryption key has then lost its strength and is providing only 128-bit of security—making it much more vulnerable to attack.* *Organizations should always consider this when managing keys to avoid inadvertently lessening the key strength.*

1.3 Acceptable Cryptography

Requirements	Guidance
8. Public keys/certificates used by the solution must be signed or MAC'd. The integrity and authenticity of the key must be ensured. Mechanisms must be in place to identify expired certificates and prevent continued processing when certificates are expired.	*Public keys/certificates due to the nature of their use, are public and may be sent and received in clear text. Requiring encryption to preserve the confidentiality of the public key/certificate is not required. However, it is important that the public key is protected to ensure it is genuine (authentic) and has not been substituted or altered (integrity). Digital signatures or message authentication codes, e.g., MAC, are methods that provides this assurance.* *Self-signed certificates that exist as part of the base COTS platform on which the PIN CVM application is executed are excluded from this requirement. However, the self-signed certificates must not be relied upon for security services by the PIN CVM application unless the integrity and authenticity of the key is ensured.* *Expired certificates introduce unacceptable risk to the solution. Primarily expire certificates could be an indication of a malicious user being an imposter of a legitimate organization/process which may associated with phishing for sensitive information.*
9. Each key must have a single unique purpose, and no keys may be used for multiple purposes (such as both signing and encrypting data).	*Keys used to encrypt PIN data should not be used for any other operation (such as general-purpose data encryption, or monitor message encryption, etc.). Requiring unique keys for dedicated purposes ensures that in the event a key has been compromised the exposure is limited.*
10. Keys used to validate authenticity must be unique to each end point so that an (H)MAC or signature generated at one end would always be different if generated by the other end point.	*(H)MAC or digital signatures protect against tampering of the message and impersonation so there is assurance that the information contained in the message is intact and was not intercepted or altered in transit. Ensuring unique keys are used for each endpoint further enhances this protection by limiting exposure in the event the key was compromised to only the affected endpoint and not the entire population.*
11. Any key "signature" or "fingerprint" values returned by the system must not reveal any details about the key itself.	*Since the secrecy of the encryption key is paramount to the overall security, a key signature or fingerprint is the value that is shared between organizations to ensure the key that was conveyed is the key that was received. Key signatures or fingerprints require this value that is shared to be public therefore, the key signature and fingerprint is created in a way that would not disclose information about the underlying encryption key or be allowed to be used to reverse-engineer the value of the key itself.*
12. KCVs must be limited to five bytes or less, and hash algorithms used for key fingerprints (on secret or private keys) must implement SHA256 or stronger (or be truncated to no more than five bytes).	*Key-check values (KCVs)—also referred to as key-verification checks (KCVs)—are values that are produced as a result of a key-generation process. Since encryption keys cannot be in clear text, KCVs provide a mechanism to validate the authenticity of a key without disclosing specific information about the key itself. Limiting the number of bytes for the KCV ensures that the ability to retrieve the underlying clear-text key value from the KCV is greatly reduced.*

1.4 Key Management

Requirements	Guidance

Successful key management is critical to the security of cryptographic systems. It is a fundamental factor for ensuring the confidentiality and integrity of data and processes that support the solution. Hardware key-management practices must conform to industry-accepted practices as described in this section.

Where software encryption is used—e.g., white-box cryptography—key-management practices must adhere to requirements specified in Module 2 of this standard.

Cryptographic keys are securely managed using recognized industry requirements throughout the cryptographic lifecycle including, but not limited to:

1. *Generation*
2. *Distribution/conveyance*
3. *Storage*
4. *Established crypto periods*
5. *Replacement/rotation when the crypto period is reached*
6. *Escrow/backup*
7. *Key compromise and recovery*
8. *Emergency procedures to destroy and replace keys*
9. *Accountability and audit*

This applies to the following components in the solution: the PIN CVM application and all relative back-end systems (attestation component, monitoring and processing).

1.4 Key Management

Requirements	Guidance
1. Documentation, including procedures, must exist to support all key lifecycle management functions used by the solution.	*A good key-management process, whether manual or automated, is based on industry standards and addresses all elements of the key lifecycle that include, distribution/conveyance, storage, established crypto periods, replacement/rotation when the crypto period is reached, escrow/backup, key compromise and recovery, emergency procedures to destroy and replace keys and accountability and audit.* *For example, the generation should conform to industry-recognized procedures that ensure the confidentiality of the underlying key. Keys should only be distributed in a secure manner, never in the clear and only to designated custodians or recipients. Procedures for distribution apply both within and external to the entity. Secret and private keys should be encrypted with a strong key-encrypting key that is stored separately, be stored within a SCD (such as a HSM), or be stored as at least two full-length key components or key shares, in accordance with an industry-accepted method. A crypto period should be identified for each key based on a risk assessment, and keys changed when this period is reached. Additionally, keys should be destroyed and replaced immediately upon suspicion of a compromise. Secure key-management practices include minimizing access to keys to the fewest number of custodians necessary, enforcing split knowledge and dual control for activities involving clear-text keys or key components and defining roles and responsibilities for Key Custodians and Key Managers.*
2. Key-management techniques must protect the integrity and purpose of symmetric cryptographic keys.	*For cryptographic keys to provide security reliably, they require mechanisms that 1) associate the type/purpose of the key to ensure that the key is not used for other than its designated purpose—e.g., as a key-encrypting key or as a PIN-encrypting key and 2) protect the integrity of the key including the order of key parts for algorithms that require multiple key parts—e.g., Triple Data Encryption Algorithm (TDEA).* *Methods of encryption of symmetric keys may not by themselves provide for key-block integrity or authentication. Because of this, there are known attacks that weaken the underlying key's security, resulting in key recovery and thereby compromising the encrypted data. Key blocks or equivalent methods provide this additional assurance.* *Additional information is available from the PCI SSC Document Library website, Cryptographic Key Blocks Information Supplement. https://www.pcisecuritystandards.org/documents/Cryptographic_Key_Blocks_Information_Supplement_June_2017.pdf*

1.4 Key Management

Requirements	Guidance
3. Cryptographic key-management processes must conform to recognized national or international key-management standards.	*Alignment with industry-accepted key-management practices provide reasonable assurance that required due diligence and execution reduce risk of unauthorized disclosure and supports the overall security of the processes.* *Applicable standards include NIST Special Publication 800-57 (all parts), Special Publication 800-130, ISO 11568 and ISO/IEC 11770; ANSI X9.24 Key Management Techniques and NIST Special Publication 800-90A, ISO/IEC 18031 including associated normative references cited within as applicable.*
4. Key-loading methods must enforce dual control to ensure that no one person is solely responsible for key-loading operations.	*The ability to perform sensitive security functions, e.g., key loading of encryption keys, requires at a minimum two individuals to perform the process. Dual control practices prevent misuse of the sensitive process—it is more difficult to establish a breach of a process when multiple entities are colluding to coordinate misuse.* *Dual-control procedures can be implemented logically. Or dual control can be implemented through physical controls where more than one individual is required.*
5. Secret and/or private cryptographic keys must be unique per devices and/or applications.	*Unique cryptographic keys per devices and/or applications limit exposure in the event the key is ever compromised.*
6. Generation and loading of clear-text secret and/or private keys or key components must ensure split-knowledge principles are enforced.	*Fundamental to cryptographic processes are the keys used for the encryption process. It is imperative that encryption keys are never disclosed so that the entire key is made available in clear text or in a form where the possibility of its disclosure in its entirety exists. The security principles of dual control and split knowledge requires at least two entities to be involved in a process to prevent a single entity from having access to the entire process, e.g., dual control as well has at least two individuals that have only partial information about the key.* *There are a number of ways to implement dual control and split knowledge either through logical or physical mechanisms or both.*

1.4 Key Management

Requirements	Guidance
7. Secret and/or private cryptographic keys must be maintained in one or more of the following approved forms: a. Encrypted by a key of equal or greater strength b. Stored within a SCD c. Managed as two or more full-length components **Note:** *These approved methods do not apply when storing secret and/or private cryptographic keys within the PIN CVM application. For the PIN CVM application (e.g., white-box cryptography) refer to Module 2.*	*Cryptographic keys need to be protected to prevent unauthorized or unnecessary access that could result in the exposure of encrypted data. Refer to industry-accepted practices for acceptable methods.* *Never store secret and/or private keys in clear text.* *Security requirements for white-box cryptography can be found in Module 2: PIN CVM Application.* *Refer to Module 2: PIN CVM Application for white-box cryptography requirements.*
8. Methods and procedures to revoke compromised public/private key pairs and certificates must be documented and implemented.	*The ability to identify and revoke compromised public keys/certificates and private keys are necessary to respond to confirmed or suspicious activity that could lead to misuse or data breaches. Ensuring that there are documented procedures in place and implemented supports common knowledge and sets expectations.*
9. All key-generation functions must implement one-way functions or other irreversible key-generation processes.	*One-way functions or other irreversible key-generation processes produce keys that are impossible to revert to the original data that formed the key. Adhering to industry-accepted cryptography algorithms and techniques supports these concepts.*
10. Keys must be generated with equivalent entropy (e.g., a 128-bit key is generated with 128 bits of entropy input).	*Entropy ensures that the cryptographic process ensures randomness is used to the fullest extent, which in turn strengthens the cryptographic process and encryption processes.*

1.4 Key Management

Requirements	Guidance
11. Audit logs must be maintained for all key-management activities and all activities involving clear-text key components. The audit log includes: a. Unique identification of the individual that performed each function b. Date and time c. Function being performed d. Purpose e. Success or failure of activity Controls must be established to protect logs from unauthorized modifications or deletion. Retention of key-management audit logs must conform to industry accepted practices and the organization's record retention policies.	*Recording the function or key-management activity being performed (for example, key loading) and the purpose of the affected key (for example, data encryption) provides the entity with a complete and concise record of key-management activities. Identifying whether the activity resulted in success or failure confirms the status upon conclusion of the activity. By recording these details for the auditable events a potential compromise can be quickly identified, with sufficient detail to know who, what, where, when and how.*
12. Incident response procedures must exist and include activities for reporting and responding to suspicious or confirmed key-related issues, including key compromises.	*Documented procedures assist with performing a process when time and access to resources are of the essence. They need to explain how the issue would be escalated for further investigation and resolution, including initiation of the organization's incident response procedures.* *Appropriate personnel need to be notified immediately of any breach impacting the keys.*

1.5 Secure Software Development Practices

Requirements	Guidance
Software needs to be developed and maintained according to a defined software-security development process. Software developers require knowledge to address software vulnerabilities and emerging risks. *These requirements address the development of software for all aspects of the solution, including the PIN CVM application, and the back-end systems (processing, monitoring, and attestation component) monitoring environment. Additional requirements specific to the PIN CVM application are stated in Module 2, PIN CVM application.*	
DEVELOPMENT	
1. All software must be developed according to the development process and to the development requirements outlined in Appendix D.	*Ensure the application is developed and software maintained in accordance with secure coding standards and best practices to reduce risk of exploitation of vulnerabilities introduced through poor coding techniques.* *Knowledge of additional industry application development standards and best practices provides information on current exploits and trends. For example, CERT secure coding standards, Institute for Security and Open Methodologies (ISECOM), Open Source Security Testing Methodology Manual (OSSTMM) and International Systems Security Engineering Association (ISSEA) Systems Security Engineering Capability Maturity Model (SSE-CMM), ISO/IEC 21827.*

Module 2: PIN Cardholder Verification Method (CVM) Application

Control Objective: *Ensure the software application that resides on the COTS device and captures the PIN from the cardholder enforces security controls to protect sensitive information and mitigate risks of unauthorized disclosure. The PIN CVM application is developed and tested to ensure application processing integrity.*

These requirements apply specifically to the PIN CVM application and client-side monitoring components if those components are not part of the PIN CVM application.

