Security Standards Council

Guideline: PCI Mobile Payment Acceptance Security Guidelines

Version: 2.0

Date: September 2017

Author: Emerging Technologies, PCI Security Standards Council

PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users

Table of Contents

Foreword

The PCI Security Standards Council (PCI SSC) is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The rapid development of payment-acceptance alternatives using mobile technologies has led PCI SSC to consider its approach to developing and providing guidance to secure all implementations.

The PCI Security Standards Council charter provides a forum for collaboration across the payment space to develop security standards and guidance for the protection of payment card data wherever it may be stored, processed, or transmitted—regardless of the form factor or channel used for payment. All this applies when a merchant, service provider, or other entity accepts payment card data from its customers. When individuals load their own primary account numbers (PAN) into their personal devices, however, they are not required to validate those devices to PCI standards. At the same time, when one of those personal devices is transformed into a point of sale (POS) for a merchant to accept account data, there is a responsibility to protect that information. Thus, PCI standards begin to apply when a mobile device is used for payment card acceptance and may be subject to PCI DSS compliance as dictated by the payment brands' compliance programs.

This document focuses on payment-acceptance applications that operate on any consumer electronic handheld device (e.g., smartphone, tablet, wearable—or collectively, "mobile device") that is not solely dedicated[1] to payment-acceptance transaction processing, where the electronic handheld device has access to clear-text data, and the device is not PCI PTS eligible. For ease of reference, this subcategory is referred to as "Category 3, Scenario 2." This scenario does not include the use of a validated P2PE solution. Separate PCI standards and documentation available on the PCI SSC website deal with all other categories and scenarios:

- *Mobile Payment-Acceptance Applications and PA-DSS FAQs*)
- *PCI PTS POI Modular Security Requirements* (Category 1) – Payment application operates only on a PTS-approved mobile device.
- *PCI Payment Application Data Security Standard (PA-DSS)* (Category 2) – Payment application meets all of the following criteria:
    i. Payment application is only provided as a complete solution "bundled" with a specific mobile device by the vendor;
    ii. Underlying mobile device is purpose-built (by design or by constraint) with a single function of performing payment acceptance; and

[1] "Solely dedicated" means that the device is purpose built and not technically able to do anything but accept payments.

iii. Payment application, when installed on the "bundled" mobile device—as assessed by the Payment Application Qualified Security Assessor (PA-QSA) and explicitly documented in the payment application's Report on Validation (ROV)—provides an environment that allows the merchant to meet and maintain PCI DSS compliance.

- *Accepting Mobile Payments with a Smartphone or Tablet* (Category 3, Scenario 1) – Payment application operates on any consumer electronic handheld device (e.g., smartphone, tablet, wearable-or collectively, "mobile devices") that is not solely dedicated to payment acceptance for transaction processing. The scenario includes the use of an approved hardware accessory in conjunction with a validated P2PE solution.

PCI SSC agreed (see *PA-DSS and Mobile Applications FAQs*) that mobile payment-acceptance applications that qualify, as Category 3 will not be considered for PA-DSS validation until the development of appropriate standards to ensure that such applications are capable of supporting a merchant's PCI DSS compliance. The PCI SSC recommends that mobile payment-acceptance applications that fit into Category 3 be developed using PA-DSS requirements and the guidance provided in this document as a baseline.

The purpose of this document is to provide guidance to merchants on how to implement a secure mobile payment-acceptance solution. While not exhaustive, this document outlines a variety of both traditional and less conventional mechanisms to isolate account data and protect it from exposure.

Disclaimer

Please consider carefully the limitations of this document. In particular:

- No presumption should be made that meeting the guidelines and recommendations expressed in this document would cause a solution to be compliant with PCI DSS. Entities wishing to use such solutions would need to make their own risk assessments around the use of such solutions in consultation with their acquirers and applicable payment brands. Such solutions would be included in an entity's annual PCI DSS assessment to ensure that the application and its operating environment are compliant with all applicable PCI DSS requirements.
- Due to its rapid evolution, payment brands may have differing approaches to mobile payment acceptance. The guidelines and recommendations expressed in this document may not be sufficient by themselves to meet the specific requirements of all payment brands or territories. For example, manual key entry on a merchant-owned mobile device may be prohibited in some territories but permitted in others. For information and in the event of any doubt, please contact your acquirer and/or the relevant payment brands/territories.

1 Document Overview

1.1 Document Purpose and Scope

The Payment Card Industry Security Standards Council (PCI SSC) recognizes that merchants may use consumer electronic handheld devices (e.g., smartphones, tablets, wearables—or collectively, "mobile devices") that are not solely dedicated to payment acceptance for transaction processing. For instance, a merchant might use an off-the-shelf mobile device for both personal use and payment acceptance. Many of these devices have yet to incorporate generally accepted information security standards.

