WisePad 2 Security Policy
# Table of Content

1. **Introduction** ..............................................................................................................3
   1.1 Purpose and Scope .................................................................................................3
   1.2 Audience ..............................................................................................................3
   1.3 Reference .............................................................................................................3
   1.4 Glossary of Terms and Abbreviations ..................................................................4
2. **General Information** ..................................................................................................5
   2.1 Product Type .......................................................................................................5
      2.1.1 Mobile Host Mode .......................................................................................5
      2.1.2 Stand-alone Mode .......................................................................................5
   2.2 Product Functionality ...........................................................................................6
      2.2.1 Card Interface .............................................................................................6
      2.2.2 Communication Interface ..........................................................................6
      2.2.3 User Interface ..............................................................................................7
3. **Product Identification** ...............................................................................................7
   3.1 Product Appearance ............................................................................................7
   3.2 Product Label ......................................................................................................8
   3.3 Information Display ............................................................................................9
   3.4 PCI Listing, ..........................................................................................................9
4. **Guidance** ..................................................................................................................10
   4.1 Delivery and Deployment Inspection ..................................................................10
   4.2 Regular Inspection ..............................................................................................10
   4.3 Operation Environment .....................................................................................10
   4.4 Firmware and Configuration Maintenance .......................................................11
      4.4.1 Self-check .....................................................................................................11
      4.4.2 Firmware/Application Update ....................................................................11
   4.5 Hardware Security ..............................................................................................11
5. **Cryptography and Key Management** .....................................................................12
   5.1 Cryptographic Algorithms ..................................................................................12
   5.2 Key Management ...............................................................................................12
   5.3 Key Table ...........................................................................................................12
   5.4 Key Decommissioning and Replacement .......................................................12
   5.5 Key Loading .......................................................................................................13
6. **Administrative Responsibilities** ................................................................................13
7. **Environmental Requirements** ................................................................................14
1 Introduction

1.1 Purpose and Scope

This security policy applies to WisePad 2 terminal, which is PCI PTS version 4.1 POI approved. It addresses the proper use of WisePad 2 in a secure fashion. Improper use of WisePad 2 will lead to incompliance to the PCI PTS POI Security Requirements version 4.1.

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

[7] BBPOS C Programming Coding Style version 0.3
### 1.4 Glossary of Terms and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard, a data encryption/decryption standard to supersede DES and TDES</td>
</tr>
<tr>
<td>ATM</td>
<td>Automatic Teller Machine, a unattended terminal for banking operations</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard, a data encryption/decryption standard</td>
</tr>
<tr>
<td>DUKPT</td>
<td>Derived Unique Key Per Transaction, a symmetric key management standard</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay MasterCard Visa, an entity governing ICC payment</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Chip Card, aka Smartcard</td>
</tr>
<tr>
<td>KDH</td>
<td>Key Distribution Host</td>
</tr>
<tr>
<td>LED</td>
<td>Light emitting diode</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication, a short-range wireless communication standard</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code, a cryptographic digital digest of a message</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-the-Air, used to denote remote operation such as remote firmware update</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry, an entity governing the security level of payment devices</td>
</tr>
<tr>
<td>PED</td>
<td>PIN Entry device</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number, a 4-12 digit numeric password associated with payment card</td>
</tr>
<tr>
<td>POI</td>
<td>Point of Interaction</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sales, referring to the terminal used to process the payment</td>
</tr>
<tr>
<td>PTS</td>
<td>PIN Transaction Security</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adelman Algorithm, an asymmetric encryption/decryption standard</td>
</tr>
<tr>
<td>TDES</td>
<td>Triple DES, a symmetric key encryption/decryption standard based on DES</td>
</tr>
<tr>
<td>TMS</td>
<td>Terminal Management System</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
</tbody>
</table>
2 General Information

2.1 Product Type

WisePad 2 is a mobile Point of Sales (mPOS) payment device for payment processing in an attended environment. There are two modes of operations.

2.1.1 Mobile Host Mode

When used in conjunction with a mobile phone or tablet, the mobile host device and WisePad 2 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 2.

