Version 1.03

December - 2023

Headquarters
Av. Jabaquara, 3060, 6º andar
São Paulo - SP, ZIP CODE: 04046-500

Service Unit
Rua Guaicurus, 145
Diadema - SP, ZIP CODE:09911-630

Manufacture Unit
Avenida Milton Santos, 102
Ilhéus – BA, ZIP CODE: 45652-565

Manufacture Unit
Avenida Buriti, 1.900, Lote 3.38/1- EPCV
Manaus – AM, ZIP CODE: 69075-000

Revision History

Version	Date	Editor	Description
1.00	30-Oct-23	Vinicius Moreira	Created.
1.01	20-Nov-23	Vinicius Moreira	Delete warning statement.
1.02	22-Nov-23	Vinicius Moreira	Update section 2.4.
1.03	05-Dec-23	Vinicius Moreira	Update section 4.2.

Table of Contents

1 Introduction

This document objective is to describe the Security Policy for the MP35,MP35P from **GERTEC BRASIL LTDA**. The document was made to attend the PCI requirements and include information about product overview, guidance and administration.

Using any unapproved method that is not addressed in this document and its references will violate the PCI PTS version 6.2 approval of the device.

1.1 Acronyms

AES	Advanced Encryption Standard
AP	Application processor
DES	Data Encryption Standard
DUKPT	Derived Unique Key per Transaction
GEDI	Gertec Encrypted Device Interface
GPRS	General Packet Radio Service
ICC	Integrated Circuit Card
LCD	Liquid-Crystal Display
MIPS	Microprocessor without Interlocked Pipeline Stages
MK	Master Key
MSR	Magnetic Stripe Reader
NDA	Non-Disclosure Agreement
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTS	PIN Transaction Security
RH	Relative Humidity
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
SK	Session Key
SRED	Secure Reading and Exchange of Data
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VDC	Voltage Direct Current

1.2 References

[1] PCI PTS POI Modular Derived Test Requirements v6.2 – January 2023

[2] PCI PTS POI Security Requirements - Technical FAQs for use with Version 6, November 2023

[3] ISO 9564-1:2011, Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card-based systems

[4] ISO 9564-1:2011/Amd.1:2015, Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card-based systems - AMENDMENT 1

[5] ISO 9564-2:2014, Financial services - Personal Identification Number (PIN) management and security - Part 2: Approved algorithms for PIN encipherment

[6] ISO/IEC 18033-3:2010, Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers

[7] ANS X9.24-1:2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[8] ANS X9.24-2:2021, Retail Financial Services Symmetric Key Management Part2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[9] ANSI X9.24-3: 2017, Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction

[10] ANSI X9.143-2022, Retail Financial Services Interoperable Secure Key Block Specification

[11] NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General, NIST-Sp-800-57-1

[12] MP35,MP35P User Manual, Version 1.00, July 2023, Gertec Brasil Ltda

[13] MP35,MP35P Application Development Guide, Version 1.01, July 2023, Gertec Brasil Ltda

[14] MP35,MP35P Open Protocol Security Guide, Version 1.02, July 2023, Gertec Brasil Ltda

[15] MP35,MP35P Security Management Guide, Version 1.00, July 2023, Gertec Brasil Ltda

Note: All proprietary non-standardized documents listed above will only be provided to authorized software developers after a firmed NDA.

2 Product Overview

The MP35,MP35P is a handheld Point of Sale (POS) PED terminal that provides a complete solution with the most common card interfaces like contactless, magnetic and contact smartcard. It is a great solution for a wide range of applications since it has USB, Bluetooth, Wi-Fi and cellular (2G/3G) connections to match indoor and outdoor uses.

2.1 Type

The MP35,MP35P should be used in an attended environment as a stand-alone POS terminal.

An attended environment is one where a transaction is completed under all the following conditions:

- Card or Proximity Payment Device is present;
- Cardholder is present;
- Cardholder completes the Transaction and, if required, an individual representing the Merchant or Acquirer assists the Cardholder to complete the Transaction.