2.1 Development

Requirements	Guidance
1. Software that handles, secures or otherwise affects the security of the PIN entry and processing on the COTS device must be logically separated from code that is used for other purposes (such as general merchant UI).	*Areas of the PIN CVM application that are not directly involved in the processing or handling of the PIN data or providing security services and interface to the monitoring system, will be able to be updated without affecting the security code. This isolation may be achieved in many ways, but simply having different functions within the same body of code for security and non-security functions is not considered sufficient isolation.* *Multiple layers/levels of separation of the code may be implemented—for example, the code used for cryptographic key storage may be logically isolated from code used for PIN entry, and both of these code segments logically isolated from the overall merchant UI code.*

2.1 Development

Requirements	Guidance
2. Documentation must exist and be maintained to detail the following: • Protections provided to the application to protect against tampering, side-channel attacks, fault injection and reverse engineering for the various supported platform and protection methods (such as TEE, white-box cryptography). • Details of all areas where functions provided by the application are executed. This should include the main processing environment of the COTS device but may also include other local execution environments (such as a TEE or embedded security processor). • Data-flow diagrams that show how the PIN is entered, processed, encrypted and validated within the application, where the data is transmitted outside of the scope of the application and any assumptions made about these external connections. • Block diagram that indicates where all sensitive data is available in clear text on the merchant-side systems. This includes, but may not be limited to, the SCRP, the COTS OS, any TEE or physically separate security-processing elements used. This diagram must indicate the flow of sensitive data through the various elements. • Guidance for merchants regarding how to ensure the PIN is entered in a way that it cannot be observed. • Identification of where internal buffers are used and cleared when collecting sensitive data. • Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system. • A policy on how to manage vulnerabilities and perform security testing.	*The solution provider and the various parties involved will need to document various aspects of their solution sufficiently so that labs, assessors and other entities are able to understand the security around the various components individually and as a full solution.*

2.1 Development

Requirements	Guidance
3. Mechanisms must exist to uniquely identify each instance of the PIN CVM application to the back-end monitoring system and the back-end attestation component.	*The solution provider should ensure that each instance of the PIN CVM application is uniquely identified to the back-end monitoring system. The solution provider should conduct a risk assessment at least annually to ensure the adequacy of the authentication mechanisms and that controls remain in place.*
4. The PIN CVM application must only communicate with known and trusted PCI PTS approved SCRPs.	*A list of known and trusted SCRPs should be associated and maintained for each authorized user after initialization.*
5. The PIN CVM application must prevent against attacks designed to expose data in storage or memory and deploy appropriate controls including minimizing such storage post transaction completion or application timeout.	*The PIN CVM application might collect other data that can be used to correlate the PIN to the user and PAN at other places. The application should be designed in a manner that there is not unexpected leakage of PIN and other correlatable data that can potentially be compromised and misused.*
6. The PIN CVM application must be securely developed to prevent screen captures.	*Controls need to be in place to ensure that sensitive data collected via the application screen is not displayed without masking where appropriate and that the application does not allow the screen to be captured to prevent leakage of sensitive data. Protection methods include restricting access to the UI components as well as controlling inter-process communications and event handling. For example, when an application goes into the background, it could prevent screen capturing by the underlying OS by intercepting the applicationDidEnterBackground event to control what information is shared with iOS (e.g., splash screen or blurred window snapshot), or preventing manual and automatic screenshots altogether by setting FLAG_SECURE on Android.*
7. The PIN CVM application must be resistant to reverse engineering.	*The PIN CVM application should have adequate controls around the code such as code obfuscation so that the code cannot be parsed and reverse-engineered. This will prevent with tampering of the code.* *Resistance is quantified through costing based on "Software Tamper-Responsive Attack Costing Framework" as contained in the Software-based PIN Entry on COTS Test Requirements.*

2.1 Development

Requirements	Guidance
8. Correlatable data that may be supplied by the cardholder—e.g., e-mail addresses and/or mobile phone numbers required for receiving virtual receipts—must only be viewed in clear text during its initial entry for the purposes of error correction by the cardholder. Thereafter, any re-presentation of this data by the PIN CVM application must be masked to prevent exposure of the information.	*The PIN and PAN should always be isolated per transaction. Design the application in a manner to ensure that there is no leakage of correlated data that can potentially be compromised and misused—e.g., display only the last four digits of the mobile phone, display, at maximum, only the first two characters of e-mail address and the first two and last two of the domain name, jcxxxxxx@coxxxxxx.com. Additional privacy controls may be required by regional/country regulations.*
9. Establishing a new session or refreshing a secure session between the PIN CVM application and the back-end monitoring system and back-end attestation component must require successful attestation between the PIN CVM application and monitoring environment.	*Every time the PIN CVM application connects to the SCRP and authenticates to the back-end monitoring system and the back-end attestation component, it would need to successfully pass the attestation requirement to ensure that the PIN CVM application, SCRP, and COTS device are all in an acceptable state.*
10. The PIN CVM application must automatically clear the internal buffers it controls when any one of the following occurs: • The transaction terminated for any reason (including success or failure), or • The PIN CVM application has timed out waiting for the response from the cardholder or merchant or • A tamper-detection event has been signaled by the back-end monitoring system, or the PIN CVM application is halted, loses focus or otherwise is moved to background processing.	*Sensitive data shall not be retained any longer, or used more often, than necessary. PIN data and other correlatable data should be encrypted within the PIN CVM application immediately after entry is complete and has been signified as such by the cardholder—e.g., via pressing the enter button.* *The device will support the encipherment of the PIN multiple times as part of a transaction series; transferring it between the PIN CVM application and SCRP, then from the SCRP to the payment back-end. Implement each merchant-side instance to clear the buffers as soon as practical after use.* *Solely relying on "garbage collection" functions for clearing buffer data is not sufficient to meet this requirement.*

2.2 Secure Provisioning

Requirements	Guidance
1. There must be a clear definition of all platforms—including device types, hardware and OSs—on which the PIN CVM application can be executed.	*Although these requirements are designed to allow for the entry of a PIN on a COTS platform that has not been directly assessed for security, it is expected that the system will have criteria for which platforms are considered acceptable for PIN entry, and which are not. For example, it is expected that systems using older COTS OSs that may contain unpatched vulnerabilities will not be deemed acceptable for PIN entry. The system vendor provides a clear methodology for determining the suitability of any PIN entry platform; this may be a whitelist, blacklist or hybrid approach, but should clearly demonstrate a risk analysis of the platform that accommodates for any known or potential vulnerabilities in each merchant device.* *There are two requirements in this standard that address the suitability of devices/OSs on which the PIN CVM application may be executed. This "supported platforms" requirement addresses the need for the PIN CVM application to be targeted to a limited subset of all available devices, and that the developer should have undertaken some risk analysis and mitigation steps to identify which platforms are suitable and secure.*
2. PIN CVM applications must be developed only for supported platforms.	*Where OSs are no longer supported, security patches might not be available to protect the system from known exploits—which poses a significant risk. Unsupported OSs expose the device, applications and data on the device to unauthorized disclosure and modification.* *All new solutions would need to ensure that they operate only on supported platforms.*

2.2 Secure Provisioning

Requirements	Guidance
3. The PIN CVM application must only support platforms that, at a minimum, provide the following features: • An enforcing mandatory access control framework • A "trusted boot" mechanism that validates the OS's authenticity • Ability to prevent all applications other than the foreground application from accessing touch-event details • Validation of an application signature upon loading and execution of that application. This signature must be calculated with cryptography, and no known bypass measures may exist for the acceptable baseline systems. • Isolation of touch-event data such that only the application currently in focus can receive or otherwise identify the location of touch events	*To ensure the security of the solution, the PIN CVM application should be enabled only on a COTS device that meets minimum acceptable criteria. The PIN CVM application developer should undertake some risk analysis and mitigation steps to identify which platforms are suitable and secure.*
4. The PIN CVM application must be installed and updated using methods that ensure its integrity and authenticity, using only the OS store implementing cryptographic validation of this store and any loaded applications. The OS store must not have publicly disclosed vulnerabilities that have not been patched or otherwise remediated by other features of the overall solution.	*The authenticity of the PIN CVM application is a paramount concern in the security of PIN entry. Loading of applications from the OS store provides a level of confidence that the application has not been tampered before being installed on the merchant system. Third-party app stores are not allowed.* *Where the PIN CVM application allows or requires download of additional data from the back-end monitoring and attestation systems, such data should also be cryptographically signed and authenticated by the PIN CVM application prior to use or execution. Reliance upon the secure channel that exists between the PIN CVM application and the back-end monitoring system and attestation component are not sufficient. This requirement implies that each datagram sent from the device to the back-end monitoring system and the back-end attestation component, or vise-versa, has an individual signature or (H)MAC applied. The validation of this datagram signature/MAC is provided by systems outside of the execution environment of the PIN CVM application (e.g., by the external SCRP used in situations where CVM may include PINs).*

2.2 Secure Provisioning

Requirements	Guidance
5. Any required cryptographic keys or other data necessary for first execution must be securely provided to the PIN CVM application and securely stored. • Where an external SCRP is used, this must include the use of cryptographic keys stored within the SCRP to provide security to the provisioning process. • Where white-box cryptography is used white-box keys must be unique per PIN CVM application instance. The reliance and use of common white-box keys must be minimized after the secure provisioning process. • Secure provisioning must implement the principles of perfect forward secrecy.	*As the PIN CVM application is downloaded as a single instance from an OS store, each application install is initially identical to all others. The system should have methods immediately upon first execution to ensure that instance is unique to any other and can be uniquely identified and secured through communication with the back-end monitoring system and the back-end attestation components.*
6. The PIN CVM application executables and scripts must be digitally signed and a signature provided to confirm the software author and guarantee that the application from the OS store (and any other updates) has not been altered or corrupted since it was last signed. The digital signatures must be checked prior to use of the application and at required attestation intervals.	*Where the PIN CVM application allows or requires download of additional data from the back-end monitoring system and the back-end attestation components, such data should also be cryptographically signed and authenticated by the PIN CVM application prior to use or execution.* *The PIN CVM application may be authenticated through the use of multiple signatures. These may be validated by the COTS OS as well as the monitoring system.*
7. The process to generate digital signatures must be performed using dual control, based on cryptographic keys that are secured within an HSM formally approved to PCI HSM or FIPS140-2 Level 3 (or above).	*In order to ensure the digital signatures are authentic, it should be performed within a controlled environment that meets industry standards.*
8. A security policy must exist for acceptable use of the PIN CVM application and be provided to all users of the PIN CVM application, and is part of the PIN CVM application End User License Agreement (EULA).	*The vendor must supply documentation to allow the merchant to understand the context of the approval of the PIN CVM application and the solution and to ensure that it does not deploy or use the system in a non-compliant manner. In this context, the security policy both informs the merchant how to use and maintain the system securely, and also provides information to the laboratory during the the solution evaluation.*

2.3 Tamper Checks

Requirements	Guidance
1. The PIN CVM application must offer tamper-resistance measures around the handling of code, application/monitor interface code and any code that is involved in the use or security of cryptographic keys (both public and private/secret keys) for all the supported platform and protection methods (such as TEE, white-box cryptography).	*Obfuscation should reduce the efficacy of common tools that may be used for decompilation of the code. Obfuscation methods may include, but not be limited to, control-flow and data obfuscation, execution of code sections in remote/cloud environments, API renaming, etc.* *These protections are not required across all code, but should be implemented to protect all code that provides PIN security features, such that code complexity can be demonstrated to be significantly increased, or execution can be shown to be possible only on un-modified environments—e.g., through use of a device Physically Unclonable Function to encrypt data/execution, or by implementing the PIN-acceptance code in a trustlet that can be executed only in a secure TEE.*
2. Documentation must exist and be maintained on how tamper resistance is achieved for each of the supported platforms, including but not limited to: • Code obfuscation • Protections provided by specific platforms • Reliance on TEE, security processor, or other security feature of the COTS devices used	*The solution provider and the various parties involved will need to document how tamper resistance is achieved for each supported platform, where it leverages protections offered by the platform and how it compensates for any security gaps. This information is critical for the labs to review and validate.*
3. The PIN CVM application must implement methods for detecting and reporting to the monitoring system if any COTS devices have been rooted or jailbroken, including but not limited to: • When the PIN CVM application is executed • As requested by the monitoring system • Whenever white-box cryptography or obfuscation methods, implementations, or instantiations are updated The monitoring system must detect when the PIN CVM application has been "side loaded" outside of normal channels and treat this as a tamper-detection event. Applications that fail this check should be prohibited from use to accept PINs.	*Even though a supported platform may offer many security and/or tamper-protection mechanisms, rooting or jailbreaking a device could impact and weaken the overall security controls and open up avenues for a malicious user to install malware or exploit other vulnerabilities to harvest sensitive data or affect the integrity of the solution.* *If such security issues are noted, a tamper-detection response should be triggered to the back-end monitoring system and the application should not be allowed to accept PIN data.*

2.4 PIN Entry

Requirements	Guidance
1. The PIN CVM application must not display the PIN entry screen if it detects that it is being run in developer or emulator mode.	*Developer, emulator mode and similar tools provide flexibility when developing applications but may circumvent required security controls required for production environments. Therefore, controls should be established to ensure when these non-secure modes are present that sensitive information and functions are not displayed or performed.* *This is specific to the production level PIN CVM application.*
2. The following events during a PIN entry session must be detected by the PIN CVM application and result in termination of the PIN entry session and deletion of all data collected during the transaction, including PIN data, and not limited to: • Switching between applications (e.g., PIN CVM application and any other application on the COTS device) • Stealing focus during PIN entry • Stealing focus at any other time during the foreground execution of the PIN CVM application to maliciously prompt for (and thereby capture) PIN entry • Screen capture during PIN entry • Not using "full screen mode" • Activating sensors or pooling sensor data • Enablement or access of the NFC interface by any other application	*The PIN entry process should be protected against manipulation or subversion. Attempts to modify or overlay the cardholder prompts, keyboard, or other UI features that are important for the security of the system should be prevented. The security of the other applications on the COTS device is not known and therefore should not be trusted.*

