RB One GmbH

Manufacturer: RB One GmbH

Address: Plosslgasse 17-23

KT-1 Security Policy

Version 1.8

Dec - 2019

Table of Contents

1 Introduction

This document objective is to describe the Security Policy for the KT-1 from RB One GmbH. 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 approval of the device.

1.1 Acronyms

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DUKPT	Derived Unique Key per Transaction
GEDI	RB One GmbH 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

- PCI PTS POI Modular Security Requirements Version 5.1 - March 2018
- ISO 9564-1:2011, Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in cardbased systems
- 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 cardbased systems - AMENDMENT 1
- ISO 9564-2:2014, Financial services - Personal Identification Number (PIN) management and security - Part 2: Approved algorithms for PIN encipherment

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

- ANS X9.24-1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

- ANS X9.24-2:2006, Retail Financial Services Symmetric Key Management Part2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

- X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

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

- Secure Software Development Guide - Version 1.0. (2019, February). RB One GmbH.

- OP Secure Software Development Guide - Version 1.0. (2019, February). RB One GmbH.

- Signing Management – Version 1.0. (2019, February). RB One GmbH.

- Software Update Procedure – Version 1.0. (2019, February). RB One GmbH.

- Device Initialization Procedure – Version 1.0. (2019, February). RB One GmbH.

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

2 Product Overview

KT-1 is a stand-alone POS terminal that provides a complete solution with the most common card interfaces like contactless and contact smartcard.

It features a complete POS solution assisting other merchant needs by the use of peripherals such as Wi-Fi and a digital camera. KT-1 has a dedicated secure processor for sensitive data handling and a highspeed main processor running an operational system that makes it easy to program and gives the developer a more flexible system to create applications.

2.1 Type

KT-1 should be used in an attended or semi-attended environment as a desktop stand-alone POS terminal or integrated with a more complex solution. A semi-attended environment is one where a transaction is completed under all of 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. The use of 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:

- Capacitive keypad
- LCD touchscreen color display

- USB interface
- ICC reader
- Contactless reader
- Bluetooth module
- Wi-Fi module
- Cellular module
- Digital camera

2.3 Identification

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

The full view of the device is presented in Figure 1.

Figure 1- KT-1 full view

There is an identification label located on the back cover of the device, which contains the product name, product code, serial number, etc., as shown Figure 2. This label must not be torn off, covered or altered.

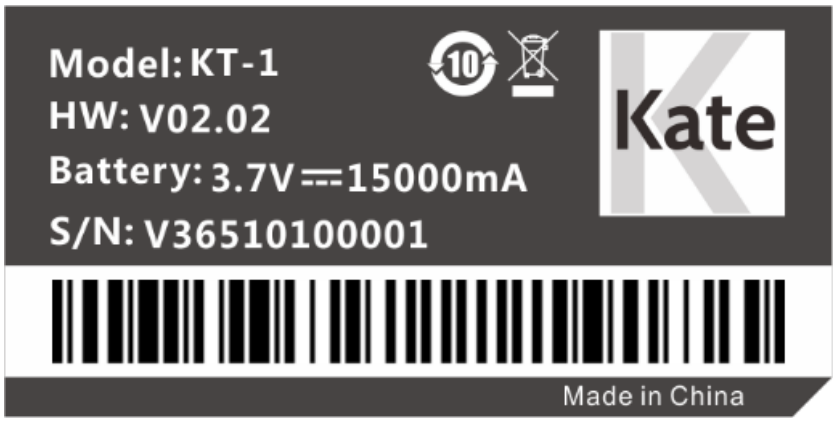

Figure 2 - Product identification label

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

2.4 Version

KT-1 has following versions:

Hardware version: V02.02

This version can be visually checked on the back of the device on the product identification label (see Figure 2).

- Firmware version: 1.0.1.xxxx

This version can be checked through the below steps,

1. After device power on, click “Main Menu” button.
2. Click “version” button to check version information

3 Guidance

3.1 Product

3.1.1 Installation

The KT-1 is designed to be portable and to work as a standalone device. No installation is required.

Prior to starting to use the terminal, it is recommended to check the user manual is available for download in the product area of RB One GmbH website.

3.1.2 Inspection

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

- The product identification, that includes the product version and the serial number on the back label;
- The serial number on the back label is the same as the one recorded in the product system, that should be displayed on the screen according to the software manual;
- The warranty label, whether it is present and not damaged;
- The ICC acceptor, for shim or any obstruction or suspicious objects;
- The appearance of the entire device for any tamper evidences, including cuts, holes, cracks, wires, additional stickers, glue marks and any other suspicious elements;
- The screen, for any tamper or warning information;

The application behavior and all logical information, such as versions, date and other control numbers available to confirm that no unauthorized changes were made.

For security reasons, it is strongly recommended the weekly inspection of the items listed in this document.