Since there is not a formal PCI SSC mobile security standard, these guidelines and best practices documents are produced to help educate and create awareness of challenges faced by the payment industry. This document focuses on guidance for merchants that plan to accept payments with a mobile device. Where merchants' mobile device hardware and software implementation cannot currently meet the guidelines documented herein, they may choose to implement a PCI-validated, Point-to-Point Encryption (PCI P2PE) solution. Implementing such a solution would include the addition of a PCI-approved Point of Interaction (POI) device. With the use of a validated solution, account data is encrypted by the POI, and the mobile device would simply act as the conduit through which the encrypted payment transaction is transmitted.

1.1.1 Implementation Scenarios

This document focuses on two different scenarios for implementing a mobile payment-acceptance solution. In the first scenario, the solution provider is responsible for the mobile app and all the back-end processes. Additionally, the solution provider is the device owner and has provided the devices to a merchant. In the second scenario, the solution provider is responsible for the mobile app and back-end processes, and the merchant is the device owner. Deciding who is responsible for which best practice can be confusing given the closely related and sometimes overlapping roles of the merchant and solution provider. For more clarity, see the "Best Practices and Responsibilities" matrix in Appendix B.

1.1.2 BYOD Scenario

There is one scenario this document does not discuss, and that is the BYOD (bring your own device) scenario. This is the scenario where an employee brings a device to work that the employee (who is not the merchant) owns and controls. Since the BYOD scenario does not provide the merchant with control over the content and configuration of the device, it is not recommended as a best practice.

This document provides guidance and good practice only, and does not replace, dilute, or remove any merchant's existing compliance requirements under PCI DSS. If you are in any doubt, please contact your acquirer.

1.2 Security Risks of Mobile Devices

This document defines mobile devices as consumer electronic handheld devices (e.g., smart phones, tablets, wearables—or collectively, "mobile devices") that are not solely dedicated to payment acceptance for transaction processing. These devices span a broad spectrum of features and functions ranging from cellular handsets that only support telephone functionality to "smart phones" and "tablets" that have a broader functionality.

Any risk that exists on a standard desktop or laptop computer may also exist on a mobile device. In addition, mobile devices may have a broader set of functionalities than standard desktop and laptop computers, resulting in more security vulnerabilities. Along with the standard communication methods of traditional desktop and laptop computers, mobile devices may also include multiple cellular technologies (e.g., LTE, CDMA, and GSM), GPS, Bluetooth, infrared (IR), and near-field communication (NFC) capabilities. Risk is further increased by removable media (e.g., SIM card and SD card), the internal electronics used for testing by the manufacturer, embedded sensors (e.g., tilt or motion sensors, thermal sensors, pressure sensors, and light sensors), and biometric readers. Furthermore, vendor and network operator-level logging and debugging configurations may introduce additional risks.

An inherent risk with mobile devices is the fact that they are ***mobile***. A mobile device with wireless connectivity allows it to be removed from a merchant's location, which is usually assumed to be safe, and taken to a location that is convenient for the customer. This can provide benefits to the merchant but it also creates many security risks. One of the risks to the merchant is the ease for a criminal to steal such a terminal, modify it, and return it without anyone realizing it was gone. Since the mobile device has no fixed location, keeping track of it, a clear merchant responsibility, becomes more challenging. Remember, merchants are the first line of defense for POS fraud and are involved in the execution of the vast majority of controls suggested or required by PCI SSC.

2 Introduction

2.1 Why mobile is different

The uniqueness of mobile devices introduces challenges in securing that environment. General-purpose mobile devices are often built with a goal of being easy to use by the consumer. These devices do not typically provide the same level of data security you would expect when using a payment card at a traditional retail store. Due to the design, almost any mobile application could access account data stored in or passing through the mobile device. This poses a challenge for merchants to demonstrate adherence to the PCI Data Security Standard.

Trust is even more significant for mobile payments because that environment is fragmented across manufacturers of devices, developers of operating systems, application designers, network carriers, and the use of various protocols to connect these different entities. Payment security has always been a shared responsibility. Ensuring mobile acceptance solutions are deployed securely requires that all parties in the payment chain work together in this effort.

PCI Mobile Payment Acceptance Security Guidelines discusses those challenges alongside opportunities to leverage emerging security controls. These controls should raise the confidence for all stakeholders to accept payments through a mobile device as a point of sale. While not exhaustive, this document outlines a variety of both traditional and less conventional mechanisms to aid the merchant in securely implementing a mobile payment-acceptance solution.

We often hear that security is about the people, processes, and technology. As you will see, this also holds true for mobile payment acceptance.