It is forbidden to use it in an unattended environment. Use of the device in an unattended environment will violate the PCI PTS approval of the device.

2.2 Features

The device contains the following physical and logical interfaces:

- Physical keypad
- LCD color display with touch panel (not used for PIN input)
- USB Type-C interface
- Magnetic stripe reader
- ICC interface
- Contactless reader
- SIM card slot
- PSAM card slot
- Bluetooth module
- Wi-Fi module
- Cellular (2G/3G) module
- Camera
- LED
- Speaker

- Printer (MP35P only)

The document [14] provides more information on the approved communication methods and protocols. The use of any method not listed in the policy invalidates the device approval.

2.3 Identification

The MP35,MP35P are compact devices, as shown in Figure 1 and 2.

Figure 1 – MP35 Overview

Figure 2 – MP35P Overview

2.4 Version

Each device has a unique serial number that is used to keep track of the devices during their lifetime, from production to decommission. The unique serial number can also be obtained by system commands to double check the authenticity of the label.

There is an identification label located on the back cover of the device, which presents the product name, product code, serial number, etc., as shown in Figure 3 and Figure 1. This label must not be torn off or altered.

Figure 3 – MP35 Identification Label

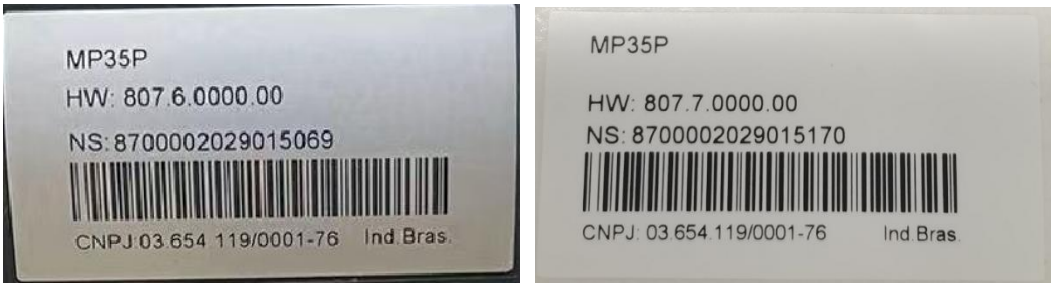

Figure 4 – MP35P Identification Label

All product information, especially the serial number, should be checked after receiving the product to guarantee that the item received is authentic.

The MP35,MP35P and has two (2) versions:

The **Hardware version** depends on card interfaces available:

**The "x" is non-security related.*

- 806.5.0xxx.xx and 806.6.0xxx.xx
- 807.6.0xxx.xx and 807.7.0xxx.xx
- 806.5.1xxx.xx and 806.6.1xxx.xx
- 807.6.1xxx.xx and 807.7.1xxx.xx

HW Wildcards meaning

<table>
<tr><td rowspan="9">Hardware Version</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr>
<tr><td>8</td><td>0</td><td>6</td><td>.</td><td>5</td><td>.</td><td>0</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>6</td><td>.</td><td>6</td><td>.</td><td>0</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>7</td><td>.</td><td>6</td><td>.</td><td>0</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>7</td><td>.</td><td>7</td><td>.</td><td>0</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>6</td><td>.</td><td>5</td><td>.</td><td>1</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>6</td><td>.</td><td>6</td><td>.</td><td>1</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>7</td><td>.</td><td>6</td><td>.</td><td>1</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>8</td><td>0</td><td>7</td><td>.</td><td>7</td><td>.</td><td>1</td><td>x</td><td>x</td><td>x</td><td>.</td><td>x</td><td>x</td></tr>
<tr><td>3</td><td colspan="13">Available Name:<table><tr><td>Value</td><td>Model</td></tr><tr><td>6</td><td>MP35</td></tr><tr><td>7</td><td>MP35P</td></tr></table></td></tr>
<tr><td>5</td><td colspan="13">Available AP module:
For MP35<table><tr><td>Value</td><td>Processor</td></tr><tr><td>5</td><td>AP1</td></tr><tr><td>6</td><td>AP2</td></tr></table>For MP35P<table><tr><td>Value</td><td>Processor</td></tr><tr><td>6</td><td>AP1</td></tr><tr><td>7</td><td>AP2</td></tr></table></td></tr>
<tr><td>7</td><td colspan="13">Available Reader:<table><tr><td>Value</td><td>Reader</td></tr><tr><td>0</td><td>With CTLS</td></tr><tr><td>1</td><td>Without CTLS</td></tr></table></td></tr>
<tr><td>8-10</td><td colspan="13">Represent the Customer Number, no security impact.</td></tr>
<tr><td>12-13</td><td colspan="13">Represent the device’s Color, no security impact.</td></tr>
</table>