If any item is not completely normal, the device should be sent immediately to maintenance. The KT-1, as any of secure equipment from RB ONE GMBH, passes for security procedures when sent back for maintenance.

These procedures aim to keep the security of the devices.

3.1.3 PIN Confidentiality

KT-1 should be given to the cardholder during the PIN entry. The KT-1 has been approved for use with a privacy shield. The KT-1 uses two polarizers mounted under the screen to provide screen protection. The picture of the approved privacy shield as below,

Figure 3 - privacy shield

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 immediate erasure of sensitive data and lock any operation.

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 a ‘Trigger!!!’ message as seen Figure 4, rings the buzzer and blocks any operation. Even if the device is rebooted, it will remain blocked for any operation, display a ‘Trigger!!!’ message and rings the buzzer to indicate the tampered state.

If the device is in the tampered state, the user must contact the device maintenance or authorized center immediately, remove it from service and keep it away from potential illegal investigation.

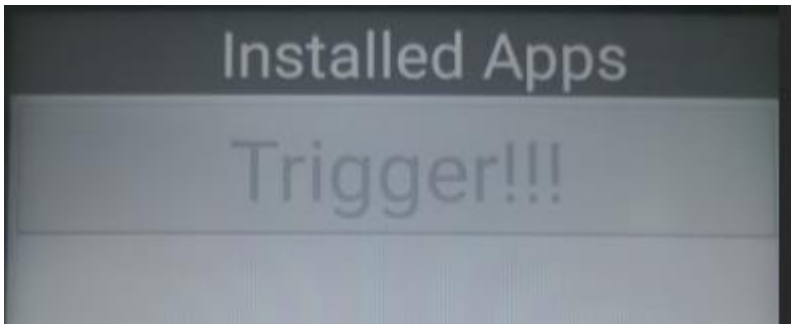

Figure 4 - Tamper Response

3.2.2 Operational Conditions

The following are the temperature and humidity specifications of the device:

- Operating temperature: 0° to 50° C (32° to 122° F)
- Storage temperature: -20°C to 70°C (-4° to 158° F) Relative humidity: 5% to 95% (RH non-condensing)

Subjecting the device to extreme environmental conditions may result in tamper events. Any temperatures above 120ºC (± 5º) or below -30ºC (±5º) may result in a tamper condition. Additionally, if the backup battery voltage drifts outside of the range of 2.1 VDC to 3.6 VDC, the unit may tamper as well.

3.3 Software

3.3.1 Development Guidance

All software development should follow the guidance listed in the references of this document. Mainly the "Secure Software Development Guide" for general development. The “OP Secure Software Development Guide” should be followed if an application uses WiFi or GPRS with open protocols.

3.3.2 Signing Mechanisms

All firmware, applications and signing keys must be signed with the following cryptographic algorithms:

- RSA 2048, used for signature checking
- SHA2-256, used for calculating hash for data integrity

More details about the signing process are described in “Sign Tools Using Guide”.

3.3.3 Update Procedures

All software, firmware and configuration parameters can be updatable. All updates and patches must be cryptographically authenticated by the device, whether performed locally or remotely. If the authenticity of the update or patch cannot be confirmed, it will be rejected by the device. In case of remote updates, the communication should be established according to “OP Secure Software Development Guide” rules. The “Software Update Procedure” provides more information regarding update procedures.

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

3.3.4 Self-Test

A complete self-test that checks all integrity of the device is performed upon start and once each day of continuous use under normal operation. Additional tests may be performed by the applications at any time.

The self-test is performed automatically, so no initialization by an operator is required.

Once any failure is detected in this process, a warning message will be displayed until the problem is solved and any operation will be blocked.

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

After released to the market, the administrator's password should be changed before use.

The steps are below,

1. After device power on, click "Main Menu" button.

2. Click "Change Admin Pwd" button. At this time, the old passwords will be required to enter for authentication the administrator's identity. If the authentication is successful, enter the new password to finish the password changes.

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.
- Fixed key, based on a unique key for each terminal.

All key management techniques are specified on ANSI X9.24 parts 1 and 2.

4.3.1 Cryptographic Algorithms

The device includes the following algorithms for key management:

- TDES (112 and 168 bits)
- AES (128 to 256 bits)

- RSA (2048 to 4096 bits)
- SHA2 (256 to 512 bits)

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

4.3.2 Key Loading Policy

The device does not support manual cryptographic key entry. Key loading must meet key management requirements described in "Device Initialization Procedure".

4.3.3 Key Usages

The usual key usages available in device are PIN encryption, data encryption or decryption and key transport. These keys can be used with TDES or AES algorithms using any of the key management techniques available.

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 “NIST SP 800-57-1”.

4.4 Roles and Services

The device has no functionality that gives access to security sensitive services, based on roles. Such services are only available in authorized facilities managed through dedicated tools, using cryptographic authentication.