2.4 PIN Entry

Requirements	Guidance
3. The PIN CVM application must not allow PIN entry to be triggered unless the transaction is EMV-based. All transactions must be processed online. **Note:** *This does not prohibit the use of offline PIN verification.*	*EMV-based transactions introduce dynamic data into the ecosystem, which will be encrypted within the SCRP to be sent to the back-end processing systems. Merchants may have alternate solutions to accept card transactions if the SCRP or the PIN CVM application is not working. But, those solutions cannot be used to accept PIN data unless they comply with the PTS PIN Standard.* *In the context of this requirement, "online" refers to the transmission of the financial message to the remote host during the performance of the transaction. Such transactions may utilize either online or offline PIN processing. Where online connectivity is not available, the transaction processing is to be prevented. If connectivity drops during a transaction and the transaction has to be reversed, all customer data has to be immediately erased from the system.*
4. PIN display in the PIN CVM application must be fully masked so as not to display any digit of the PIN value.	*PIN data should be protected from intentional or unintentional exposure when the data is collected and displayed for confirmation.* *Refer to PCI PTS POI Security Requirements for additional information on PIN display.*
5. The PIN entry keyboard must not rely on the COTS device OS keyboard, and it must be securely rendered by the PIN CVM application.	*The PIN entry process should be protected against manipulation or subversion.* *OS keyboards could be susceptible to compromise and spoofing.*
6. During PIN entry, any signal or event (visual, audible, etc.) must be uncorrelated to the touch event position and the PIN digit being selected. In addition, this must account for other leakage factors—e.g., local haptic feedback, numeric key animation when pressed, on device sensors, etc.	*The PIN entry process should be protected against manipulation or subversion. There are products in the marketplace that can convert audible tones into actual numbers thus exposing the underlying PIN value, as well as products in the marketplace that can convert touch events and their emitting lights to the actual values. Understanding these techniques and protecting against them is important to ensure PIN values are not disclosed through unintended channels.* *Therefore, additional considerations are necessary to prevent identifying the PIN values through audible tones and emission of touch-event light.*
7. The PIN CVM application must not cache PINs.	*The PIN CVM application should prevent storing of PINs.*

2.5 PIN Encryption

Requirements	Guidance
1. PIN data must be encrypted upon entry into the PIN CVM application and remain encrypted when transmitted by the PIN CVM application through a trusted and secure interface to the SCRP.	*Encryption of the cardholder's PIN as it is entered into the PIN CVM application and as it is transmitted to the SCRP is essential and sets the expectation of PIN protection throughout the solution. Since PIN encryption is performed in software within the PIN CVM application, additional measures are required to ensure the confidentiality of the encrypted PIN and the processes performing the encryption.*
2. Encrypted PIN data must be protected from malicious activity, attacks and attempts to extract masked PIN values.	*The PIN CVM application should provide assurance that even encrypted PIN values are not susceptible to non-authorized disclosure.*
3. The PIN-encryption keys and algorithms in the PIN CVM application used to initially encrypt the PIN must adhere to requirements specified in Appendix C – Minimum and Equivalent Key Sizes and Strength for Approved Algorithms.	*Industry accepted requirements are based on substantial research and testing. Conformance to these requirements greatly increases an organization's security posture.*
4. PIN-encryption keys must be established in the PIN CVM application in a secure manner.	*Key loading is to be performed to ensure no one individual has knowledge of or access to the key that encrypts/decrypts PINs. The procedures used should align with industry accepted key-management practices including key-agreement protocols (e.g., mutually authenticated ECDH).*
5. Secret keys associated with PIN encryption must be protected to ensure their confidentiality as well as their integrity.	*Encryption keys are fundamental to the overall protection of assets and security of the solution. Mechanisms are to be implemented to ensure the confidentiality and integrity of the secret keys used for PIN encryption. Protection mechanisms may include software obfuscation, key chain, and white-box cryptography, use of secure elements or TEEs.*
6. Where white-box cryptography is used, the white-box cryptography keys must be changed monthly, at a minimum.	*Frequently changing the white-box encryption keys used to protect data substantially increases the security of the solution. When encryption is performed in software, it is critical to change the white-box key often to prevent unauthorized disclosure.*

2.5 PIN Encryption

Requirements	Guidance
7. The customer PIN data must be encrypted using ISO format 4 for transport between the PIN CVM Application and the SCRP.	*For ISO format 4 PIN blocks, to address separation of PIN and PAN, a PAN token as described in the POI Security Requirements, is supplied by the SCRP to the PIN CVM application.* *The SCRP may translate the PIN block into ISO format 0, 3 or 4 for online PIN verification and format 2 for offline PIN verification.* ***Note:** The use of TDES for encryption of the customer PIN on the SCRP is the only exception allowing the use of TDES in this standard.*

2.6 Audit Logs

Requirements	Guidance
1. The PIN CVM application must ensure logs exist and are communicated securely to the back-end monitoring system. The logs must not contain correlatable data or PIN data.	*Application logs assist with providing individual accountability, reconstruction of events, intrusion detection and problem identification.* *Sensitive information should not be included in audit logs as they may not be protected in the same manner.*
2. The audit trail generated by the PIN CVM application must support reconstructing the following events: • All user access to correlatable or PIN data. • All activity that impacts security functions of the PIN CVM application (e.g., changes to cryptographic functions, changes to application permissions, failure or success to establish secure channel with monitoring system, etc.) • All access to the audit trail managed by or within the PIN CVM application. • Use of and changes to the PIN CVM application's identification and authentication mechanisms. • Initialization, stopping or pausing of the PIN CVM application logs.	*Logging of the security events enables an organization to identify and trace potentially malicious activities. While the correlation and analysis of the event could occur on the back-end monitoring system, the PIN CVM application should be able to capture and securely communicate events that could be used by the back-end monitoring system.*

2.6 Audit Logs

Requirements	Guidance
3. All recorded events must capture at least the following information: • User identification • Type of event • Date and time • Success or failure • Origination of event • Identity or name of affected data, system component or resource	*By recording these details for the auditable events, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when and how.*

Module 3: Back-end Systems – Monitoring/Attestation

Control Objective: *Assurance that components in the solution are in a secure state and the ability to react and address anomalies is fundamental to the overall security of the solution. Attestation sets the framework for this assurance.*

Attestation is the interaction between a verifier (possibly server-based) and a prover (possibly client-based) to determine the current security state/behavior of the prover based on predefined measurements and thresholds provided by the prover. For the purposes of this document, attestation may be based on a hardware or software-based verification.

Attestation may be demonstrated using a protocol between the prover and the verifier that provides the measurements to the verifier. The measurements may be determined in various ways, for example through a health-check interface that can be accessed by the prover.

Attestation provides necessary assurance to the verifier that established security controls at the prover are in an acceptable state and have not been modified.

PIN CVM Application Remote Software Attestation Components

- The PIN CVM application software attestation component is the process on the COTS platform used by the PIN CVM application to manage attestation. It may perform the role of the *verifier* and the *prover*.

  For example, in the role of *verifier* it may perform an attestation of the COTS platform (as the *prover*) by taking measurements and comparing these with locally stored information (followed by any necessary action), whereas in the role of *prover* it may service a remote software attestation request sent from the server-based attestation component (as the *verifier*) and return the results back to the server.
- The back-end attestation component (a server-based attestation component) is a process that manages attestation. It performs the role of *verifier*.

Thus, the solution may implement various types of attestation. Two *verifier* types are presented in the table below corresponding to possible locations of the *verifier*.

For PIN entry on COTS, the attestation health checks will be performed on varying components (provers): SCRP, COTS platform and the PIN CVM application.

The solution may use various types of attestation. Three prover types are presented in the table below indicating possible locations of the verifier.

Note: *During attestation, the prover is assumed to be untrusted and the verifier is trusted. During Type 1 and Type 2 attestations, if the PIN CVM application component has the role of the verifier, it may itself be compromised. Therefore, the security model must account for this risk when using the results of Type 1 and Type 2 attestations provided by the PIN CVM application if used as part of a Type 3 attestation.*

PIN CVM Solution Attestation Types and Components

Type	Prover	Verifier	Purpose
1.	SCRP	a) PIN CVM application attestation component b) Back-end attestation component	*Verifies the SCRP is valid.* *A PIN CVM application instantiated attestation and response may be fairly limited due to limited processing availability and security afforded to local storage of measurement parameters, whereas an attestation call performed by the back-end attestation component (required) can be more robust since parameter checking is performed in close association by the monitoring system.*
2.	COTS platform (via various sampled measurements)	a) PIN CVM application attestation component b) Back-end attestation component c) SCRP	*Verifies that the COTS platform security model is intact.* *The assurance for Type 2 attestation relies on the inability of the attacker to spoof the measurements that are performed or, by the time it is possible for spoofing to be reliably performed, the presence of the attacker in the COTS device has been detected by the fraud systems and appropriate action taken.* *A PIN CVM application/SCRP instantiated attestation and response may be fairly limited due to limited processing availability and security afforded to local storage of measurement parameters, whereas an attestation call performed by the back-end attestation component (required) can be more robust since parameter checking is performed in close association by the back-end monitoring system.*
3.	PIN CVM application (attestation component)	a) Back-end attestation component b) SCRP	*Verifies that both the security model of the PIN CVM application and its COTS platform are intact.* *An SCRP instantiated attestation and response may be fairly limited due to limited processing availability and security afforded to local storage of measurement parameters, whereas an attestation call performed by the back-end attestation component (required) can be more robust since parameter checking is performed in close association with the back-end monitoring system.*

Example attestation flows corresponding to each attestation type are shown on the following page.

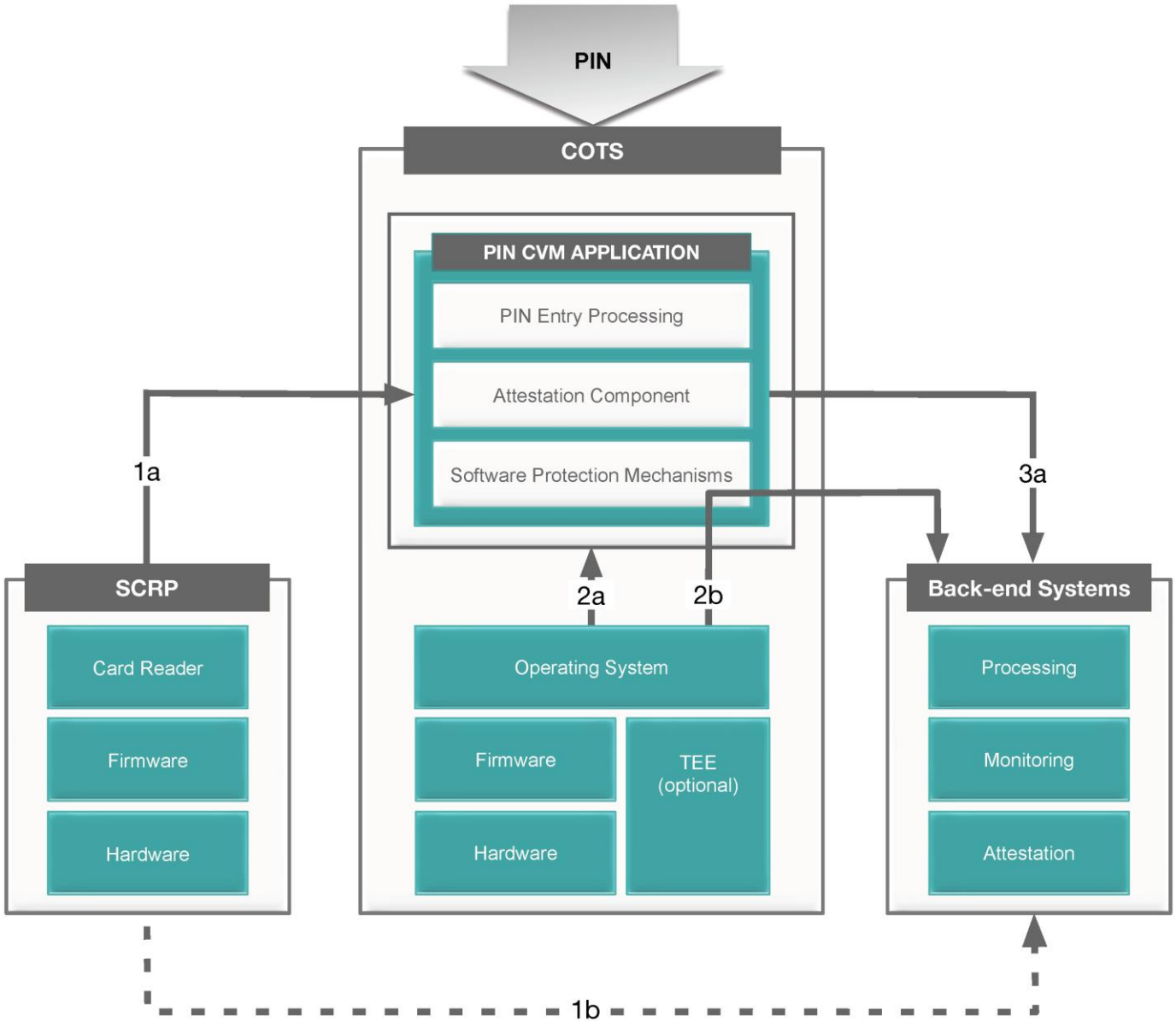


Figure 6: Attestation Flows

The diagram above shows software attestation flows corresponding to each attestation type. For example, a Type 2a attestation is initiated by the PIN CVM application attestation component (as verifier) and sampled measurements returned to the PIN CVM application attestation component for local action (according to the attestation policy). On the other hand a Type 2b attestation request originates from the server (as verifier), is processed by the attestation component of the PIN CVM application (protected by software-protection mechanisms), which returns any required sampled measurements of the COTS platform (as *prover*) in the response to the back-end attestation component for further processing and action.