2.2 People

The same PCI principles apply to mobile for secure coding best practices and protection of account data but the people doing the coding are often different. Developers writing applications for mobile devices may not be the same developers who were trained to code web applications or traditional POS applications. As such, they may not be aware of their responsibility to create a secure work environment with quality assurance for the security that others will rely on.

Users of those applications, such as a new merchant, may be unaware of their responsibilities for safely accepting payment cards. The more secure the solution is prior to entering the market, the less risk there is to the merchant accepting payments on mobile devices. Still, adopting new technology requires a good amount of awareness for these businesses and their employees to operate the applications and devices correctly.

2.3 Processes

Several issues may arise when considering how to implement mobile acceptance processes. For example: If the reader fails, is there a manual key-entry process to accept payment card data securely? The business owner might use the mobile device both for accepting account data and for personal use; in which case, can the activities be segregated? What if the mobile device is owned by an individual and not the employer? This raises process challenges for updating the mobile device against malware and for other patch management as part of company procedure, as these processes may be deemed as invading the privacy of the device owner. Similarly, applications may be downloaded for personal use, and an enterprise may be unable to prevent and/or monitor mobile activity leading to unauthorized access to the account data. These are just some examples of the processes introduced by mobile devices that previously may not have been an issue for merchants using traditional, trusted POS terminals.

2.4 Technology

Technology to protect data within mobile devices is evolving at a rapid rate. How will these devices be developed to provide protection equivalent to current POS systems? Can the device mimic the protections of an Encrypting PIN Pad (EPP) and the trust it provides for access to PIN? Can the technology help detect fraudulent use of mobile devices? Can it also be designed to respond to tampering of the application or the mobile device? As the technology matures, solutions will emerge that provide confidence to merchants that they are securing their customers' data and preventing attacks against the powerful tool that they hold in their hand.

PCI Mobile Payment Acceptance Security Guidelines encourages the secure implementation of mobile payment-acceptance solutions to guard against both the expected and the unexpected attacks. It encourages monitoring for advancements that improve integrity and preparing for newly discovered threats. It advises diligence in the use and enforcement of policy and a newly required awareness for what is a safe transaction. By following these guidelines, merchants can safely implement a mobile payment-acceptance solution that will enable mobile commerce to flourish.

3 Mobile Payments Guidance Overview

The cardholder data environment (CDE) is comprised of people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components. This document does not focus on a PCI-validated P2PE solution, but on providing guidance to reduce security risks in otherwise noncompliant mobile devices.

This document organizes the mobile payment-acceptance security guidelines into the following three sections:

- **Section 4:** Objectives and Guidance for the Security of a Payment Transaction

  This section addresses the three main risks associated with mobile payment transactions:

  i. Account data entering the device,
  ii. Account data residing in the device, and
  iii. Account data leaving the device.

- **Section 5:** Guidelines for Securing the Mobile Device

  This section contains a non-exhaustive list of possible measures merchants should take regarding the physical and logical security of mobile devices.

- **Section 6:** Guidelines for Securing the Payment-Acceptance Solution

  This section consists of guidance for the different components of the payment-acceptance solution including the hardware, software, the use of the payment-acceptance solution, and the relationship with the customer.

4 Objectives and Guidance for the Security of a Payment Transaction

This section addresses the three main risks associated with mobile payment transactions:

i. Account data entering the device,

ii. Account data residing in the device, and

iii. Account data leaving the device.

An objective with associated guidance is given to address each of the three risks.

Objective 1: Prevent account data from being intercepted when entered into a mobile device.

Guidance:

If the solution incorporates PIN-entry capability, it should only occur through a PTS-approved PIN Entry Device, otherwise the merchant should contact its payment brand to ensure the solution has been approved for PIN entry. Additionally, when entering account data, the merchant should take measures to ensure that no one stationed nearby is "shoulder-surfing."

The merchant should verify that the mobile device accepting account data is authorized, by validating its hardware and electronic serial numbers. Additionally, the software, firmware, and application version numbers should be verified before account data is entered. The solution provider should supply the merchant with documentation that explains to the merchant how to accomplish this verification.

If an external device, such as a secure card reader, is used for account data entry into the mobile device, the merchant should ensure that the mobile device it intends to use has been approved by the solution provider for connection with the external device. It is essential that you enable all proper security functions on the mobile device and, where necessary, apply all security updates and patches in accordance with solution provider documentation.

Objective 2: Prevent account data from compromise while processed or stored within the mobile device.

Guidance:

The merchant should ensure that only trusted individuals have access to the payment application and its associated environment.

The mobile device should be stored in a secure location when it is not in use. The merchant should consider locking the mobile device to the merchant's physical location when possible. The merchant should place mobile devices in a manner that offers the greatest level of security (less customer and employee access), observation, and monitoring when possible.

Where data passes through a network under the merchant's control (e.g., Wi-Fi or Bluetooth), ensure

that it is implemented as a secure network per PCI DSS Requirement 4.