Where:

- ICCR = Integrated Circuit Card Reader interface
- MSR = Magnet Stripe Reader
- CTLS = Contactless Card Reader interface

This hardware version can be visually checked at the product identification label (Figure 3 and Figure 34).

Firmware version:

This firmware version can be obtained by entering the PCI Menu and selecting “About” to find the “FW:” character, which shows the firmware version (Figure 3).

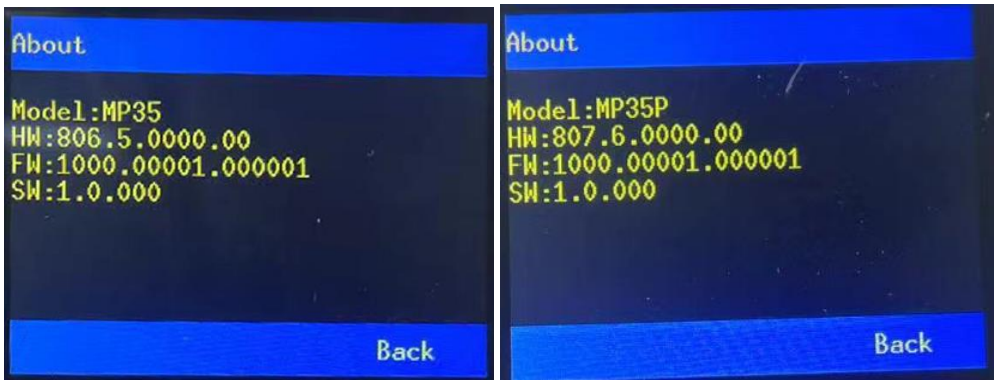

Figure 5 – MP35,MP35P firmware Identification Info

The encoding formats for this version:

- 10xx.xxxxx.xxxxxx

MP35,MP35P FW	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	1	0	x	x	.	x	x	x	x	x	.	x	x	x	x	x	x
3-4	Third party open source lib patch version, no security impact																
6-10	Main SDK API build times, no security impact																
12-17	System build times, no security impact																

3 Guidance

3.1 Product

3.1.1 Installation

The device was designed to be portable and to work as a standalone device. No installation is required.

Prior to using the terminal, it is recommended to check the user manual that is available for download in the product area of GERTEC's website.

3.1.2 Inspection

After receiving the product via shipping, the items listed below should be inspected:

- The product identification, that includes the product version and the serial number on the label;
- The serial number on the label is the same as the one recorded in the product system, and should be displayed on the LCD according to the software manual;
- The warranty label, confirming it is present and not damaged;
- The ICC acceptor, for shim or any obstruction or suspicious objects, refer to Figure 7 – MP35P MSR and ICC card slot for comparison;

- The MSR slot, checking for any obstruction or additional readers, refer to Figure 7 – MP35P MSR and ICC card slot for comparison;
- The keypad is firmly in place, without any fissures, shims or other anomalies;
- The appearance of the entire device for any tamper evidence, including cuts, holes, cracks, wires, additional stickers, glue marks and any other suspicious elements;
- The screen, for any tamper or warning information, please refer to section 3.2.1 - Tamper Response;
- The physical keypad, checking for any incorrect or redundant keyboard overlays;
- The application behavior and all logical information, such as versions, date and others control numbers available to confirm that no unauthorized changes were made.

