VERSION 1.1

16th November 2021

WisePad Q Security Policy

Table of Content

1 Introduction

1.1 Purpose and Scope

This security policy applies to the WisePad Q terminal, which is PCI PTS version 6.0 POI approved. It addresses the proper use of WisePad Q in a secure fashion. Improper use of WisePad Q will lead to incompliance to the PCI PTS POI Security Requirements version 6.0.

1.2 Audience

This policy is targeted for site administrators, managers, operators, technicians that can access the device during normal business operations and maintenance operations.

1.3 Reference

[1] ANSI X9.24-1:2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[2] ANSI X9.24 Part 2: 2016, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[3] ANSI X9.24 Part 3: 2017, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
[4] ANSI X9.8 Banking - Personal Identification Number Management and Security - Part 1: PIN protection principles and techniques for online PIN verification in ATM & POS systems
[5] ANSI X9 TR-39/TG-3 Retail Financial Services Compliance Guideline - Part 1: PIN Security and Key Management
[6] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements Version 6.0, June 2020
[7] Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide Version 1.9, June 2020
[8] C Programming Coding Style version 0.3
[9] Security Guidance version 1.0
[10] POI Transfer and Storage Guidance version 1.0

1.4 Glossary of Terms and Abbreviations

AES	Advanced Encryption Standard, a data encryption/decryption standard superceding DES and TDES
ATM	Automatic Teller Machine, a unattended terminal for banking operations
COTS	Commercial off-the-shelf. A mobile device that is designed for mass-market distribution and is not designed specifically for payment processing.
DES	Data Encryption Standard, a data encryption/decryption standard
DUKPT	Derived Unique Key Per Transaction, a symmetric key management standard
EMV	Europay MasterCard Visa, an entity governing ICC payment
GPRS	General Packet Radio Service, a data service on 2G and 3G cellular communication System
ICC	Integrated Chip Card, aka Smartcard
KDH	Key Distribution Host
LED	Light emitting diode
NFC	Near Field Communication, a short-range wireless communication standard
MAC	Message Authentication Code, a cryptographic digital digest of a message
OTA	Over-the-Air, used to denote remote operation such as remote firmware update
PCI	Payment Card Industry, an entity governing the security level of payment devices
PED	PIN Entry device
PIN	Personal Identification Number, a 4-12 digit numeric password associated with payment card
POI	Point of Interaction
POS	Point of Sales, referring to the terminal used to process the payment
PTS	PIN Transaction Security
RSA	Rivest-Shamir-Adelman Algorithm, an asymmetric encryption/decryption standard
SCRP	Secure Card Reader PIN approval class
SPoC	Software-based PIN-entry on COTS
TDES	Triple DES, a symmetric key encryption/decryption standard based on DES
TMS	Terminal Management System
USB	Universal Serial Bus

2 General Information

2.1 Product Type

WisePad Q is a handheld PIN Entry Device (PED), mobile Point of Sales (mPOS) payment device for payment processing in an attended environment. It provides the ability to conduct contact and contactless transactions. The device will be operated in Mobile Host Mode.

The PCI approval is only valid when using the device as described in this document.

2.1.1 Mobile Host Mode

When used in conjunction with a mobile phone or table, the mobile host device and WisePad Q together acts as a payment processing terminal at the point-of-interaction. The operation flow is partially controlled by the mobile host device and partially by the WisePad Q.

2.2 Product Functionality

2.2.1 Card Interface

WisePad Q is equipped with the following payment card interfaces:

- ICC/EMV Contact Card Reader
- NFC/EMV Contactless Card Reader
- Magnetic Stripe Reader

WisePad Q also has a built-in Secure Key Pad for entry of PIN associated with the payment card.

2.2.2 Communication Interface

WisePad Q can communicate with the mobile host device through one of the following interfaces:

- Bluetooth LE
    - Version 4.2
    - Mode 1 Level 4
- USB
    - Generic HID

2.2.3 User Interface

The user-interface consists of the following elements:

- A dot-matrix display
- 4 blue color LEDs for NFC indication
- Buzzer for transaction status indication
- 4x4 key pad
- 1 Button for reset the device hardware

WisePad Q has an internal battery and can be recharged via the USB interface.

3 Product Identification

Operators and owners of WisePad Q should get familiar with its appearance so that any alterations and tampering attempts can be detected and reacted to in a timely manner.