3.1 COTS System Baseline

Requirements	Guidance
A defined set and state of COTS devices and OSs must be specified on which the PIN CVM application may be executed. The system baseline is a subset of all currently deployed COTS platforms. The attestation process is required to define which of those COTS platforms is secure for use by the PIN CVM application based on data about current attack methods, new vulnerabilities or other relevant information. *The attestation process includes monitoring of the COTS platform to ensure that the platform is in, and remains in, the system baseline.* *The solution provider is responsible for establishing and maintaining system baselines.*	
1. Documentation must exist and be maintained for the following: • Implemented processes to determine the system baseline for acceptance of COTS devices (for example whitelist, blacklist, or hybrid approach) • How these processes account for known and potential vulnerabilities in systems • Clear identification of roles and responsibilities for which aspects of the system baseline validation process are performed by the PIN CVM application itself, and which are performed by other systems or execution environments. • Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system.	*Documentation assists with establishing common knowledge of the security controls and system baselines required for secure PIN processing. These processes and risk management that underlie the management of the system baseline should be specified and comprehensive.*
2. Documentation must exist and processes be demonstrably in use that identify methods used for updating the system baseline as new threats are identified.	*The system baseline will change over time and so the process performed by the attestation system to determine the system baseline will not be a single "point in time," but instead an on-going process that continually assesses the threat environment and allows for decisions to be made about the security of the solution at a platform level.*

3.1 COTS System Baseline

Requirements	Guidance
3. The system baseline must be validated by the attestation process upon provisioning of the PIN CVM application.	*The solution should establish a trusted status (aka, baseline) for its components at the onset (provisioning) in order to provide meaningful and relevant information to make security decisions, identify anomalies, or take actions.* *If the system baseline permits the use of COTS platforms that are no longer supported with security patches by the product vendor or platform vendor, mitigations are necessary for use of such platforms and demonstrable proof that the risk of subversion of the payment process and exposure of PIN is not extended beyond use of COTS devices that are supported by security patches.*
4. The system baseline must not include rooted or jailbroken devices.	*To provide reasonable assurance that the system baseline reflects a secure, trusted state of the environment the baseline should be free from influences that could negatively impact or affect the integrity of the baseline, e.g., devices that have been compromised.*
5. Validation of the system baseline must be performed during each attestation check performed by the back-end attestation component.	*Ongoing verifications to the system baseline by the back-end attestation component helps to identify deviations that could indicate unauthorized access or a compromise. Therefore, ensuring validation is consistently performed is imperative to retain a trusted state.*
6. COTS devices that use unsupported COTS platforms must be prohibited from processing transactions.	*Any exceptions are considered compliance-related issues and should be referred to the payment card brands.*

3.2 Attestation Mechanism

Requirements	Guidance
General requirements for PIN CVM application, COTS device and attestation components (in the PIN CVM application and the back-end *system).* *Attestation is used to determine whether the COTS device that hosts the PIN CVM application is being, or has been, maliciously altered or does not meet specified criteria. Underpinning the attestation are policies and procedures and the staff that implement them.* *The solution provider is responsible for defining policies and procedure.*	
1. A documented attestation policy that defines health-check rules for the SCRP, COTS platform, and PIN CVM application attestation mechanisms must exist. • The policy must include detailed response procedures for successful and non-successful results. • The policy must be maintained and strictly controlled including reviews and updates as necessary, at least annually.	*A policy that defines the specifics to support the attestation mechanisms is necessary for common understanding on how each attestation component works individually and together.* *The policy should explain the security trust model, how it protects the privacy of the solution users, the thresholds used, triggers and acceptable errors, categorization of attestation findings as well as response procedures and timeframes for responses.*
2. The attestation system must manage attestation parameters and measurements securely and maintain their integrity wherever they are stored or processed. (Note that measurement parameters can be static or behavior-based, privileges, intents, system calls). • Attestation data must be cryptographically signed. ***Note:*** *If no assurance is available, any security dependence on the proxy is a residual risk.*	*If any attestation parameters or results of attestation can be maliciously altered, then the integrity of the attestation system is impacted.* *Examples of attestation parameters and measurements include:* • *Use of nonces – Requires integrity-protected storage of the hashes for previous nonces.* • *Use of counters – Requires integrity-protected storage for the counters.* • *Use of timestamps – Requires trusted synchronized clock at prover side.* • *Specialist attestation proxies may be used to collect measurements as part of a multi-layer approach.*
3. Attestation must be performed at a minimum: a. At initialization/initial installation of the PIN CVM application initiated by the attestation system, back-end systems, or other trusted non-local execution environment. b. At least every five minutes (if not otherwise activated by one of the events above during that time). c. As indicated in following sections.	*Certain events require an attestation to be performed at certain intervals to ensure system integrity and trust is maintained. Attestation values set are the minimum checks required; however, entities are encouraged to implement the most robust attestation and monitoring processes.*

3.2 Attestation Mechanism

Requirements	Guidance
4. For any attestation response, The solution provider must be able to identify: a. Where the process is implemented (in the PIN CVM application, in a server-based attestation component, remotely or locally to the consumer device, etc.). b. Whether the process was developed by the attestation vendor. c. Whether the process is managed by a third-party provider that provides an API to the attestation vendor but no other privileged access.	*The attestation response should provide sufficient detail to enable the correct action to be taken by the system or staff operating the system.*
5. Escalation procedures must be defined for undocumented and unknown attestation responses.	*The attestation policy should provide staff with escalation procedures for dealing with unexpected scenarios or results from remote attestation.*
6. Attestation code implemented in the PIN CVM application must be protected by the tamper-resistance features implemented in the PIN CVM application.	*Any attestation code that is present in the PIN CVM application should be protected from reverse engineering and any static or dynamic attacks that could subvert attestation processing.*
7. If the attestation system tamper response involves a manual process—e.g., a potential tamper event, it must be escalated to vendor staff to validate: a. Written procedures for manually processed events must exist and be demonstrably in use. b. These procedures must cover events where staff relied upon for such determinations are unavailable. c. Events must be immediately escalated for manual review and then actioned within 48 hours. d. Automated systems must be in place to disable any further payment processing from systems when an event has not been actioned for 48 hours.	*Manual processes for managing attestation system responses, including escalation procedures, should be well documented to avoid possible errors in interpretation by operational staff.*
8. Requisite skilled staff must be provided to implement and interpret attestation health-check rules, associated controls and findings, along with the associated training.	*Attestation results that do not have an automated response may require skilled staff to interpret specific attestation findings or to interpret them within a wider risk management framework; for example, use of telemetry and transaction heuristics.*

3.2 Attestation Mechanism

Requirements	Guidance
9. Retention requirements must be defined and implemented for attestation results.	*Defining retention requirements ensures attestation data is available for troubleshooting and investigation purposes. Local regulation may impact retention. The policy should provide mitigations to address such regulation.*
10. Retained attestation findings must have a unique ID, date and time stamp and description.	*Unequivocal identification of findings is required for subsequent audit and troubleshooting.*
11. Attestation mechanism changes must be performed using authorized processes.	*It should not be possible to circumvent or create false attestation results by unauthorized modifications to the system.*
12. Attestation mechanism changes must adhere to formal change-control procedures.	*All changes to the solution components require identification of changes, business justification, testing and approvals. Without following fundamental change-control principles, changes can be intentional or unintentionally omitted that would jeopardize the security and processing of the solution.*
13. For manual updates of the attestation system: • There must be documented procedures. • Deployment of changes to the production environment must require dual control.	*Manual processes may be subject to misinterpretation, leading to misconfiguration or other insecure practices if sufficient documentation of the procedures required to drive them is not available. In particular, manual changes to the attestation production environment should only be possible under dual control.*

3.3 Type 1 – Attestation of SCRP

Requirements	Guidance
This attestation is used to ensure that the SCRP used by the solution is valid.	
1. The PIN CVM application attestation component must be able to determine that the connected SCRP is valid. At a minimum verify the following: a. Firmware version is acceptable b. SCRP is in a secure state and supports SRED functionality c. Correct unique identifier of the SCRP	*Prior to sharing any PIN encryption key with the SCRP the PIN CVM application should determine that a valid SCRP is connected.* • *SCRP firmware is up to date* • *SCRP meets all integrity checks associated with SRED deployment* • *SCRP provides a unique, verifiable identifier*
2. Attestation of the SCRP must be performed in accordance with the specified attestation policy. At a minimum the attestation must occur: a. At system initialization b. Before business processing commences (prior to first transaction) c. If initiated by a monitoring environment request d. Polled at unpredictable intervals during an online session e. Whenever the SCRP is physically or logically disconnected and reconnected to the COTS platform	*The attestation policy specifies when and how attestation should be performed. Contents of the policy may be deemed confidential, therefore the policy itself should be protected and access to and knowledge of the specific details within the policy should be based on a need to know.* *At initialization the PIN Entry Solution should be in a trusted state. Establishing the status of the SCRP is one step of the initialization of the system.* *Attestation is required when preparing to process a PIN transaction to confirm security status.* *The monitoring environment should have the ability to request attestation at any time as part of its responsibility to maintain overall security for the solution.*

3.4 Type 2 – Attestation of COTS

Requirements	Guidance
Establish reasonable assurance that the COTS platform executing the PIN CVM application is running as trusted. The attestation system must implement methods to actively detect and respond to events that indicate that the COTS device is being, or has been, maliciously altered. These tamper-detection and response methods cannot be wholly implemented in the same execution environment of the PIN CVM application.	
1. An attestation baseline of the COTS platform must be performed at PIN CVM application provisioning.	*The COTS platform attestation should be established as soon as possible after application provisioning is performed in order to confirm that it is part of the system baseline.*
2. The COTS platform attestation must include comprehensive configuration information.	*Firmware version, app version, SCRP ID, merchant ID, integrity of configuration, or whatever data is available for verification.*
3. Mechanisms must be in place to validate the integrity of the attestation results.	*Attestation measurements should be an accurate representation of the state of the platform security model.*
4. Attestation mechanisms must not be vulnerable to TOCTOU (time-of-check, time-of-use) attacks.	*It should not be possible for an attacker to influence system resources between the time the attestation measurements are made and the time they are checked.*
5. Information about the platform state must be accessible to measurement tools.	*Attestation measurements reflect the state of the platform running the PIN CVM application. Any tools or methods used to obtain measurement information should not require privilege escalation on the COTS platform.*
6. Attestation mechanisms must not interrupt payment-transaction processing.	*If the attestation is running when the solution is online, it should not interrupt transaction processing.*
7. Attestation responses must not leak information about the attestation mechanism.	*Attestation responses provided to the verifier should not provide deterministic information to a malicious provider.*
8. Attestation responses must be unclonable.	*Attestation responses should be unclonable, for example by cloning part of the PIN CVM application configuration using an emulator and performing MITM attacks.*
9. Attestation responses must complete within an expected timeframe as defined in the attestation policy. If not, the monitoring environment must be notified.	*A malicious process may interfere with attestation processing, for example to create a denial of service. The PIN CVM application attestation component should notify the monitoring environment if the response timeout is exceeded.*

3.4 Type 2 – Attestation of COTS

Requirements	Guidance
10. Attestation mechanisms must be provided and maintained with up-to-date information about known vulnerabilities to detect at a minimum: a. Modifications to the COTS platform OS firmware b. COTS platform OS firmware tamper c. PIN CVM application execution in developer mode d. PIN CVM application execution in debug mode e. Emulator use f. Use of a hooking framework g. PIN CVM application modification h. PIN CVM application tamper i. Use of PIN CVM application code, or part thereof, within another (valid and/or invalid) operational environment—e.g., through "code lifting" of the entire, or partial, application to another platform after initialization and personalization j. Asynchronous rooting and un-rooting of the COTS platform OS k. Relay attacks on PIN entry	*Specific data is required to ensure the security state of the COTS platform. Attestation parameters will vary depending on OSs but should include basic verification and be as comprehensive as possible.* *It should not be possible to perform or enable remote screen display of the PIN CVM application on another device (which is therefore not running the system attestation and monitoring).*
11. Implement controls to protect the attestation mechanism from reverse engineering.	*It should be difficult for an attacker to learn details about the attestation mechanism's design, construction and operation. Use of obfuscation and use of native code are techniques that can be used.*

3.4 Type 2 – Attestation of COTS

Requirements	Guidance
12. The COTS platform attestation must be performed in accordance with the specified attestation policy. At a minimum, the attestation must occur:	*The attestation policy specifies when and how attestation should be performed.*
a. At PIN CVM application startup	*At initialization the solution should be in a trusted state, otherwise it may not be possible to trust any subsequent attestations.*
b. Before business processing commences (first transaction of the day)	*When the solution is about to commence transaction processing, it should establish a trusted status for its components.*
c. If initiated by a monitoring environment request	*The monitoring environment should have the ability to request attestation at any time as part of its responsibility to maintain overall security for the solution.*
d. At unpredictable intervals, polled during an online session	*The attestation of the COTS platform should be part of a process that requests an attestation response at unpredictable intervals. Re-occurring attestations ensures real-time evaluation of the state of security and allows for intervention if anomalies are present.*
e. After changes have been made to the solution or to major configuration files	*When the solution has undergone changes, the solution should re-establish a trusted status for its components.*
f. When the "Application" loses "focus" and regains "focus"	*If the Application has lost and regained focus the solution may no longer be in a secure state.*
g. Continuously, polled at periodic, unpredictable intervals	*The attestation of the COTS platform should be part of a continuous process that requests an attestation response at unpredictable intervals.*