Objective 3: Prevent account data from interception upon transmission out of the mobile device.

Guidance:

Protect wireless transmissions per PCI DSS Requirements. Controls should include, but are not limited to the following:

- Change wireless vendor default encryption keys, passwords, and SNMP community strings.
- Facilitate use of industry best practices to implement strong encryption for authentication and transmission.
- Ensure that clear-text account data is never stored on a server connected to the Internet.

5 Guidance for Securing the Mobile Device[2]

Where a merchant either owns or is otherwise responsible for a mobile device being used as part of a payment solution, it is the merchant's responsibility to take steps to establish and maintain the security of that device. The measures described in this section should also be applied to any additional hardware components that form part of the mobile payment-acceptance solution (e.g., card readers).

5.1 Prevent unauthorized physical device access

5.1.1 The merchant is responsible for ensuring the integrity and security of the mobile device and its secure storage when not in use (e.g., locked in a cabinet, tethered to a counter, or under 24-hour surveillance).

5.2 Prevent unauthorized logical device access

5.2.1 Restrict logical access to the mobile device to authorized personnel. Consider using operating system multi-user support, if available, to separate user accounts and application data, and to restrict non-privileged access to the payment functionality.

5.2.2 Always use logical device access protection methods (e.g., biometrics, complex passwords, or multi-factor authentication) provided as part of a payment solution either in preference or in addition to built-in methods provided by the device or the operating system manufacturer.

5.2.3 If payment solution vendor-provided authentication measures are not present, merchants should require users to authenticate themselves positively to the device using a secure, built-in device-authentication method such as password, PIN, or pattern. Do not rely on "Slide" or similar methods, as they do not provide authenticated access security. If possible, configure the authentication method to force the user to re-authenticate to the device after a specified amount of time.

5.2.4 Merchants should consider using full device encryption on mobile devices, if available. This provides additional protection in the event of theft or loss of the device and may also prevent users from disabling device-level authentication.

5.3 Protect the mobile device from malware

5.3.1 As with other sophisticated computing devices, mobile devices are susceptible to infection by malware and other threats. Therefore, establish sufficient security controls to protect mobile devices from malware and other software threats. For example, install and regularly update the latest anti-malware software (if available). As another example, consider application wrapping, which can be employed with an MDM (Mobile Device Management) solution to prevent and/or remove malicious software and applications.

[2] See *PCI Mobile Payment Acceptance Security Guidelines for Developers* for more information.

5.3.2 Deploy security software products on all mobile devices including antivirus, antispyware, and software authentication products to protect systems from current and evolving malicious software threats. All software should be installed from a trusted source.[3] If anti-malware software is not available, employ MAM (Mobile Application Management) or MDM solutions that can monitor, evaluate, and remove malicious software and applications from the device. Furthermore, if possible, it is ideal to deploy both anti-malware and MDM solutions (mentioned above) to protect the device from malicious software and applications.

5.3.3 Merchants should not circumvent any security measures on the mobile device—e.g., enabling USB debugging if already disabled or rooting the mobile device.

5.3.4 To avoid introducing new attack vectors onto a mobile device, install only trusted software that is necessary to support business operations and to facilitate payment.

5.3.5 The merchant should require the following activities of its solution provider:

- The solution provider should regularly update their payment application and indicate to the merchant when updates are available and are safe to install.
- The solution provider should have restrictions on their payment application so that it only functions on a device running approved firmware.
- The solution provider should supply documentation that details any update procedures the merchant needs to follow.
- The solution provider should be in communication with the merchant and make them aware of newly discovered vulnerabilities in their payment-acceptance solution. Additionally, the solution provider should provide guidance to merchants when new vulnerabilities are discovered, as well as provide tested patches for any of these vulnerabilities.

5.4 Ensure the mobile device is in a secure state

5.4.1 It is strongly recommended that mobile devices be scanned by security software prior to the implementation of any payment solution, and regularly thereafter throughout the lifespan of the solution. Examples of functions that should be performed by such a scan are:

- Detecting unwarranted app privileges,
- Detecting apps that store clear-text passwords,
- Determining whether other apps have access to payment application data, and
- Detecting apps that are vulnerable to man-in-the-middle (MITM) attacks).

[3] A “trusted source” is to be defined by the solution provider.

5.4.2 The merchant should look for an indication of a secure state (e.g., by a displayed icon) as detailed by the solution provider. If no indication is present, the payment application should not be used.

5.4.3 Disabling USB debugging and disallowing of untrusted sources should be enforced on an ongoing basis. As an additional defense-in-depth, the device should be monitored for jailbreaking or rooting activity, and when detected the device should be quarantined by a solution that either removes it from the network or removes the payment-acceptance application from the device. Also, some attackers may attempt to put the device in an offline state to further circumvent detection, so offline jailbreak and root detection and auto-quarantine are also key.