3.1 Product Appearance

3.2 Product Label

Product information is Laser-etched at the back of the device. This includes:

- Product Name
- Serial Number
- Hardware Version
- Compliance Logos, e.g., CE Mark

The operator should check that the information is complete and not altered, covered or otherwise rendered incomprehensible.

	Hardware Version no. WPC4x.01-xxxxxx-xxx The “x” are non-security relevant variables Firmware Version no. System Table WPC4x.01-xxxxx The “x” are non-security relevant variables

3.3 Information

Additional Information about the WisePad Q can be retrieved by sending the “Get Device Info” command to the WisePad Q through Bluetooth or USB

The following information will be sent to host:

- Model name
- Bootloader Version
- Hardware Version (refer to Hardware Version in Section 3.2)
- Firmware Version (refer to Firmware Version in Section 3.2)
- Serial Number

This data can also be read from the device after pressing the “power/menu” button.

3.4 PCI Listing

To verify that WisePad Q is a PCI approved device, visit the PCI Security Standards Council web site www.pcisecuritystandards.org.

4 Guidance

4.1 Delivery and Deployment Inspection

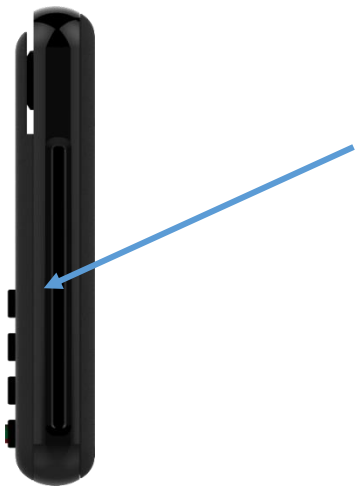
At the initial delivery and deployment of the WisePad Q the merchant or acquirer must visually inspect the device for signs of tampering. In particular, the following items must be checked:

- The label on the delivered/deployed device is complete and not altered.
- The Model and Serial Number match with the information provided in the documents that accompany the delivery/deployment, e.g., Delivery Note, Invoice, etc.
- The device is intact and there are no signs of tampering, such as torn labels, cracks, holes, loose or missing screws.
- No other attachments are added to the device: no overlay, inserts, plugs, wires or other unidentified appendages.
- The IC card insertion area of the device has no signs of tampers such as cracks or holes.
- No hidden objects are present inside the card slot

4.2 Regular Inspection

In normal operation environment, the merchant or acquirer must visually check the device for any signs of tampering every 24 hours. This includes:

- The label on the delivered/deployed device is complete and not altered.
- The device is intact and there are no signs of tampers such as torn labels, cracks, holes, loose or missing screws.
- No unidentified attachments are added to the device. Security locks and chains with known purposes are acceptable.
- The IC card insertion area of the device has no signs of tampers such as cracks or holes.
- No hidden objects are present inside the card slot



4.3 Operation Environment

The device should be used in an attended environment where the cardholder presents the card in the presence of the merchant or acquirer. WisePad Q is a handheld device which is given to the customer to enter the PIN. The body of the customer and the orientation of the device towards him will protect the PIN entered from visual observation.

When choosing the operation location, one should take into consideration the following:

- The presence of any surveillance camera that can unintentionally capture the PIN entered by a cardholder.
- The presence of any mirrors that can unintentionally reveal the PIN entered by a cardholder.

4.4 Decommissioning

The device may be removed from operation for the following reasons:

1. **Retiring of the device/discontinue of the device rental contract**:
   A remote decommissioning command will be sent from the TMS to the terminal via the authentication of TMK0 and this will reset the IKEK (the KEK to encrypt all other secret and private keys inside the terminal). The device will then be returned to the distributor/service centre either via face-to-face return/collect or via mail by a tracked courier.

2. **Repair of the device**:
   The device will need to be sent back to service centre either via face-to-face return/collect or via mail by a tracked courier. The terminal ID needs to be reported to the service centre before sending the terminal back, so the TMS can un-register the terminal from normal service.

3. **Decommissioning due to compromised keys**:
   A remote decommissioning command will be sent from TMS to terminal via the authentication of TMK0 and this will reset the IKEK (the KEK to encrypt all other secret and private keys inside the terminal). The device will then be recalled or recommissioned via remote key loading (in the cases that the compromised key(s) are not related to the keys and certificates to support remote loading)

The merchant should send the device back to repair centre according to their acquirer procedure. For detail, please refer to “Transfer and Storage Guidance”.