3.5 Type 3 – Monitoring Environment Attestation of PIN CVM application

Requirements	Guidance
Establish assurance that: *1) The PIN CVM application attestation component, with which the monitoring environment is communicating, is trusted;* *2) The COTS platform is trusted; and* *3) The monitoring environment is adequately prepared to take appropriate action.*	
1. The PIN CVM application's attestation must meet requirements of Type 2 attestation.	*Provide COTS platform attestation (e.g., see Type 2 items).*
2. The PIN CVM application must support a set of attestation criteria that meet the attestation baseline.	*Attestation criteria determines the health of the system through interrogation of a "health-check" interface and access to any security service checks provided by the monitoring environment.*
3. A set of rules must be defined for analyzing the attestation responses and assign a risk-severity rating for the attestation responses that aligns with the attestation policy.	*Analysis may be automatic, semi-automatic or fully manual.*
4. Establish detailed procedures or automated responses for attestation responses. Procedures must include, at a minimum: a. Send an alert to the monitoring environment support personnel based on attestation-response severity. b. Conduct corrective actions (e.g., modify a hash of a configuration file) for false positives. c. Completely block transaction processing in the most significant cases as defined in the attestation policy. d. Temporarily stop transaction processing to update obsolete solution components (either internal or third-party dependencies).	*Defined and known procedures ensure correct follow-up actions are performed.*
5. Maintain up-to-date configuration measurements to support attestation criteria.	*Attestation measurements should reflect up to date information to ensure accurate responses to support attestation requests.*
6. Establish controls to defend against attestation abuses to subvert the prover—e.g., defend against DoS through malicious verifier attacks.	*The solution should provide mitigation again compromise of the attestation component that may result in DoS.*

3.5 Type 3 – Monitoring Environment Attestation of PIN CVM application

	Requirements	Guidance
7.	Establish controls to defend against attestation abuses that exploit system automation such as data poisoning attacks.	*Invalid data is deliberately injected into the system to bias the detection algorithms incorrectly.*
8.	The monitoring environment-based attestation must be performed in accordance with the specified attestation policy. At a minimum the attestation must occur:	*The attestation policy specifies when and how attestation should be performed.*
	a. At system startup	*At initialization, the solution should be in a trusted state; otherwise it may not be possible for the verifier to trust any subsequent attestations.*
	b. Before business processing commences (first transaction of the day)	*When the solution is about to commence transaction processing, it should establish a trusted status for its components.*
	c. At unpredictable intervals, polled during an online session	*Re-occurring, unpredictable attestations ensure real-time evaluation of the state of security reduces opportunity for spoofing attestation results by a malicious process and allows for intervention if anomalies are present.*
	d. If triggered by the PIN CVM application attestation component	*The PIN CVM attestation component may detect a local finding with the platform during a type 2 attestation and request a type 3 attestation.*
	e. If initiated by a monitoring environment request	*The monitoring environment should have the ability to request attestation at any time as part of its responsibility to maintain overall security for the solution.*
	f. After changes have been made to the solution or to major configuration files	*When the solution has undergone changes, the solution should re-establish a trusted status for its components.*
9.	A documented policy and procedure for assessing these changes to the system baseline must exist and provide details on how: • Decisions are made to remove previously acceptable platforms from the system baseline. • Such changes will affect the parties using these platforms, so the documentation must also include how communication is handled in these cases.	*As the security landscape changes, platforms or OSs that may be acceptable under the system baseline may become vulnerable. A documented policy and procedure for assessing these changes should exist and provide details on how decisions are made to remove previously acceptable platforms from the system baseline. Such changes will affect the parties using these platforms, so the documentation should also include how communication is handled in these cases.*

3.5 Type 3 – Monitoring Environment Attestation of PIN CVM application

Requirements	Guidance
10. The solution provider must have a documented risk-assessment policy and procedures that provide details on: • The methods used to assess on-going risk of the solution; • How and when updates to the system baseline are performed; and • How such changes are communicated to affected merchants. The risk-assessment policy and procedures must be reviewed at least annually. It is not considered acceptable for the policy to require a minimum number of PIN CVM applications to be using a vulnerable platform before it is removed from the system baseline.	*The solution provider should have a documented risk-assessment policy and procedure, which is reviewed at least annually.* *This policy should include the methods used to assess on-going risk of the solution, how and when updates to the system baseline are performed, and how such changes are communicated to affected merchants.* *It is not considered acceptable for the policy to require a minimum number of PIN CVM applications to be using a vulnerable platform before it is removed from the system baseline.*
11. Thresholds for minimum acceptable PIN CVM application versions must be maintained by the solution provider. A risk-assessment methodology must exist, be documented and followed to ensure that merchants are using the most current acceptable version of the PIN CVM application. In instances where a merchant is using an acceptable version, but it is not the current, there must be notifications sent to the merchant to require them to update it. PIN CVM applications using a version that is not within the version threshold must not be permitted to accept PIN data. Installation of previous versions of the PIN CVM application must not be permitted.	*The solution provider should maintain thresholds for minimum acceptable PIN CVM application versions. A risk-assessment methodology should exist, documented and followed to ensure that merchants are using an acceptable version of the CVM app. For example, in instances where a merchant is using an acceptable version, but not the current version, there should be notifications sent to the merchant to require it to update.* *A PIN CVM application version that is not acceptable should not be permitted to accept PIN data.*

3.6 Basic Protections

Requirements	Guidance
1. When the back-end monitoring system and back-end attestation component reside in an organization's cardholder data environment (CDE), each of these must adhere to PCI DSS, including DSS Appendix A3: Designated Entities Supplemental Validation (DESV).	*Implementation of industry-recognized logical and physical protections are necessary for the confidentiality, integrity, and availability of the solution back-end environments. Appropriate scoping and identification of controls assist with ensuring the back-end monitoring system and back-end attestation component environments are adequately protected.*
2. If PAN is not present in the back-end monitoring and attestation systems' environment and it is not part of an organization's existing CDE, the environment must comply with the logical and physical security requirements as defined in Appendix A.	*PAN includes clear-text PAN and encrypted PAN. Encrypted PAN may be out of scope if it can be verified by a PCI QSA that PAN decryption mechanisms or PAN decryption keys are not accessible from the monitoring and attestation environments.*
3. All traffic to/from back-end monitoring and attestation systems must be strictly controlled.	*Prevents unauthorized communication and processes from the PIN CVM application and SCRP to the back-end monitoring system and back-end attestation component from gaining access.* *Ensures that all traffic to/from authorized PIN CVM application and SCRPs can be validated by back-end monitoring systems and back-end attestation component.*

3.7 Operational Management

Requirements	Guidance
1. Documented procedures to support the operation of the monitoring environment must exist and be demonstrably in use.	*Supports controlled operations and management of the environment and ensures common understanding for those involved in the operations of the environment.*
2. Staff responsible for monitoring environment duties must be provided up-to-date security training upon hire and at least annually in order to support monitoring, alerting and response responsibilities.	*Staff responsible for supporting the monitoring environment have specific training needs exceeding that which is typically provided by general security awareness training. Additional specialized training should focus on vulnerability management, monitoring/alerting, problem solving, systems baseline, etc. in order to perform duties completely and correctly.*
3. Reviews must be performed at least quarterly to verify operational procedures are being followed. Reviews must be performed by personnel assigned to the security governance and include the following: • Confirmation that all operation-management processes are being performed • Confirmation that personnel are following security policies and operational procedures—for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.	*Business as usual procedures and processes should be followed to ensure continued security of the environment. BAU breakdowns lead to non-compliance but more importantly risk of security exposure.* *The intent is to provide evidence as requested for audits.*

Module 4: Solution Integration Requirements

Control Objective: *Overall oversight, governance and responsibility of the solution is necessary to ensure all security controls are in place and functioning as intended.*

The solution provider is responsible for ensuring these requirements are implemented.

4.1 Pairing of Disparate Components

Requirements	Guidance
The PIN CVM application and SCRP must be uniquely identified and paired, and this pairing validated by the monitoring system at each startup of the application, as well as during any tamper-detection scans.	
1. Mechanisms must exist to identify and validate the SCRP and PIN CVM application as authorized prior to communication of any sensitive data between the SCRP and PIN CVM application.	*The PIN CVM application and SCRP should be uniquely identified and paired, and this pairing validated by the monitoring system at each startup of the application, as well as during any tamper-detection scans.* *This will ensure that all communications are coming from a legitimate and authorized PIN CVM application and SCRP.*
2. The monitoring system must be able to associate the PIN-based transaction to a specific merchant, COTS device and SCRP combination for tracking. If not successful, the transaction must fail.	*The back-end monitoring systems should be able to uniquely identify all transaction details for tracking based on the following at a minimum:* • *COTS device used for the transaction;* • *SCRP used for the transaction;* • *Merchant details for the transaction; and* • *PIN processing details for the transaction.* *If the CVM Application or SCRP fails in any way, the transaction should fail. This will ensure transactions will not be manipulated by any malicious activity. The back-end monitoring should be able to detect these failures and take appropriate action to block transactions coming from COTS, CVM Applications or SCRPs where failures are occurring in real time.* *Note: If an optional MSR is implemented in accordance to* Software-based PIN Entry on COTS™ Magnetic Stripe Readers Annex*, then magnetic-stripe read transactions may continue to be accepted for non-PIN based transactions even in situations where the SCRP is unavailable subject to the controls described in the SPoC Annex.*
3. The back-end monitoring system must be able to accept and process attestation data from the SCRP and PIN CVM application and take appropriate action based on predefined rules (for example, suspending transactions).	*The monitoring system should implement methods to actively detect and respond to events.*

4. The back-end monitoring system must establish mechanisms to ensure attestation data is refreshed and up to date.	*Maintaining and using the current attestation data every time is important to ensure the integrity of the COTS, SCRP, and PIN CVM application to ensure that established controls have not been modified.*

4.2 Secure Channels

Requirements	Guidance
Secure channels must be established to protect all communications between the solution components. The secure channels must be implemented to prevent MITM and replay attacks and provide mutual authentication and unique identification of each component.	
1. A secure channel must exist between each of the physically and logically disparate components of the system.	*The various components that make up the solution exchange information between them. The secure channel used for that purpose should demonstrate data confidentiality and authenticity during the establishment and subsequent usage of the channel to ensure 1) data sent is the data received and 2) data sent is to the intended recipient. Ensure no secret or sensitive data is transferred between the devices prior to the establishment of the secure channel.*
2. Each secure channel must provide mutual authentication to uniquely identify each component prior to exchanging sensitive data, as well as protect against MITM and replay attacks. Mutual authentication between the communicating components must be based on cryptography that aligns with Appendix C — Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms of this document.	*The ability to uniquely identify each of the channels established between the various components that make up the software-based PIN Entry Solution so that changes to these of components can be detected and potentially flagged as tamper events by the monitoring system.*
3. Cryptographic keys used to establish secure channels between components and for data encryption must be unique, except by chance.	*A different set of cryptographic keys is required for channel encryption versus data encryption to ensure key separation.*
4. Documentation must exist and be maintained to identify logical connections between the PIN CVM application and other components of the system. Documentation must identify how data confidentiality and authenticity is maintained.	*Documentation of the connections between the various components that make up the software-based PIN Entry Solution will assist in the testing of the solution as well as the subsequent implementation. It will help identify where each security control exists and how it has to be managed.*
5. Use of standard protocols must prevent against downgrade attacks.	*Many communication protocols support backward compatibility with previous versions of the protocol that may have vulnerabilities. Hence, solutions should ensure that such downgrades to unsecure versions of the protocol will not happen.*

4.3 PIN CVM Solution Requirements

Requirements	Guidance
Overall oversight, governance and responsibility of the solution is necessary to ensure all security controls are in place and functioning as intended. *The solution provider is responsible for ensuring these requirements are implemented.*	
1. A user guide that provides information about the solution, including identifying control points and security responsibilities for the merchant(s) must exist and be made available to the merchant.	*Documentation to support the use and management of the solution provides for common knowledge and definition of procedures to ensure the security controls are in place and functioning as intended.* *User guide information should address implementation and administration tasks associated with the solution as well as guidance on maintenance for technical controls and processes.*
2. The security assets of the solution must be identified and managed. At a minimum, the solution provider must ensure identification of authorized SCRPs, linking SCRPs to the PIN CVM application and back-end monitoring environment and verification that firmware/application updates are current.	*Appropriate device registration and linking them to authorized processes and system components reasonably ensure that substitution of rogue devices is prevented.*
3. The solution must be "online," connected to the back-end systems (monitoring, attestation component and processing) and in an operational state before initiating any PIN entry functions.	*As most of the security controls and mechanisms involve the ability of the solution to monitor and mitigate via controls located and coordinated by the back-end environment, the ability to be connected to the back-end environment is critical. Hence, connectivity is necessary between the PIN CVM application and the back-end systems to facilitate execution of various controls including but not limited to attestation functions.*
4. The SCRP and PIN CVM application (including the attestation component) must have the ability to be identified as authorized and validated to the monitoring environment, by cryptographic means, before initiating a PIN entry session.	*Verification of the correct and expected state of the solution components is necessary to ensure subsequent processing is secure. This process should include the establishment of a system baseline that can then be used to ensure that changes are expected or authorized.*