5.4.4 When technically feasible, it is strongly recommended to utilize logging and monitoring solution for near real-time notification if a security state of the device was affected by known or unknown user activity. Whatever solution is selected to perform logging and monitoring of the mobile device, it is recommended any logging from the mobile payment acceptance solution be included.

5.4.5 Merchants should consider only using new mobile devices received in a factory state[4] configuration as part of a payment solution, and recognize that mobile devices whose history and provenance are unclear should be avoided.

5.5 Disable unnecessary device functions

5.5.1 Merchants should disable any communication capabilities not necessary for the functioning of the payment solution.

5.6 Detect loss or theft

5.6.1 An essential step in protecting your mobile device is to record identifying attributes of the device and its use. These attributes include but are not limited to the following:

- Serial number (hardware and electronic should match)
- Model number
- Operating system, firmware, and payment-acceptance application versions
- The merchant implementing some form of log that lists who is using the device, when, and where it is used

5.6.2 To help identify devices and control inventory, the merchant should mark each device with a unique identifier. For instance, mark the device with a ultra-violet (UV) security pen or an

[4] "Factory state" is the device state when received from an authorized representative of the OEM.

embedded RFI tag.

5.6.3 A process should exist for the timely detection and reporting of the theft or loss of the mobile device. Inherent to such a process should be a means for testing and for confirming that it remains active. Examples include the use of GPS or other location technology with the ability to set geographic boundaries, periodic re-authentication of the user, and periodic re-authentication of the device.

5.6.4 If a device is presumed to be lost or stolen, the merchant should immediately disable and securely wipe the device remotely. Note that this may require that the merchant notify the solution provider where such actions require execution by the solution provider.

5.7 Ensure the secure disposal of old devices

5.7.1. Merchants should dispose of old devices in a consistent manner. When guidance is provided by the solution provider, the merchant should follow it. Some items to consider include:

- Remove all tags and business identifiers.
- If possible, develop a contract with an authorized vendor who can help securely dispose of electronic materials and components.
- If possible, do not dispose of devices in trash containers or dumpsters associated with your business.

6 Guidance for Securing the Payment-Acceptance Solution

A mobile payment-acceptance solution consists of software and/or hardware components, which reside on or interface with a mobile device. For example, a solution might consist of a payment application and card-reader device that a merchant must install and set up to accept payments. These components must be protected using measures applied **in addition to** any that are undertaken to secure the mobile device.

6.1 Implement secure solutions

6.1.1 Merchants should only implement mobile payment-acceptance solutions that meet all relevant security requirements. Specific requirements intended to assist merchants in choosing an appropriate solution are provided in Appendix C: Solution Provider Selection Criteria.

6.2 Ensure the secure use of the payment-acceptance solution

6.2.1 Implement policies for secure use. To prevent unintended consequences from the misuse of a mobile payment-acceptance solution, ensure that the solution is used in a manner consistent with the guidance provided by an acquiring bank and solution provider. This includes ensuring that any software downloaded onto the mobile device comes from a trusted source. In addition, to ensure that the mobile payment-acceptance solution is treated like any other asset with cardholder data (CHD)[5].

6.2.2 Train users. The solution provider should provide the merchant with implementation instructions and possibly training materials. The implementation instructions and training materials should be understood and completed by any staff operating the payment-acceptance solution.

6.3 Prefer online transactions

6.3.1 By policy and by practice, the merchant should not use the mobile payment solution to authorize transactions offline or store transactions for later transmission, for example, when the mobile payment application on the host is not accessible.

6.4 Prevent unauthorized use

6.4.1 Access to any payment applications or other software residing on or accessed via a mobile device should be restricted to authorized personnel, and records should be maintained as appropriate.

6.4.2 Merchants should ensure they have the ability to manage access to payment-acceptance software on an ongoing basis, including enablement, changing permission levels, and revocation.

6.5 Inspect system logs and reports

6.5.1 The solution provider should ensure that logging capabilities exist with sufficient granularity to

[5] Refer to PCI DSS.

support detection of abnormal activities.

6.5.2 The merchant should work with its solution provider to ensure that any audit or logging capability is enabled. The solution provider should provide guidance to merchant on the merchant's responsibility to review the logs. Additionally, regularly inspect system logs and reports for abnormal activity. If abnormal activity is suspected or discovered, discontinue access to the mobile device and its payment application until the issue has been resolved. Abnormal activities include, but are not limited to, unauthorized access attempts, escalated privileges, and unauthorized updates to software or firmware.