4.5 Firmware and Configuration Maintenance

4.5.1 Self-check

When the WisePad Q is turned on, a self-test is run to check the integrity of the firmware, configuration and keys. The firmware will also perform self-test automatically every 24 hours.

4.5.2 Firmware Update

The firmware can be updated using two different methods:

- Using a PC tool via USB, which can only be done by authorized technicians or administrators in a secure environment.
- Using the over-the-air (OTA) remote update process, where the WisePad Q communicates with a Key Distribution Host via a mobile host device.

Update of the configuration is similar and can be done by the aforementioned two methods.

4.5.3 Signing Mechanisms

The firmware must be signed before being downloaded to the terminal.

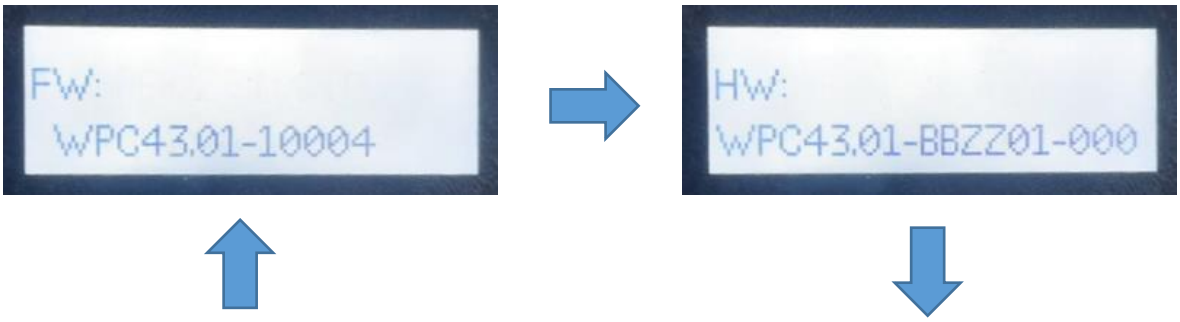
- The firmware is hashed with SHA256
- The hashed value will be signed with a RSA key, FSK, to generate firmware signature.
- A header will be added to the signature and encrypted with a TDES key, FAK.
- The cryptogram will be downloaded to terminal together with the firmware.

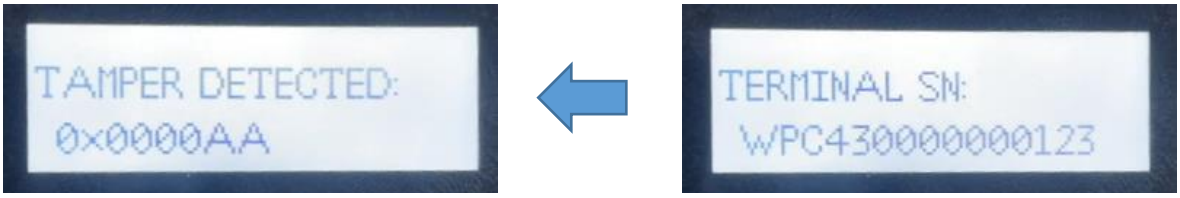
The terminal will reject the firmware if the signature is incorrect.

The signing process should be performed under dual control.

4.6 Hardware Security

WisePad Q has several tamper detection mechanisms. When a tamper detection mechanism is triggered, the internal working keys will be erased. A sequence of screen will be shown on the device.





Please contact the device provider if the device is tampered.

4.7 Software development

When developing an application interface to the device, the developer must respect the following guidance:

- Read the API document.
- Make sure parameter and length of the command is correct.
- No clear-text account data is outputted.

Developer should also refer to following guidance documents:

- “C Programming Coding Style” guideline.
- Security Guidance version 1.0.

5 Cryptography and Key Management

5.1 Cryptographic Algorithms

WisePad Q supports the following cryptographic algorithms:

- TDES
- AES
- RSA
- MAC X9.19

5.2 Key Management

WisePad Q supports the following key management schemes:

- **Master Key/Session Key – ANSI x9.24-1-2017 Section 8.3 Method**: Master/ Transaction Keys is implemented for Data Encryption. A master key and session key hierarchy is used where the Session Keys are encrypted/decrypted by the Master Keys.
- **DUKPT –ANSI x9.24-3**: DUKPT is implemented for Data Encryption. DUKPT is based on a unique key per transaction technique. Every transaction will derive a unique key for encryption and/or decryption.