For security reasons, daily inspections shall be conducted on the the items listed above. If any item that is not completely normal, please stop using the device immediately and contact the customer service.

These procedures aim to keep the security of the devices.

Figure 6 – MP35 MSR and ICC card slot

Figure 7 – MP35P MSR and ICC card slot

3.1.3 PIN Confidentiality

The MP35,MP35P are hand-held devices without a privacy shield. The terminal should be given to the cardholder during the PIN entry. The customer should be advised to take care and protect the device keypad so that it is off the field of vision of any people or cameras while entering the PIN code.

Figure 8 - Safe PIN entry example

The following table shows the combination of methods that should be used when installing the device to protect the cardholder's PIN during PIN entry.

Method	Observation Corridors				
	Cashier	**Customer in Queue**	**Customer Elsewhere**	**On-Site Cameras**	**Remote Cameras**
With stand	No Action Needed.	No Action Needed.	No Action Needed.	Out of sight of the cameras.	Out of sight of the cameras.
Without stand	Block the view of cashier by body.	Block the view of other customers by body.	Block the view of other customers by body.	Out of sight of the cameras.	Out of sight of the cameras.
Customer Instruction	Remind the customer to shield PIN.	Keep a distance.	Keep a distance.	Out of sight of the cameras.	Out of sight of the cameras.

Table 1 - Pin Confidentiality table

3.1.4 Decommissioning

Before decommissioning or refurbishing the device, all sensitive data must be erased. This can be done by putting the device into tampered status. The recommended way of doing so is by disassembling the device, which will cause the device to enter the tamper state and lock; this also erases all the sensitive data immediately.

For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely by the main board hardware tamper mechanism.

3.2 Hardware

3.2.1 Tamper Response

The device has a protection mechanism for physical tamper attack. At the tamper event, the device will display the tamper message and beep warning sound. Even if the device is rebooted, it will remain blocked for any operation and will display the serial number to indicate the tampered state.

If the device is in tampered state, it should immediately be removed from service and be sent to an authorized maintenance facility, where the device will pass for the necessary inspection.

Figure 9 - Tamper screen

3.2.2 Operational Conditions

The environmental conditions to operate the device are specified below:

- Working Temperature:-10℃~55℃
- Storage Temperature: -20℃~70℃
- R.H.: 5%~95% (Non-condensing)
- Power supply: DC 5V/2A

When the following conditions occur, the tamper detector will clear sensitive data information immediately:

- The battery voltage VBAT rises above 4.2V±0.1V
- The battery voltage VBAT falls below 2.1V±0.1V
- The on-chip temperature rises above approximately 90°C~120°C
- The on-chip temperature falls below approximately -50°C~-30°C

The security of the device may be affected by altering the environmental conditions (e.g., place the device outside the stated operating range temperature or operating voltages).

3.3 Software

3.3.1 Development Guidance

All software development should follow the guidance listed in the references of this document. Mainly the [13] is for general development, including SRED requirements for protection of account data, which is mandatory in case of attachment to a mobile device.

The [14] shall be followed if application uses Bluetooth, Wi-Fi or Cellular (2G/3G) interfaces for the Open Protocols.

The device does not allow unauthorized or unnecessary functions.

3.3.2 Communication Methods and Protocols

The following describes the communication methods and protocols available in the device.

	Interface	Protocols
Communication	Cellular	TLSv1.2
	Wi-Fi	TLSv1.2
	Bluetooth	Bluetooth 4.0 (Bluetooth BR/EDR Mode 4 Level 3)
	USB	USB 2.0, Serial over USB

Table 2 - Communication Methods and Protocols

Use of any method not listed in the policy invalidates the device approval.

3.3.3 Signing Mechanisms

The firmware and application signing mechanisms of the device use the RSA2048 and SHA256 algorithms.

All the signing process used the SCD under dual control in the secure room.

More details about the signing process are described in [15].

3.3.4 Update Procedures

The device will obtain the latest updates and patches from TMS every time it is powered on. All updates and patches must be cryptographically authenticated by the device. If the authenticity of the update or patch cannot be confirmed, it will be rejected by the device.