6.6 Ensure that customers can validate the merchant / transaction

6.6.1 The merchant should ensure its service provider facilitates cardholders' ability to confirm that the merchant is a legitimate customer of their solution. This can be accomplished with ID cards, payment brand acceptance marks, serial numbers, a publicly available website with a list of registered merchants, or through other automated technologies that permit a cardholder to confirm quickly the validity of a merchant.

6.6.2 The merchant should determine that a mechanism exists to validate that the entity receiving account data is the intended recipient and agrees to protect the account data per PCI DSS Requirement 12.8.

6.7 Issue secure receipts

6.7.1 Regardless of the method used for producing receipts (e.g., e-mail, SMS, or attached printer), the method should mask the PAN in support of applicable laws, regulations, and payment-card brand policies. By policy and practice, the merchant should not permit the use of non-secure channels such as e-mail and SMS to send PAN or SAD.

Appendix A: Glossary

This glossary contains definitions of words and phrases that are specific to *PCI Mobile Payment Acceptance Security Guidelines.* For all other definitions, please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*.

Term	Definition
Application wrapping	Application wrapping typically involves the addition of a dynamic library to the existing application binary. This library can provide additional controls for certain aspects of the application—e.g., required user authentication, forced use of a VPN, or prohibit cut and paste.
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
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 (SAD)* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Card reader	A mechanism for reading data from a payment card.
Clear text	Intelligible data that has meaning and can be read or acted upon without the application of decryption.
Developer	An organization that architects, designs, or builds hardware or software components (e.g., manufacturer, operating-system software company, mobile network operator [MNO], third-party application software company, integrator, or implementer); this may include solution providers or merchants who modify or create hardware or software.
Encrypting PIN pad (EPP)	A device for secure PIN entry and encryption in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (e.g., an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell. Encrypting PIN pads require integration into UPTs or ATMs.
Entry Device	A type of electronic device that interacts directly with and takes input from humans to facilitate mobile payment acceptance.
GPS (Global Positioning System)	A satellite communication system that provides location and time information.

Term	Definition
Host-based	This refers to the computer at the solution provider—i.e., not the mobile device
Jailbreak/ jailbroken	The rendering of a cell phone such that it is no longer subject to the limitations originally imposed on it by its manufacturers/proprietors. Jailbroken mobile devices allow access to their proprietary operating system, which then allows the installation of third-party applications not released or controlled by the manufacturer or proprietor. Also, see *Rooting.*
Malicious software/malware	Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Mobile app	A program for a phone, tablet, or other mobile electronic device.
Mobile device	A consumer electronic handheld device (e.g., smartphone, tablet, or wearable) that is not solely dedicated to payment acceptance for transaction processing and that has wireless connectivity to a network (e.g., cellular or Wi-Fi).
Near field communication (NFC)	A short-range, wireless RFID technology that makes use of interacting electromagnetic radio fields instead of the typical direct radio transmissions. Refer to ISO/IEC 18092 for specifications.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Payment-acceptance application	Refers to only the application on the device and/or the host computer as applicable by context.
Payment-acceptance solution	Includes all hardware, software and processes of the solution.
Rich OS (Operating System)	An environment created for versatility where device applications—such as Android, Symbian OS, and Windows Phone, for example—are executed. It is open to third-party download after the device is manufactured.
Rooting	Gaining unauthorized administrative control of a computer system; also, see *Jailbreak/jailbroken.*
Secure Digital (SD) card/Micro-SD card	A non-volatile memory card format often used as additional memory for mobile devices.
Secure element	A formally certified, tamper-resistant, stand-alone integrated circuit often referred to as a "chip" as defined by the European Payments Council or other recognized standards authority.

Term	Definition
Sensitive authentication data (SAD)	Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Subscriber identity module (SIM)	A memory card that typically stores the IMSI (International Mobile Subscriber Identity) and other related information used to authenticate subscribers.
UPT (Unattended Payment Terminal)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment, including, but not limited to, the following: ▪ ATM ▪ Automated fuel dispenser ▪ Ticketing machine ▪ Vending machine

Appendix B: Best Practices and Responsibilities

The table below outlines each best practice described within this document along with who should be responsible for its implementation. The definitions of those entities that are responsible for the best practices include:

- **Merchant as an End User (M):** Any entity that utilizes the mobile payment-acceptance solution to accept payments
- **Mobile Payment-Acceptance Solution Provider (SP):** The entity that integrates all pieces in the mobile payment-acceptance solution and is responsible for the back-end administration of the solution. This includes the merchant as a solution provider.