2.1.2 Stand-alone Mode

When used in stand-alone mode, the WisePad 2 acts as the payment processing terminal. The operation flow is controlled solely by the WisePad 2.
2.2 Product Functionality

2.2.1 Card Interface

WisePad 2 is equipped with the following payment card interfaces:

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

WisePad 2 also has a built-in Secure Key Pad for entry of PIN associated with the payment card. The PIN Pad can be used for entering other data such as transaction amount.

2.2.2 Communication Interface

In the mobile-host mode operations, WisePad 2 can communicate with the mobile host device through one of the following interfaces:

- Bluetooth
  - Version 2.1
  - Profile L2CAP
  - Secure mode: Mode 4 with SSP passkey
  - Authentication method: passkey only
  - Application profiles: SSP
- Audio Jack
- USB

Specific on the Security Guidance on Bluetooth as mentioned above, there are 3 potential attacks identified which are Blueprinting, BluleStumbling and BlueSmack. The use of the device may introduce an avenue of attack for an adversary to capture keystrokes and spoof a user to gain access to the device.

To mitigate the risk, the capabilities of both authentication and encryption are used on Bluetooth communication ports.

- For end user it needs to enable the connection only when needed and make devices discoverable only when necessary.
- Pairing with PIN exchange is required for each new connection even if it has previously been authenticated.

In addition, the default configuration of the Bluetooth can be defined and modified by btstack-config
2.2.3 User Interface

The user-interface consists of the following:

- A dot-matrix display
- 4 LEDs
- Buzzer
- Key Pad

WisePad 2 has an internal battery and can be recharged via the USB interface.

3 Product Identification

Operators and owners of WisePad 2 should get familiar to its appearance so that any alterations and tampering attempts can be detected and reacted to in a timely manner.

3.1 Product Appearance

![Front View](image1)

![Back View](image2)
3.2 Product Label

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

- Product Name and Model
- Serial Number
- Hardware Version
- IMEI
- Compliance Logos, e.g. CE Mark
- Voltage and Current Rating

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

3.2.1 Current Version

Hardware Version: WPC22001-01-001
Software Version: WPC2 0.003-12 (Refer from LCD display)
3.3 Information Display

Additional information about the WisePad 2 can be displayed by pressing the Menu button and then selecting the Device function.

Menu button -> Device

The following information will be displayed:

- Bootloader Version
- Firmware Version (refer to Software Version no. System Table)
- Application Version
- Serial Number
- Battery Level

3.4 PCI Listing

To verify that WisePad 2 is a PCI approved device, browse at 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 WisePad 2, the merchant or acquirer must visually inspect the device for signs of tampering. In particular, the following must be checked.

- The label on 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 is no signs of tampers such as torn labels, cracks, holes, loosen 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, hole or loosen.
- No warning message is displayed.
- The keypad area has no signs of being modified.

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 delivered/deployed device is complete and not altered.
- The device is intact and there is no signs of tampers such as torn labels, cracks, holes, loosen or missing screws.
- No unidentified attachments are added to the device. Protective jackets, mounting fixture, security locks an chains with known purposes are acceptable.
- The IC card insertion area of the device has no signs of tampers such as cracks, hole or loosen.
- No warning message is displayed, as defined in section 4.5.
- The keypad area has no signs of being modified.

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 2 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 Firmware and Configuration Maintenance

4.4.1 Self-check

When the WisePad 2 is turned on, a self-test is run to check the integrity of the firmware, application, configuration and keys. The firmware will also perform self-test automatically for every 24 hours.

4.4.2 Firmware/Application Update

The firmware and application can be updated in two manners:

- Using a PC tools 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 2 communicates with a Key Distribution Host via a mobile host device.

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

4.5 Hardware Security

WisePad2 has several tamper detection mechanism. When a tamper detection mechanism is triggered, the internal working keys will be erased and a warning will be displayed.