4.3 PIN CVM Solution Requirements

Requirements	Guidance
5. The solution must incorporate a detection system or feed other detection systems capable of detecting anomalous and potentially fraudulent activity, including suspicious transactions.	*Detection systems should assist with monitoring, detecting and blocking suspicious or fraudulent transactions and be capable of issuing timely alerts to responsible personnel upon detection. Alerts should be acted upon in accordance with documented investigation and response procedures.* *Examples of activity that should be monitored for relative to PIN-based transactions include:* • *Unusual transaction velocity at the merchant level.* • *Anomalous merchant activity related to geographic origin of transactions* • *Unusual individual PIN authorization attempts that may be associated with probing or testing* • *Signals associated with cardholder/merchant collusion involving PIN-based transactions*
6. Plans and procedures must be defined to address interruptions to the solution due to unplanned business disruption, major disaster or failure of services. Testing to ensure viability of such plans and procedures must be performed annually at a minimum.	*Adequate preparedness is necessary for business continuity of processing and security of the solution.*
7. The solution provider must have a documented risk-assessment policy and procedure, which is reviewed at least annually. This policy must include the methods used to assess on-going risk of the solution as well as how and when updates to the system baseline are performed and how such changes are communicated to affected merchants.	*As the security landscape changes, platforms or OSs that may have been acceptable under the system baseline may become vulnerable. A documented policy and procedure for assessing these changes should exist and provide details on how decisions are made to remove previously acceptable platforms from the system baseline. The policy should also define how affected merchants using these platforms are notified and the plan to migrate them to the supported platform.* *The solution provider cannot use the number of merchants using a vulnerable platform as the only criterion to keep a vulnerable platform on the approved list of system baseline.*

4.3 PIN CVM Solution Requirements

Requirements	Guidance
8. A threat-management process must be established to monitor for newly discovered vulnerabilities that may impact the security of the solution. A risk assessment of these vulnerabilities must be performed against currently implemented security and attestation controls to: • *Determine the residual risk and* • *Ensure that the vulnerability does not change the baseline integrity of the solution.*	*As vulnerabilities are constantly being announced and discovered, a process with resources to proactively monitor and evaluate each vulnerability as it is announced will ensure that the organization is able to modify its detection and response process to accommodate new vulnerabilities.*
9. The solution configuration and release management process must be integrated with the threat management process. The firmware- and software-release process must take input from the threat-management process on the development of the minimum viable product (MVP).	*With the assessment of new vulnerabilities, the solution provider should ensure mitigation controls to address any incremental risks as a result of the vulnerability is quickly taken into consideration in the development of the next product release. This will allow accelerated integration of critical security patches to be deployed via firmware and software updates to the solution in the field.* *Where machine learning or other methods are employed to allow for the monitoring system to automatically adapt to changes in the risk landscape, protections should be put in place to prevent "data poisoning" or other types of adversarial manipulation of input data to cause invalid rules to be put in place by the system.* *Given the dynamic nature of the software risk/vulnerability discovery process, the solution provider is expected to have a tightly integrated process where the development team and the threat management team are closely collaborating to identify and mitigate any threats to their solution and environment.*
10. The the solution Provider must provide the PCI-approved lab with a test platform to evaluate the solution. This test platform must be developed in a manner that provides full accessibility and visibility into the solution. The test platform must provide an interface or a report that would enable an external company to validate the detection of potential vulnerabilities present on systems used in the testing.	*To enable testing and continued validation of the detection and response capability of the solution, visibility into the monitoring environment should be provided to the assessor during the testing so that the assessor can validate claims by the vendor that indicators of anomalous behaviors are detected. The platform will enable the assessor to validate compliance to the monitoring requirements that require the establishment of an initial system baseline as well as subsequent changes and updates to that baseline.*

4.3 PIN CVM Solution Requirements

Requirements	Guidance
11. All encryption keys associated with the SCRP must be injected by a key-injection facility that meets the PCI PIN Security Requirements, including Normative Annex B, "Key Injection Security Requirements."	*Secrecy of encryption keys is fundamental to the protection of sensitive data. Ensuring encryption-key loading is performed by an organization that understands and complies with key-loading requirements supports this principle.*

Module 5: Back-end Systems – Processing

Control Objective: *The environments that decrypt cardholder data and PIN data and process the payment transaction subsequent to the solution must adhere to payment industry requirements for the protection of cardholder data and PIN processing.*

5.1 Security of Cardholder Data and PIN Processing Environment

Requirements	Guidance
1. Decryption of all cardholder data and PIN data received from the SCRP must only occur in back-end payment and PIN-processing environments, respectively.	*The solution has outlined specific technical and procedural controls to protect the secrecy of PIN and cardholder data. Therefore, decryption of this information should only be performed in environments designated and authorized to perform these functions. The back-end payment and PIN-processing environments require security controls that are separate and distinct from this standard to address the risks of clear-text data in those environments.*
2. The processing environment that performs the decryption of the cardholder data must maintain and comply with PCI DSS requirements. Additionally, if the monitoring environment is located within the CDE, the processing environment must also comply with DSS Appendix A3: Designated Entities Supplemental Validation (DESV).	*To ensure the confidentiality and integrity of the cardholder data, verification that data decryption is only performed in a PCI DSS compliant environment is required. Environments that are PCI DSS compliant demonstrate that the minimum set of industry expected security controls have been applied to that environment which reduces the risk over environments that do not have security controls applied.*
3. PIN processing performed in the processing environment must meet the PCI PIN Security Requirements.	*PCI PIN Security Requirements define the industry security requirements for PIN-processing environments to protect against compromise or exposure of PIN data. Back-end systems that perform PIN decryption and their conformance to these requirements ensure the cardholder's PIN is protected throughout the transaction.* *To ensure the confidentiality and integrity of the PIN-block decryption process, use of a PCI-approved or FIPS140-2 Level 3 or above HSM in the back-end processing environment is the only acceptable means for PIN decryption.*

Module 6: Secure Card Reader (SCRP)

Control Objective: *Reduce the likelihood and limit potential impact of unauthorized disclosure and data compromise by ensuring cardholder data-acceptance devices specially designed for PIN entry on COTS—e.g., SCRP—are certified to recognized industry security requirements for design and manufacturing.*

6.1 Use of a PCI PTS Approved Device

Requirements	Guidance
1. The solution must require the use of a PCI PTS approved SCRP for the COTS device for EMV chip cards.	*SCRP is a PTS approval class that supports software-based PIN entry for EMV transactions on a COTS device according to these requirements. Characteristics of SCRP include:* • *Has the ability to receive an encrypted PIN from the PIN CVM application.* • *Will securely translate the PIN into the appropriate PIN block and re-encrypt.* • *Support functionality to support both methods of offline PIN verification specified by EMV.* *Optionally, in accordance to Software-based PIN Entry on COTS™ Magnetic Stripe Readers Annex, the SCRP may provide the physical interface necessary for reading magnetic stripe cards. Software PIN entry is not permitted for magnetic stripe read transactions.* *SCRPs are listed on the PCI Approved Device List.*

Appendix A: Monitoring Environment Basic Protections

PAN is the underlying factor for determining the applicability of PCI DSS security requirements. Recognizing that PAN may not exist in the back-end monitoring system and the back-end attestation component that supports the solution, the security requirements defined in this appendix define the minimum requirements that must exist to ensure fundamental security of the back-end monitoring system and back-end attestation component.

A.1 Governance and Security Policies

Requirements	Guidance
Control Objective: *Security policies set the security tone for the organization and inform personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.*	

A.1 Governance and Security Policies

Requirements	Guidance
1. Executive management must establish responsibility for the protection of sensitive data and system components within the monitoring environment. Responsibilities include: • Overall accountability for maintaining compliance to all required standards • Implementing a security governance program • Providing updates to executive management on security initiatives and issues, at least annually.	*Executive management assignment of responsibilities ensures senior management visibility into the security of the monitoring environment and allows for the opportunity to ask questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the compliance program may be assigned to individual roles and/or to business units within the organization.* *An established governance program assists with the ongoing, business as usual activities necessary to maintain a strong security posture.* *Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. The level of detail provided to executive management should be appropriate for the particular organization and the intended audience.*

A.1 Governance and Security Policies

Requirements	Guidance
2. The security governance program must include: • Definition of activities for maintaining and monitoring overall standards compliance, including business-as-usual activities • Annual assessment processes • Processes for the continuous validation of security requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • A process for performing business-impact analysis to determine potential security and compliance impacts for strategic business decisions	*Establishing a governance program that monitors the health of its security controls allows the organization to be proactive in the event that a control fails within the solution. It supports effectively communicating activities and statuses throughout the organization.* *The program can be a dedicated program or incorporated into an over-arching compliance and/or governance program. It should include a well-defined methodology that demonstrates consistent and effective evaluation. Example methodologies include: Deming Circle of Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, and Six Sigma.*
3. Changes to organizational structure, for example a company merger or acquisition, change or reassignment of personnel with responsibility for security controls, must result in a formal (internal) review of its impact to the environment scope and applicability of controls.	*An organization's structure and management define the requirements and protocol for effective and secure operations of the monitoring environment. Changes to this structure could have negative effects to the processing and security of the environment by reallocating or removing resources that once supported the solution. Therefore, it is important to revisit monitoring environment scope and controls when there are changes to ensure to management structure to ensure required controls are in place and active.*
4. Documented polices must exist and be demonstrably in use to require background checks on staff involved with the monitoring environment.	*Performing background investigations prior to hiring potential personnel who are involved with the monitoring environment assists with hiring qualified personnel and reduces losses from an employee's dishonesty.*

A.1 Governance and Security Policies

Requirements	Guidance
5. Determine monitoring environment scope impact for all changes to systems or networks, including additions of new systems and new network connections. Processes must include: • Performing a formal impact assessment • Identifying applicable security requirements to the system or network • Updating monitoring environment scope as appropriate • Documented sign-off of the results of the impact assessment by responsible personnel	*Changes to systems or networks can have significant impact to the environment scope. For example, firewall rule changes can bring whole network segments into scope, or new systems may be added to the monitoring environment that was not protected to the same level previously.* *Organizations require processes to determine the potential impact that changes introduce to systems and networks within monitoring environment to ensure they do not negatively impact the security of the monitoring environment.*
6. Configuration standards must be defined and applied to system components within the back-end monitoring systems. Configuration standards must align with industry-accepted standards.	*Configuration standards support approved software versions, updates and security controls. They also assist with security management and baseline configurations that are approved by the organization.*
7. Configuration standards must include: • Changing all vendor-supplied default accounts and system settings • Removing or disabling all unnecessary system or application functionality • Preventing functions that require different security levels from co-existing on the same system component	*Requirements to harden IT resources provide reasonable assurance that malicious users cannot exploit well-known vulnerabilities.*

A.2 Secure Networks

Requirements	Guidance
Control Objective: *Businesses depend on the ability of their networks to operate. Protections to ensure network availability, security and reliability reduce risk to the organization.*	
1. Network and data-flow diagrams must exist to support the monitoring environment identifying architecture and security control points.	*Network and data-flow information—for example, diagrams or network mapping tools—document how networks are configured, the identity and location of system components and how systems are connected to each other and to other systems and all communication paths with trusted and untrusted networks. This information provides a common understanding and helps to identify where security controls could be overlooked.*
2. Network configuration and controls must be reviewed at least quarterly to ensure they remain active and relevant.	*Reviewing device configurations allows the entity to identify and remove any unneeded, outdated or incorrect rules and confirm that only authorized connections, ports, protocols, services and APIs are allowed and have not changed from the baseline. All other services, protocols and ports should remain disabled or be removed through periodic reviews. Review processes may include real-time monitoring and analysis, periodic maintenance cycles to ensure the controls are accurate and working as intended and periodic reviews of network traffic connectivity across ports, protocols and services. For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).*
3. Alerts must be generated for action by responsible personnel upon detection of suspicious activity or anomalies. Establish and follow procedures for investigation and response.	*An alert should be generated that is actively monitored and immediately investigated. Where suspicious traffic is automatically blocked, a record of the traffic should also be generated and investigated to determine whether action is needed to prevent further attack.*
4. Controls must be implemented to detect and/or block network attacks.	*Controls should be implemented at the perimeter and critical systems points. The controls include consideration of both network-based and application-based attack vectors. Methods of detection may include signature-based, behavioral and other mechanisms that analyze traffic flows. Examples of tools include IDS/IPS, host firewalls and real-time traffic analysis tools. All mechanisms—such as detection engines, baselines and signatures—should be configured, maintained and updated per vendor instructions to ensure optimal protection.*