Best Practice	M	SP
1. Prevent account data from being intercepted when entered into a mobile device.	X	X
2. Prevent account data from compromise while processed or stored within the mobile device.	X	X
3. Prevent account data from interception upon transmission out of the mobile device.		X
4. Prevent unauthorized physical device access.	X	
5. Protect mobile device from malware.	X	X
6. Ensure the device is in a secure state.		X
7. Disable unnecessary device functions.	X	X
8. Detect loss or theft.	X	X
9. Ensure the secure disposal of the device.	X	
10. Implement secure solutions.	X	X
11. Ensure the secure use of the payment-acceptance solution.	X	
12. Prefer online transactions.		X

Best Practice	M	SP
13. Prevent unauthorized use.	X	
14. Inspect system logs and reports.	X	X
15. Ensure that customers can validate the merchant / transaction.		X
16. Issue secure receipts.		X

Appendix C: Solution Provider Selection Criteria

The following checklist is provided to assist the merchant in selecting a solution provider for mobile payment acceptance. The ideal candidate would meet all applicable criteria; however, the criteria are provided to facilitate a discussion between merchant and solution provider and between the merchant and the merchant's sponsoring financial institution or acquirer. It is not intended as qualification or disqualification of a solution provider.

Criteria	Meets	Comments
1. Solution provider's host-based payment-acceptance application runs in a PCI DSS compliant environment as attested by a QSA.		
2. If the solution provider is providing the mobile device, maintenance and support are provided.		
3. The merchant will have the ability to contact the solution provider at any time.		
4. Solution provider has good documentation and training for merchant employees who will be end-users.		
5. Onboarding process includes provision of sample policies and procedures for merchant.		
6. Access control mechanism is in place with means for merchant to authorize, to monitor, and to revoke access privileges.		
7. Solution includes logging of user and device access and includes mechanism for reporting activity to merchant.		
8. Termination of agreement includes provisions for secure transfer of historic data back to merchant and removal of any merchant data from mobile devices (if such devices are returned to solution provider).		
9. Clear terms for warranty and liability that are not onerous to merchant.		

Appendix D: Additional Risks Associated with Mobile Devices

The number of possible attack vectors targeting mobile payment transactions will continue to increase and there will be risks associated with them. Secure payments that are made today may not be secure in the future for reasons that are not yet known or covered. Therefore, it is important to include some of the possible residual risks concerning device validation, jurisdictional differences, and technological limitations in this guideline.

D.1 Device Validation

Numerous manufacturers, carriers, software developers, and vendors take part in developing a single mobile device. The various combinations of these entities result in an extremely large number of unique mobile devices. The resulting lack of vertical integration would make a program to validate compliance to requirements difficult.

All the intervening steps during the production of a mobile device build upon components of the previous steps. For instance, a mobile network operator sells a mobile device manufactured by a specific handset company that contains a chip manufactured by one of several chip-manufacturers and that runs an operating system created by another third party. At each layer, the components added can either increase or decrease the security of the device. For the devices to be adequately tested and validated, proprietary information would have to be shared among all the contributors. If a manufacturer, software developer, or carrier refused to share security-critical proprietary information, validation would be unrealizable. Consequently, the validating of these devices would be problematic.

The unknown trustworthiness of mobile devices for which no independent, standardized security validation is done remains a residual risk.

D.2 Regional Jurisdiction

Rules and regulations pertaining to communications and forms of payment vary by jurisdiction. Preventative measures implemented in one jurisdiction may be unlawful to implement in another. For instance, remotely zeroizing a device (i.e., rendering it inoperative) may be legal in the US but not in the EU, since it may be unlawful to zeroize or otherwise do anything to a mobile device that would remove the user's ability to make emergency calls. Adjustments made to accommodate jurisdictional legal issues may adversely affect security. This is likely to remain an intractable residual risk.

D.3. Technological Limitations

D.3.1 Physical

A mobile device may be shielded in such a way that it may not have the capability of being zeroized remotely (e.g., a Faraday cage). For instance, today mobile phones are being stolen and immediately put into metallic bags that shield them from sending/receiving commands, thereby removing the ability to zeroize the device remotely before the device can be used to divulge sensitive information. This type of attack could also remove the ability to "track" the device.

D.3.2 Data Accessibility

Even with USB debugging disabled, other ways exist in which sensitive data can be accessed on a mobile device. Depending on the device, sensitive data may be accessible through the UART port, audio ports (e.g., headset connection and/or microphone), HDMI ports, IR ports, hardware test points (e.g., JTAG), or through various (non-native) phone states accessed by key sequences or combinations.

When a mobile device is in a non-native state like emergency recovery mode, it can often be backed up, re-flashed, or have its memory wiped. These actions can usually be performed from the user interface or an external device (e.g., a side-loaded ROM or executable from an SD card).

Mobile devices come with resets from the chipset manufacturer, device manufacturer, and the carrier. These resets can be referred to as public or private resets. Public resets are generally available to the user and can be accessed through the device's user interface. Private resets are generally not available to the user and require a key sequence, a passcode, or the device to be in a non-native state. Both public and private resets are usually not harmful to a device's security features, although many of these resets delete large amounts of data and access different memory locations. Therefore, resets could adversely affect the security and the basic functionality of the device. For instance, a harmful reset may remove the requirement for users to be authenticated to the device.