In case of updates, the communication should be established according to [14] documentation. The [13] provides more information regarding update procedures.

It is recommended to use the latest stable version of application and firmware.

3.3.5 Self-Test

The device will perform a self-test upon start-up and every 23.5 hours. Periodical self-test is done by automatically reboot. This reboot period starts it's count once the device is powered on.

Self-Test include:

- Firmware and application integrity and authenticity

- Hardware security status
- Check keys KCV

And if there is any kind of failure detected by self-test mechanism, it will cause the device to not function properly. In this situation, the device will be disabled and cannot be used. It should be sent to an authorized service centre for repair.

3.3.6 Account Data Protection

The device always provides SRED functionality and doesn't support the disablement (turning off) of SRED functionality.

For the SRED module, account data can be encrypted by TDES and AES encryption under MK/SK.

The device does not support the pass-through of clear-text account data.

4 Administration

4.1 Configuration Settings

After released to the market, the device does not have any security sensitive configuration set-up necessary to meet security requirements.

4.2 Default Value Update

The device is functional when received by the merchant or acquirer and there is no security sensitive default value. The dual control password must be set for the first time enter the sensitive services, the password setting operation for the first time can refer to [12].

The device does not include any certificate for testing purpose after manufacture.

4.3 Key Management

The device implements the following key management techniques:

- DUKPT, based on key derivation to allow a unique key for each transaction.
- Master Key / Session Key, based on hierarchy of keys. The session keys used can be unique per cryptographic operation.

All key management techniques are specified on [7] and [8].

Use of the POI with different key management system will invalidate any PCI approval of this device.

4.3.1 Cryptographic Algorithms

The device includes the following algorithms for key management:

- RSA (2048 bits).
- SHA-256.
- Triple DES (128 bits and 192 bits).
- AES (128 bits, 192 bits and 256 bits).
- ECC (P-224, P-256, P-384, P-521).

Other cryptographic algorithms are also available or may be used for non-key related operations.

4.3.2 Key Types

Key Name	Purpose/Usage	Algorithm	Size(bits)	Storage
MMK	Key storage protection key	AES	256	BPK
KBPK	Key Block Protection Key of X9.143, it is used to encrypt the keys transported from KLD to Device.	AES	256	SRAM
TMK (MK/SK)	Encrypt or decrypt SK (PEK, MAK, TDK)	TDES, AES	TDES: 128/192 AES: 128/192/256	Flash
PEK (MK/SK)	Encrypt PIN blocks	TDES, AES	TDES: 128/192 AES:128/192/256	Flash
TDK (MK/SK)	Encrypt account data	TDES, AES	TDES: 192 AES: 128/192/256	Flash
MAK (MK/SK)	Generate or verify MAC of data blocks	TDES, AES	TDES: 128/192 AES: 128/192/256	Flash
IPEK	Initial DUKPT Key	TDES, AES	TDES: 128 AES: 128/192/256	RAM
DUKPT PEK (Future Keys Register)	Encrypt PIN blocks	TDES, AES	TDES: 128 AES: 128/192/256	Flash

Table 3 - Key Table

4.3.3 Key Loading Policy

The device supports the following key-loading techniques:

- Key components entry through the Keypad
- Clear-text key injection from KLD;
- Symmetric encrypted keys;
- Asymmetric key loading method

4.3.4 Key Replacement

Any keys should be replaced with a new key value whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses, as defined in [11].

4.4 Roles and Services

The customers of maintainer are acquirer or administrator. We also refer to administrator as acquirer directly. Maintainer sells devices to administrator and provides technique and maintenance supports to administrator. Administrator sells the devices to end users and provides services to their end user. Maintainer, administrator, and operator play different roles in operating the device. The below table shows different roles and operations:

Roles	Operations
administrator	1. Organize the third party to develop application program; 2. Download firmware and application
operator	Perform transaction
maintainer	1. Sign customer public key 2. Repair device and unlock the device if tampered. 3. Download customer public key

Table 4 - Different roles and operations