A.2 Secure Networks

Requirements	Guidance
5. Mechanisms must be implemented to detect and prevent clear-text data from leaving the monitoring environment via an unauthorized channel, method or process, including generation of audit logs and alerts.	*Mechanisms to detect and prevent unauthorized loss of data may include appropriate tools—such as data loss prevention (DLP) solutions—and/or manual processes and procedures. Coverage of the mechanisms should include, but not be limited to, e-mails, downloads to removable media and output to printers. Use of these mechanisms allows an organization to detect and prevent situations that may lead to data loss.*
6. Penetration testing on segmentation controls must be performed at least every six months and after any changes to segmentation controls/methods to confirm monitoring environment scope.	*If segmentation is used to isolate networks, those segmentation controls should be verified using penetration testing to confirm they continue to operate as intended and effectively. Penetration- testing techniques should follow the existing penetration methodology as specified in PCI DSS Requirement 11.* *For additional information on effective penetration testing, refer to the PCI SSC's Information Supplement on Penetration Testing Guidance, X9.111 Penetration Testing, NIST SP800-115.*
7. File-integrity monitoring must be used to protect configuration files, executables and public keys/certificates used for security services on any back-end components of the attestation system.	*Changes that impact file integrity or the security posture of the attestation system must be detected by the attestation system.*

A.3 Vulnerability Management

Requirements	Guidance
Control Objective: *Identify security vulnerabilities in order to effectively determine mitigating controls and security requirements.*	
1. Implement controls to prevent and/or detect and remove malicious software. Controls must be active and maintained.	*Controls should prevent the introduction and execution of malicious software (malware). A combination of methods, tools and programs may be used – for example, anti-malware software, application whitelisting, host-based and network-based intrusion prevention tools and system instrumentation. A combination of real-time protection and periodic scans should be considered.* *The implemented controls should be kept current (e.g., updated signatures, baselines, etc.). Anti-malware controls should not be disabled unless specifically authorized by management on a case-by-case basis for a limited time period.*
2. Procedures to identify and rate vulnerabilities based on their criticality must exist and be in use. Procedures must align with industry-accepted practices.	*Not all vulnerabilities pose the same risk to an organization's environment. Vulnerabilities should be ranked and prioritized in accordance with an industry-accepted methodology or organizational risk-management strategy.*
3. Internal and external vulnerability scans to the monitoring environment must be performed at least quarterly to identify and address vulnerabilities.	*Malicious users exploit vulnerabilities in systems and application to gain unauthorized access to environments and sensitive information. Vulnerability scans provide a means for the organization to identify weaknesses that could be exploited and take corrective action to remove the risk. Rescans should be performed as needed to verify vulnerabilities have been addressed.* *Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds.*
4. External scans must be performed by a PCI SSC Approved Scanning Vendor (ASV). Internal scans are performed by qualified personnel.	*Internal vulnerability scans can be performed by qualified, internal staff or outsourced to a qualified third party. For scans managed by the entity, the entity should ensure that scanning engines and vulnerability fingerprints are up to date, and that the scanning engine is configured in accordance with vendor guidance documentation.* *Personnel should have sufficient knowledge to review and understand the scan results, and to determine appropriate remediation. Internal personnel that interact with the ASV should also be knowledgeable in the network architecture and implemented security controls, in order to provide the ASV with information needed to complete the scan.*

A.3 Vulnerability Management

Requirements	Guidance
5. Penetration test to the monitoring environment must be performed by qualified personnel at least annually.	*Penetration tests identify weaknesses in an organization's security boundaries and controls therefore are necessary to identify gaps and take corrective action.* *The penetration-testing methodology should be based on industry-accepted approaches and incorporate both application-layer and network-layer testing. The scope of testing should cover the monitoring environment perimeter and critical systems, and it should include testing from both inside and outside the network.*
6. Penetration test findings must be remediated based on predefined criteria that align with industry-accepted practices.	*Security patches and fixes should be implemented based on risk ranking. Where high-risk vulnerabilities cannot be addressed per defined criteria, a formal exception process should be followed, including approval by personnel with appropriate responsibly and accountability.* *Once remediation activities have been performed, penetrations tests should be performed as necessary to verify the remediation is effective and the identified vulnerability or security issue has been mitigated.*

A.4 Access Controls

Requirements	Guidance
Control Objective: *Access to information and security assets in the back-end monitoring and attestation environment is provided on least-privilege and need-to-know principles.*	
1. Access to system components and data must be based on least privileges and need to know that is specific to job functions or processes being performed.	*Access to system components should be appropriate for job functions to prevent misuse. Access to systems and data within the monitoring environment is restricted based on business need, while also accounting for the sensitivity of the data being transmitted between the systems.*
2. Documented procedures for granting and managing access must exist and be in use.	*Users with special access to create or modify other user IDs should follow established procedures to prevent errors or inadvertently grant unauthorized access. Procedures should address approval process for provisioning, monitoring, changing and revocation of accounts used to access the monitoring environment.*
3. Individuals must be assigned a unique user ID.	*Assigned unique IDs allow the organization to maintain individual responsibility and accountability for actions performed using the ID and is an effective audit trail.*
4. Controls must be implemented to protect the confidentiality and integrity of accounts and credentials.	*Implemented controls should protect the confidentiality and integrity of accounts for both local and remote users. The controls should include ensuring that account and credential information is securely transmitted and stored at all times.*
5. Mechanisms must be established to support the organization's password-composition policies, session timeout and inactivity rules.	*Organizations should have rules that govern the protection and use of user IDs and passwords to protect the organization IT assets.*
6. Controls must be defined and active for managing and monitoring third-party access to the monitoring environment.	*Third parties pose significant risks since they may be the "weak link" into the organization. Third parties' security posture may not be consistent with the monitoring environment, therefore understanding their security posture and limiting and controlling their abilities is required. Configuration and connection requirements should be defined and implemented for all access by third-party personnel – for example, ensuring accounts are enabled only during the time needed and disabled when not in use, and monitoring account activity when in use.*
7. All user access to system components in the monitoring environment must utilize multi-factor authentication.	*User access to sensitive resources and processes requires additional assurance and verification that the individual who is attempting access, is who they claim to be. Refer to PCI SSC Information Supplement – Multi-factor authentication for more information.*

A.4 Access Controls

Requirements	Guidance
8. User accounts and access privileges must be reviewed at least every six months to ensure user accounts and access are authorized and remain appropriate based on job function.	*Ensures that user access remains appropriate for job functions.* *Bi-annual review of user accounts and access privileges ensures that user access remains appropriate for the user's job functions and identifies inactive accounts that could be used to gain unauthorized access by malicious users. Inactive accounts should be removed from the system.*

A.5 Physical Security

Requirements	Guidance
Control Objective: *Ensure the physical premises and associated assets are protected in commensurate with the sensitivity and value of those premises and assets, and the information contained therein.*	
1. Documented policies and procedures must exist for physically protecting the system components and limiting access to the monitoring environment.	*Documented policies and procedures ensure common understanding and communicate management's expectation for securing these resources. It should include defining the physical access controls required to prevent monitoring environment being physically accessed by unauthorized persons. The controls should cover all physical access points and include procedures for managing onsite employees and third parties. Specific procedures should be defined for managing visitors, including a visible means for identification and escorts by authorized personnel.*
2. Physical access to monitoring environment must be monitored to ensure access is authorized and based on business need.	*The ability to oversee and review security controls assists with timely identification and the ability to address anomalies.* *Monitoring controls should include use of video cameras and/or access-control mechanisms. Data from video cameras and/or access-control mechanisms should be logged to provide an audit trail of all physical access to the environment.* *Monitoring and periodic reviews of physical access controls and audit logs should be performed to allow early identification of incorrect controls and for timely response to suspicious activities. Personnel should be trained to follow procedures at all times.* *All suspicious activity should be managed per incident security procedures.*
3. Procedures to remove access and return assets such as keys, access cards for terminated personnel or when job duties change must be defined and demonstrably in use.	*Individuals leaving the organization or moving to a different position with access to security assets poses risk and may lead to unauthorized access. Procedures assist with defining actions required to remove access and security assets in a timely manner.*
4. Media associated with the monitoring environment must be protected to ensure secure storage, transport and disposal of media.	*Physical media with which information assets are associated require the same level of protections as logical access to ensure consistent security protections.* *Controls and process should cover secure storage, transport and disposal of storage media. Specific controls/rigor may vary for different levels of sensitivity of the data stored on the media.*

A.5 Physical Security

Requirements	Guidance
5. Implement response procedures to be initiated upon the detection of attempts to remove clear-text data from the monitoring environment via an unauthorized channel, method or process. Response procedures must include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	*Defined and documented plans and procedures assist with responding to security incidents in a timely and efficient manner. Procedures should include response activities, escalation and notification, and cover all assets and processes that could impact the monitoring environment operations or data.* *The incident response plan should be comprehensive and include coverage of all systems.* *Communication and contact strategies should include required notifications. Incident response personnel/teams should be trained and knowledgeable in IR procedures, and be available to respond immediately to an incident.*
6. System back-up requirements for the monitoring environment must be defined and address the following: • Back-up copies of information, software and system images must be created and tested regularly. • The frequency and retention of backups must be adequate to support day-to-day production activities and sufficient to facilitate recovery and achieve recovery objectives associated with those systems that require a recovery capability. • Back-up information must be stored securely, with appropriate physical and environmental controls. • Duration and frequency must match documented retention policy.	*Information backups help maintain the integrity and availability of information. Backups from the monitoring environment support recovery of the monitoring environment in the event a disruption of services. Also, backups provide a point-in-time snapshot for investigation and analysis purposes.* *Frequency and retention of backups should align with the organization's overall risk-management strategy.*

A.6 Incident Response

Requirement	Guidance
Control Objective: *Address non-standard processing or events in order to prevent losses and maintain continuity of processing.*	
1. Procedures must be defined, documented and communicated to support incident response policies.	*Ensures common understanding and defines process to be followed to address non-standard processing or events.*
2. A process must be implemented to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit-logging mechanisms • Segmentation controls	*The ability to quickly identify and address anomalies in processing or failures in security controls reduces risk of losses.*
3. Respond to failures of any critical security controls in a timely manner not to exceed 48 hours. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time, start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure	*Well-defined procedures and processes limit exposure.*

A.6 Incident Response

Requirement	Guidance
4. Implement response procedures to be initiated upon the detection of attempts to remove clear-text data from the back-end monitoring and attestation environment via an unauthorized channel, method or process. Response procedures must include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	*Data loss-prevention techniques assist with identification of suspicious activity and notification to applicable support staff members.*
5. Incident response procedures must be reviewed and tested at least annually.	*Testing an organization's incident response procedures identifies inadequacies and required improvements that can be addressed prior to actual events.*

A.7 Audit Logs

Requirement	Guidance
Control Objective: *Audit logs accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection and problem identification. Prompt review of logs permits early detection of hackers, who otherwise might be encouraged by an apparent lack of monitoring.*	
1. Policies and procedures must exist and be demonstrably in use for generating and managing audit logs for all system components.	*Audit logs support common understanding and set management requirements.*
2. Audit logs must identify all security-related activity. At a minimum, they must include: • User-oriented security events—e.g., log-on and log-off • Successful and rejected network access attempts • Successful and rejected data and system access attempts • Changes to system and security configurations • System administrator and system operator activities • Use of administrative privileges • Use of system utilities and applications • Files accessed and the kind of access • Alarms raised by access-control systems • Activation and de-activation of protection systems, such as anti-virus systems and intrusion-detection systems (IDS)	*Audit logs should be able to reconstruct activities and have sufficient specificity to clearly identify events.*
3. Time synchronization must be in place for audit logs.	*Effective forensics requires audit logs to be synchronized to adequately correlate events.*
4. Audit logs and security events must be monitored to identify anomalies or suspicious activity.	*Ongoing review ensures timely identification and response to prevent losses.*
5. Audit logs must be protected to prevent modification or deletion.	*Malicious users attempt to hide their presence and activity by changing audit log entries. It is imperative that the integrity of audit logs is preserved.*
6. Audit logs must be retained for least one year, with a minimum of three months immediately available for analysis.	*Retention facilitates access to audit logs for investigations.*

A.7 Audit Logs

Requirement	Guidance
7. A methodology must be implemented for the timely identification of attack patterns and undesirable behavior across systems—for example, using coordinated manual reviews and/or centrally managed or automated log- correlation tools—to include at least the following: • Identification of anomalies or suspicious activities as they occur • Issuance of timely alerts upon detection of suspicious activity or anomaly to responsible personnel • Response to alerts in accordance with documented response procedures	*Analysis of network activity assists with identification of non-standard processing that may be the result of malicious activity.*

Appendix B: Software Tamper-responsive Attack Costing Framework

Details associated with this Appendix can be found in *Software-based PIN Entry on COTS Test Requirements*.

Appendix C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange or establishment and for data protection in connection with these requirements. Other key sizes and algorithms may be supported for non-PCI payment brand relevant transactions:

Algorithm	RSA	Elliptic Curve	DSA	AES
Minimum key size in number of bits:	2048	224	2048/224	128

Key-encipherment keys must be at least of equal or greater strength than any key that they are protecting. This applies to any key-encipherment keys used for the protection of secret or private keys that are stored or for keys used to encrypt any secret or private keys for loading or transport. For purposes of this requirement, the following algorithms and key sizes by row are considered equivalent.