4.6 Software development

Software development on WisePad 2 should follow the guidance in the BBPOS C Programming Coding document.
5 Cryptography and Key Management

5.1 Cryptographic Algorithms

WisePad 2 supports the following cryptographic algorithms:

- TDES
- RSA
- MAC X9.19
- SHA-256

5.2 Key Management

WisePad 2 supports the following key management schemes:

- Fixed Key
- Master Key/Session Key
- DUKPT

5.3 Key Table

The following table lists all keys and Certificates that may be stored in a WisePad2:

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Size</th>
<th>Algorithm</th>
<th>Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Public Key</td>
<td>2048-bit</td>
<td>RSA</td>
<td>OTA Remote Update – terminal auth</td>
</tr>
<tr>
<td>Sub CA Public Key</td>
<td>2048-bit</td>
<td>RSA</td>
<td>OTA Remote Update – terminal auth</td>
</tr>
<tr>
<td>KDH Public Key</td>
<td>2048-bit</td>
<td>RSA</td>
<td>OTA Remote Update – KDH auth</td>
</tr>
<tr>
<td>DUKPT PIN key</td>
<td>112-bit</td>
<td>TDES</td>
<td>PIN encryption</td>
</tr>
<tr>
<td>DUKPT PIN key</td>
<td>112/168-bit</td>
<td>TDES</td>
<td>PIN encryption</td>
</tr>
<tr>
<td>DUKPT Data key</td>
<td>112-bit</td>
<td>TDES</td>
<td>Data encryption</td>
</tr>
<tr>
<td>Fixed/MK/SK Data key</td>
<td>112/168-bit</td>
<td>TDES</td>
<td>Data encryption</td>
</tr>
<tr>
<td>DUKPT Track key</td>
<td>112-bit</td>
<td>TDES</td>
<td>Mag Track encryption</td>
</tr>
<tr>
<td>Fixed/MK/SK Track key</td>
<td>112/168-bit</td>
<td>TDES</td>
<td>Mag Track encryption</td>
</tr>
<tr>
<td>DUKPT MAC Key</td>
<td>112-bit</td>
<td>TDES</td>
<td>MAC calculation</td>
</tr>
<tr>
<td>Fixed/MK/SK MAC key</td>
<td>112/168-bit</td>
<td>TDES</td>
<td>MAC calculation</td>
</tr>
</tbody>
</table>

5.4 Key Decommissioning and Replacement

When the tamper-protection mechanism is triggered, the keys stored inside the WisePad 2 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 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

The remote key distribution follows asymmetric method.

5.5.3 Service Centre Loading

The reloading of device in service centre follows all requirements for a KIF (key injection facility).

5.6 Configuration

The device does not support any modes or configuration that will output any sensitive information in plaintext.

6 Administrative Responsibilities

The following lists the roles and operations allowed to each role.

Operator – The regular operator of the terminal at the payment site with minimum authorization level.

Supervisor – The supervisor of the terminal at the payment site has higher authorization level than the operator. Some sensitive operations need his/her approval and authentication.

Administrator/Technician – This is authorized personnel from the merchant, the payment service provider or the device vendor who has the authorization to perform firmware/configuration and key updates at the payment site or remotely using the OTA feature.

<table>
<thead>
<tr>
<th>Role</th>
<th>Operations</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Purchase/Sales</td>
<td></td>
</tr>
<tr>
<td>Operator/Supervisor</td>
<td>Refund/Void</td>
<td>Depends on Terminal Management Requirement</td>
</tr>
<tr>
<td>Administrator/Technician</td>
<td>Firmware/Application Update</td>
<td></td>
</tr>
<tr>
<td>Administrator/Technician</td>
<td>Configuration Update</td>
<td></td>
</tr>
<tr>
<td>Administrator/Technician</td>
<td>Key Update</td>
<td></td>
</tr>
</tbody>
</table>
7 Environmental Requirements

WisePad 2 must be kept within specific environmental conditions during normal operation and storage.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature (Working)</td>
<td>0 °C</td>
<td>45 °C</td>
</tr>
<tr>
<td>Humidity (Working)</td>
<td>0%</td>
<td>95%</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
<td>-20 °C</td>
<td>55 °C</td>
</tr>
<tr>
<td>Humidity (Storage)</td>
<td>0%</td>
<td>95%</td>
</tr>
</tbody>
</table>