D.4. Indeterminable Risks

D.4.1 Evolution of Technology and Unforeseen Attack Vectors

In order to bypass security mechanisms such as a secure element or various biometric mechanisms, a person or organization might require very expensive and technologically advanced equipment. Today, attacks on security mechanisms like these are too difficult and not financially beneficial for the development of extensive countermeasures. However, in the future, this may not be the case and protecting against such attacks may become a higher priority.

Any new connections added to a device may result in additional risks in the future. There may be security vulnerabilities to components currently on the device of which the industry is unaware. For example, data captured by an embedded camera may prove to be an exploitable weakness.

D.4.2 Vulnerabilities Markets

There are criminal enterprises today devoted to finding vulnerabilities within devices and selling information. Individuals and organizations stand ready to buy the vulnerabilities with the intent of keeping them secret so they can exploit them when they choose. Until made public, these are "zero-day" exploits and, as such, are a residual security risk.

D.4.3 Intentionally Inserted Backdoors

At each step in the process of producing a mobile device, the potential exists for a renegade employee to introduce exploitable security vulnerabilities. Currently, no commercial vendors perform the level of hardware or software review necessary to assure detection of this kind of sabotage. Additionally, the level of employee screening feasible in these commercial enterprises is unlikely to prevent this insider threat. As a result, there is no realistic way of preventing these "zero-day" exploits. Exploitation by the employee or sale by the employee in the aforementioned vulnerability marketplace is a residual security risk.

D.5. Miscellaneous Risks

D.5.1 Network Connections

The mobile device will likely be connected to various networks using a variety of open protocols. Additionally, it cannot be assumed that the mobile device will operate within a network that is controlled by a securely implemented firewall.

D.5.2 Memory Management

Mobile devices are developed for the ease of use of the consumer with optimized usability. As a result, the memory-management techniques of mobile devices will shut down applications and discard data based on the needs of the system as a whole. These memory-management techniques will likely result in a payment-acceptance application being shut down before account data could be securely deleted.

Most mobile devices do not come with a secure subsystem (e.g., secure element) that could be used to isolate and store account data. Therefore, depending on the permissions of the application, any application can access any memory location on the mobile device.

D.5.3 Anti-malware

Current anti-malware products would be impractical to employ because of the tremendous amounts of resources required to run them (e.g., battery life significantly decreased). Additionally, such products would have no assurance that they could complete their testing before being terminated by the OS to release resources for other tasks.

D.5.4 Variation of Devices

Today, mobile devices are ubiquitous and the number of different platforms and variations in platforms is enormous. Each of these platforms seems to have new vulnerabilities being discovered constantly. The task of tracking and testing for all these vulnerabilities would be daunting and currently impractical.

D.5.5 Access Control

Mobile devices generally do not have secure, role-based access control mechanisms that may be needed to support multiple users. This would include access controls to the device and to the application data.

Appendix E: Industry Documents and External References

Following are the sources of reference for this document.

1. ANSI X9.112-2016, *Wireless Management and Security — Part 1: General Requirements*.
2. *Best Practices for Mobile Device Banking Security.* ATM Industry Association (ATMIA). 2008.
3. CTIA – The Wireless Association®: *Best Practices and Guidelines for Mobile Financial Services*, Version 01.14.2009, Effective Date: January 28, 2009.
4. World Bank Working Paper No. 146, *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing,* May 2008.
5. NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg, MD.
6. *Security of Proximity Mobile Payments* – A Smart Card Alliance Contactless and Mobile Payments Council White Paper, May 2009, Publication Number: CPMC-09001.
7. *White Paper Mobile Payments*, Version 5.0, 8th March 2017, Document EPC492-09.
8. NIST Special Publication 800-57, Part 1 Rev. 4 , *Recommendation For Key Management,* January 2016. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg, MD.
9. ISO/IEC 11770-5:2011 *Information technology -- Security techniques -- Key management*
10. *OWASP Top 10 Mobile Risks*. OWASP Mobile Security Project, The OWASP Foundation. February 13, 2017. WWW.OWASP.ORG
11. "Biometric Standards Program And Resource Center". NIST, 2017, https://www.nist.gov/programs-projects/biometric-standards-program-and-resource-center.
12. *ANSI X9.84-2010 (R2017) - Biometric Information Management And Security For The Financial Services Industry*. American National Standards Institute, 2010.
13. European Union Agency for Network and Information Security. Smartphone Secure Development Guidelines. ENISA, 2016, p. all.
14. *Effective Daily Log Monitoring*. PCI Security Standards Council, May 2016.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 700 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.