Algorithm	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	2048	224	2048/224	–
Minimum key size in number of bits:	3072	256	3072/256	128
Minimum key size in number of bits:	7680	384	7680/384	192
Minimum key size in number of bits:	15360	512	15360/512	256

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

For implementations using Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH):

- **DH implementations entities** must securely generate and distribute the system-wide parameters: generator *g,* prime number *p* and parameter *q,* the large prime factor of (*p* - 1). Parameter p must be at least 2048 bits long, and parameter q must be at least 224 bits long. Each entity must generate a private key x and a public key *y* using the domain parameters (*p, q, g*).
- **ECDH implementations entities** must securely generate and distribute the system-wide parameters. Entities may generate the elliptic curve domain parameters or use a recommended curve (see *FIPS186-4*). The elliptic curve specified by the domain parameters must be at least as secure as P-224. Each entity must generate a private key *d* and a public key Q using the specified elliptic curve domain parameters. (See FIPS 186-4 for methods of generating d and Q.)

- Each private key must be statistically unique, unpredictable and created using an approved RNG as described in this document.
- Entities must authenticate the DH or ECDH public keys using DSA, ECDSA, a certificate, or a symmetric MAC (see *ISO 16609 – Banking – Requirements* for message authentication using symmetric techniques. One of the following should be used: MAC algorithm 1 using padding method 3, MAC algorithm 5 using padding method 4.

PIN encryption within the SCRP must adhere to ISO 9564 Part 2 approved algorithms for PIN encryption. If TDES is used, keys must have a minimum strength of 112 bits.

TLS implementations must prevent the use of cipher suites that do not enforce the use of cryptographic ciphers, hash functions and key lengths as outlined in this Appendix.

For hash algorithms used for authentication or security purposes, only the following algorithms and associated bit lengths are permitted:

Algorithm	Length
SHA2 family	>255
SHA3 family	>255

Appendix D: Application Security Requirements

The following are software application requirements and corresponding guidance that provide a baseline for software application development activities that support the solution. Design, development and software maintenance used by a vendor affect the overall security of the solution, therefore it is important that these vendor processes adhere to industry recognized and accepted practices.

Application Security Requirements	Guidance
1. The software development process must be based on a formal process for secure development of applications, which includes: • Development processes based on industry standards and/or best practices • Information security incorporated throughout the software development life cycle • Security reviews performed prior to release of an application or application update At a minimum, the documentation must include quality controls standards and measurements as well as change-control practices to ensure oversight of the development processes.	*Without the inclusion of security during the requirements definition, design, analysis and testing phases of the software-development process, security vulnerabilities can be inadvertently or maliciously introduced into application code.* *Examples of secure software development practices include:* • *ISO/IEC 27034 application security guideline* • *NIST Special Publication 800-64 Revision 2* • *SEI CERT Coding standards* *Documentation should include techniques and methods used and include specific notes on how things should be done to ensure security controls are functioning as well as how to prevent vulnerabilities through misconfigurations, etc.* *Included in vendor document should include information that relates to the development process which can be audited. Examples of such documentation include:* • *Software quality procedures* • *Documentation and software control procedures* • *Change forms* • *Change-control logs* • *Change records*

Application Security Requirements	Guidance
2. Test data and accounts, user IDs and passwords must be removed before release.	*Test data and accounts should be removed from the application before it is released, since inclusion of these items may give away information about key constructs within the application.* *Pre-release custom accounts, user IDs and passwords could be used as a back door for developers or other individuals with knowledge of those accounts to gain access to the application, and could facilitate compromise of the application and related account data.*

Application Security Requirements	Guidance
3. Application code must be reviewed prior to release and after any significant change, to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines. • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. • Documented code-review results include management approval, code author and code reviewer and what corrections were implemented prior to release. ***Note:*** *This requirement for code reviews applies to all application components (both internal and public-facing applications), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties.*	*Security vulnerabilities in application code are commonly exploited by malicious individuals to gain access to a network and compromise sensitive data. In order to protect against these types of attacks, proper code-reviewing techniques should be used.* *Code-review techniques should verify that secure coding best practices were employed throughout the development process. The application vendor should incorporate relevant secure coding practices as applicable to the particular technologies used.* *This may include the use of static and/or dynamic code analysis tools, as well as, validation of any known vulnerabilities and weaknesses in third party applications and libraries that are used.* *Reviews should be performed by an individual knowledgeable in the technology and experienced in code-review techniques in order to identify potential coding issues. Assigning code reviews to someone other than the developer of the code allows an independent, objective review to be performed.* *Correcting coding errors before the code is released prevents faulty code from exposing customer environments to potential exploit. Faulty code is also far more difficult and expensive to address after it has been deployed. Including a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.*
4. Secure source-control practices must be implemented to verify integrity of source code during the development process.	*Good source-code control practices help ensure that all changes to code are intended and authorized, and that changes are performed only by those with a legitimate reason to change the code. Examples of these practices include check-in and checkout procedures for code with strict access controls, and a comparison immediately before updating code to confirm that the last approved version has not been changed (for example, using a checksum).*

Application Security Requirements	Guidance
5. Applications must be developed according to industry best practices for secure coding techniques, including: • Developing with least privilege for the application environment. • Developing with fail-safe defaults (all execution is by default denied unless specified within initial design). • Coding techniques include documentation of how sensitive information (e.g., cryptographic material, certificates, PIN, etc.) is handled in memory. • Developing for all access point considerations, including input variances such as multi-channel input to the application.	*Developing applications with least privilege is the most effective way to ensure insecure assumptions are not introduced into the application. Including fail-safe defaults could prevent an attacker from obtaining sensitive information about an application failure that could then be used to create subsequent attacks. Ensuring that security is applied to all accesses and inputs into the application avoids the likelihood that an input channel may be left open to compromise.* *Attackers use various tools to capture sensitive data from memory. Minimizing the exposure of sensitive information while in memory will help reduce the likelihood that it can be captured by a malicious user or be unknowingly saved to disk in a memory file and left unprotected.* *This requirement is intended to ensure that consideration is given for how sensitive information is handled in memory. Understanding when and for how long sensitive data is present in memory, as well as in what format, will help application developers to identify potential insecurities in their applications and determine whether additional protections are needed.* *Failure to consider these concepts while developing code could result in the release of an insecure application and potentially excessive remediation at a later time.*

Application Security Requirements	Guidance
6. Up-to-date training must be provided in secure development practices for application developers at least annually, as applicable for the developer's job function and technology used, for example: • Secure application design • Secure coding techniques to avoid common coding vulnerabilities • Managing sensitive data in memory • Code reviews • Security testing (for example, penetration-testing techniques) • Risk-assessment techniques. ***Note:*** *Training for application developers may be provided in-house or by third parties. Examples of how training may be delivered include on-the-job, instructor-led and computer-based.*	*Ensuring developers are knowledgeable about secure development practices will help minimize the number of security vulnerabilities introduced through poor coding practices. Trained personnel are also more likely to identify potential security issues in the application design and code. Software-development platforms and methodologies change frequently, as do the threats and risks to software applications. Training in secure development practices should keep up to date with changing development practices.*
7. All applications must be developed to prevent common coding vulnerabilities in software-development processes.	*The application layer is high-risk and may be targeted by both internal and external threats. Without proper security, cardholder data and other confidential company information can be exposed. As industry-recognized common coding vulnerabilities change, vendor coding practices should likewise be updated to match.*
8. Software vendor must follow change-control procedures for all application changes. Change-control procedures must follow the same software development processes as new releases, and include the following: • Documentation of impact • Documented approval of change by appropriate authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out or product de-installation procedures	*If not properly managed, the impact of software updates and security patches might not be fully realized and could have unintended consequences.*

Application Security Requirements	Guidance
9. The software development process must document and follow a software-versioning methodology, including: • The format of the version scheme, including number of elements, separators, character set, etc. (consisting of alphabetic, numeric and/or alphanumeric characters). • Definition of what each element represents in the version scheme (for example, type of change, major, minor, security or maintenance release, etc.)	*Without a thoroughly defined versioning methodology, changes to applications may not be properly identified, and customers and integrators/resellers may not understand the impact of a version change to the application.* *Versioning methodology should include a defined version scheme that specifically identifies the elements being used, format of the version, hierarchy of different version elements and so on, for the particular application.* *The version scheme should clearly specify how each of the various elements is used in the version number.* *The version scheme can be indicated in a number of ways—for example, N.NN.NNA, where "N" indicates a numeric element and "A" indicates an alphabetic element. The versioning scheme should include identification of the character set (for example, 0-9, A-Z, etc.) that can be used for each element in the version.* *Without a properly defined version scheme, changes made to the application may not be accurately represented by the version number format.*

Application Security Requirements	Guidance
10. Risk assessment techniques (for example, application threat-modelling) must be used to identify potential application security design flaws and vulnerabilities during the software-development process. Risk assessment processes include the following: • Coverage of all functions of the application, including but not limited to, security-impacting features and features that cross trust-boundaries. • Assessment of application decision points, process flows, data flows, data storage and trust boundaries. • Identification of all areas within the application that interact with sensitive information or the monitoring system. • A list of potential threats and vulnerabilities resulting from data flow analyses and assign risk ratings (for example, high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of risk-assessment results for management review and approval.	*To maintain the quality and security of applications, risk-assessment techniques should be employed by application developers during the software-development process.* *Threat modeling is a form of risk assessment that can be used to analyze an application's constructs and data flows for opportunities where confidential information may be exposed to unauthorized application users. These processes allow software developers and architects to identify and resolve potential security issues early in the development process, improving application security and minimizing development costs.*

Application Security Requirements	Guidance
11. A process must be established to identify and manage vulnerabilities, as follows: • Identify new security vulnerabilities using reputable sources for obtaining security vulnerability information. • Assign a risk ranking to all identified vulnerabilities, including vulnerabilities involving any underlying software or systems provided with or required by the application. • Test applications and updates for the presence of vulnerabilities prior to release. • Perform application-layer penetration test at least annually or whenever there is a significant change that modifies security functionality.	*Developers knowledgeable of vulnerabilities within their own applications or in underlying components should then be able to resolve those vulnerabilities prior to release or implement other mechanisms to reduce the likelihood that the vulnerability may be exploited in the event a third-party security patch is not immediately available.* *Reputable sources should be used for vulnerability information and/or patches in third-party software components. Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing lists, or RSS feeds. Examples of industry sources include NIST's National Vulnerability Database, MITRE's Common Vulnerabilities and Exposures list and the U.S. Department of Homeland Security's US-CERT websites.* *Once vulnerability that could affect the application is identified, the risk that the vulnerability poses should be evaluated and ranked. This requires a process to actively monitor industry sources for vulnerability information. Classifying the risks (for example, as "high," "medium," or "low") allows vendors to identify, prioritize and address the highest risk items (for example, by releasing high-priority patches more quickly) and reduce the likelihood that vulnerabilities posing the greatest risk to customer environments will be exploited.* *Finally, adequate testing by a qualified internal (with organizational independence) or external third party should be included in application vulnerability management process to ensure that any identified vulnerabilities have been properly addressed prior to release. Without a formal review and acknowledgment from a responsible party, critical security processes may be missed or excluded, resulting in a faulty or less secure application.* *Additional information can be found in the PCI SSC Information Supplement, Penetration Testing Guidance.*

Application Security Requirements	Guidance
12. A process must establish for timely development and deployment of security patches and upgrades, as following: • Patches and updates are delivered in a secure manner with a known chain of trust. • Patches and updates are delivered in a manner that maintains the integrity of the patch and update code. • Provide instructions for customers about secure installation of patches and updates.	*Software updates to address security vulnerabilities should be developed and released to customers as quickly as possible once a critical vulnerability has been identified, to minimize the timeframe and likelihood that the vulnerability could be exploited.* *All software requires mechanisms to ensure its integrity and authenticity.* *Security patches should be distributed in a manner that prevents malicious individuals from intercepting the updates in transit, modifying them and then redistributing them to unsuspecting customers.* *Distribution for the mobile application component typically relies on commercially hosted application repositories like Google Play store or Apple App Store. While these repositories have mechanisms to ensure the integrity and authenticity of the software they distribute, it is expected that these not be relied upon to ensure authorized update to the software. The application should contain built-in mechanisms to ensure that updates are authorized.* *Security updates should include a mechanism within the update process to verify the update code has not been replaced or tampered with. Examples of integrity checks include, but are not limited to, checksums, digitally-signed certificates, etc.*
13. Release notes must be included for all application updates, including details and impact of the update and how the version number was changed to reflect the application update.	*Release notes with details about software updates, including which files may have changed, which application functionality was modified, as well as any security-related features that may be affected. Release notes should also indicate how a particular patch or update affects the overall version number associated with the patch release.*
14. A process must be implemented to document and authorize the final release of the application and any application updates. Documentation includes: • Signature by an authorized party to formally approve release of the application or application update • Confirmation that secure development processes were followed by the vendor.	*Without a formal review and acknowledgment from a responsible party, critical security processes may be missed or excluded, resulting in a faulty or less secure application.*

Application Security Requirements	Guidance
15. Develop, maintain and disseminate an implementation guide that must: • Provide relevant information specific to the application • Address all requirements in this document • Include a review at least annually and upon changes to the application and is updated as needed to keep the documentation current with all changes affecting the application, as well as to the requirements in this document.	*A well-designed and detailed implementation guide helps in the implementation of appropriate security measures and configurations within the application and its underlying components to meet the relevant SBPE requirements for protecting sensitive information.* *With each application update, system functionality and, in some cases, critical application security mechanisms are modified or introduced. If the implementation guide is not kept current with the latest versions of the application, users of the application could overlook or misconfigure critical application security controls that could ultimately enable an attacker to bypass such security mechanisms and compromise sensitive data.*