Use of the POI with different key-management systems will invalidate any PCI approval of this POI.

5.3 Key Table

The following table lists a high-level overview of all the keys and certificates that are stored in the WisePad Q.

Key Name	Algorithm and Key Size	Key Usage
Terminal Public Key *	RSA (2048 bit)	OTA Remote Update – terminal auth
Sub CA Public Key **	RSA (2048 bit)	OTA Remote Update – terminal auth
KDH Public Key ***	RSA (2048 bit)	OTA Remote Update – KDH auth
DUKPT PIN key	TDES (112-bit)/AES (128-bit)	PIN encryption
MK/SK PIN key ******	TDES (112-bit/168-bit)/AES (128-bit)	PIN encryption
DUKPT Data key	TDES (112-bit)/AES (128-bit)	Data encryption
MK/SK Data key *******	TDES (168-bit)/AES (128-bit)	Data encryption
DUKPT MAC Key	TDES (112-bit)/AES (128-bit)	MAC calculation
MK/SK MAC key	TDES (168-bit)/AES (128-bit)	MAC calculation
EMV CA Key	RSA (1408/1536/1984-bit)	For EMV ODA process

*Terminal Public Key is self-generated.

** Sub CA public key is downloaded to terminal through Key Loading process in Service Centre

*** KDH Public key is downloaded to terminal through Key Loading process in Service Centre

**** The device only operates in a PTS compliant mode for MK/SK transaction when the algorithm is TDES and key size is 112-bit/168-bit or algorithm is AES and key size is 128 bit

***** For TDES the device only operates in a PTS compliant mode for MK/SK transaction when the key size is triple length (168-bit)

5.4 Key Decommissioning and Replacement

When the tamper-protection mechanism is triggered, the keys stored inside the WisePad Q are erased. If a key is suspected to be compromised or its life-time has ended, the key must be replaced with a new key. A key replacement can only be done by authorized personnel either on-site or remotely via a KDH. If a terminal is suspected to be compromised, the terminal cannot be used again and must be returned to the service provider immediately.

5.5 Key Loading

5.5.1 Manual Key Component Loading

The device does NOT support any manual plaintext key components loading, manual encrypted key loading, and public key loading.

5.5.2 Remote Key Distribution

Terminal and KDH will authenticate each other by using RSA-2048 based asymmetric cryptographic technique. A temporary Key Encryption Key will be exchanged during the authentication process. A key bundle will be sent from the KDH to the terminal under TDES/AES encryption by the aforementioned with Temporary KEK.

5.5.3 Service Centre Loading

The key loading device which complies with the PCI PTS requirement shall be placed in secure environment. A terminal can only be loaded in a secure environment under dual control. A Key Encryption Key is exchanged between the terminal and HSM with RSA-2048 encryption. A Key bundle will be sent from HSM to Terminal with TDES/AES encryption.

5.6 Configuration

The device does not support any modes or configuration that will output any sensitive information in plaintext. All sensitive information is encrypted Data key using either TDES in CBC mode or AES in CBC mode before sending it out of the terminal.

No configuration setting is needed to be done by the user in order to meet the security requirement defined in this document.

6 Administrative Responsibilities

The device does not implement role-based access to security sensitive services or operation.

The following section lists the role and operations allowed.

Operator: The regular operator of the terminal at the payment site.

Role	Operations	Note
Operator	Purchase/Sales	
	Refund/Void	
	Firmware Update	Cryptographic based Authentication is performed in server
	Configuration Update	Cryptographic based Authentication is performed in server
	Key Update	Cryptographic based Authentication is performed in server

7 Environmental Requirements

WisePad Q must be kept within specific environmental conditions during normal operation and storage.

Parameter	Min	Max
Temperature (Working)	0°C	45°C
Humidity (Working)	0%	95%
Temperature (Storage)	-20°C	55°C
Humidity (Storage)	0%	95%

The table below describes the environmental conditions that will trigger the environmental failure-protection.

Parameter	Min	Max
Voltage (Backup Battery)	2.1 ± 0.1V	4.1 ± 0.2V
Temperature	-35°C ± 10°C	100°C ± 10°C