ROAM™
POWERING MCOMMERCE
An ingenico company

RP450&RP456&RP457 PCI Security Policy

September 2015

280 Summer Street, Lobby Level, Boston, MA 02210 | Phone: +1.888.589.5885 | Fax: +1.617.904.0151
www.roamdata.com

Table of Contents

Document Information

Document History

Revision	Type of Modification	Date
1.0	Document creation	09-28-2015
1.1	Add self-test failure evidence, software development guidance, communication methods and protocols, Attack display, File update mechanism, Signature description, Methods of update software, OEM module security policy, State key replacement base on NIST SP 800-57-1. Environment requirements.	12-28-2015
1.2	Add RKI and BT4.2	3-31-2016

Acronyms

The following acronyms will be referenced in this document.

- **DUKPT** – Derived Unique Key Per Transaction
- **N/A** – Not Applicable
- **TDES** – Triple Data Encryption Standard

References

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

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

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

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

[5] ISO 9564-2, Banking — Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment

[6] PCI PTS POI Derived Test Requirements V4.0 - June 2013

Introduction

This document addresses the proper use of the POI in a secure manner including information about key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

The use of the reader in an unapproved method, as describe on the security policy, will violate the PCI PTS approval of the reader.

General Description

Product Overview

ROAM's RP450&RP456&RP457 is a financial magnetic card reader, Chip(smart Card) reader and Contactless reader. The RP450&RP456&RP457 works with select supported devices and works in conjunction with an application that runs on the connected device. An additional layer of encryption is added by the RP450&RP456&RP457 to guarantee the card data is protected as it travels from the reader to the device.

The card reader requires a battery as an internal power source. It does not allow users to replace the battery. When the RP450&RP456&RP457 is plugged into the mobile device using an audio jack, the RP450&RP456&RP457 is powered on. Alternatively, the RP450&RP456&RP457 can be powered on by the pressing the Power button to be used with Bluetooth.

The firmware running on the RP450&RP456&RP457 can be updated. Special tools are required to update the reader.

Product Identification
The product name and hardware version is printed on the sticker of the device.

RP450 includes audio jack.

RP456 includes audio jack and bluetooth.

RP457 includes audio jack、bluetooth and MFI.

The firmware version includes the BOOT version and the CTRL version.
Get BOOT Vesion
For example,
-Sending command F6 00 0a 80 44 dd 5a a5 00 ff 01 00 00 18 03 to device with COM tool just once.If you have already sent this command before, you don't need to send it again.
-The BOOT version can be read through COM tool by sending command 02 01 00 00 00 06 F0 0C 03 00 00 00 F9 03,the device will reutrn 02 01 00 00 00 23 90 00 20 30 30 30 31 2D 46 2D 35 30 31 2D 30 30 30 31 2D 30 30 30 31 2D 30 38 00 20 20 20 00 00 00 00 00 E5 03. The characters in yellow show the BOOT version is 0001-F-501-0001-08.
Get CTRL Version
For example,
-Sending command F6 00 0a 80 44 dd 5a a5 00 ff 01 00 00 18 03 to device with COM tool just once.If you have already sent this command before, you don't need to send it again.
-The BOOT version can be read through COM tool by sending command 02 01 00 00 00 06 F0 0C 01 00 00 00 FB 03,the device will reutrn 02 01 00 00 00 2390 00 20 30 30 30 31 2D 46 2D 35 30 32 2D 30 30 30 31 2D 30 31 30 31 2D 30 43 00 20 20 20 00 00 00 00 00 9C 03. The characters in yellow show the CTRL version is 0001-F-502-0001-0101-0C.

The merchant or acquirer must visually inspect the reader when received and should ensure that:

1. There is no evidence of unusual wires that have been connected to any ports of the reader
2. There is no shim device in the slot of the magnetic card acceptor

Communication methods and protocols

Communication methods: USB、Audio Jack、Bluetooth

Communication protocols: RP450&RP456&RP457 doesn’t has IP stack and other open protocols except Bluetooth interface.The Bluetooth support specification 3.0 and 4.2.

Guidance

Installation Guide
An installation guide containing the following information is provided with the reader:

- Reader
- User manual
- Clamp

Product Service Removal
Sensitive data must be erased before refurbishing the reader or removing it permanently from service.

Periodic Inspection
The merchant or acquirer should daily check the appearance of reader:

1. Inspect the appearance of reader to make sure it is the right product
2. Inspect whether the MSR card slot has an additional card reader or other inserted bugs
3. Observe the slot of smart card reader, whether there are any wires or suspicious object.
4. Inspect whether the product appearance has been changed
5. Check if the firmware version is correct
6. Observe whether there are any visual observation corridors, and deter them by body or other shields
7. Power on the reader and check that the firmware runs well, as the startup will inspect the hardware security, authenticity and integrity of firmware

Such checks would provide warning of any unauthorized modification to the terminal and other suspicious behavior of the reader.

The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

Product Hardware Security

Tamper Response Event

The reader contains tamper mechanisms that will trigger when a physical penetration attempt of the reader is detected.

- Merchants can easily detect attack base on device display as shown below.

If the device detects attack, the device will be set tampered state. Then the device will be interval time to beep and the 4 LEDs will be continuously on and off.

- If devices tampered like above evidence, the device should be returned back to vendor.

Any physical penetration will result in a “tamper event”. This event causes the activation of tamper mechanisms that make the reader out of service. There are two separate modes in which the reader can be:

1. Normal mode – the reader is fully operational
2. Tampered mode – the reader is tampered, unable to perform any transactions

Environment Requirements

The security of the reader is not compromised by altering the environmental conditions (e.g. subjecting the reader to temperature or operating voltages outside the stated operating ranges does not alter the security).

The K21 is a secure processor, and has voltage and temperatur sensor to monitor the operational and environmental conditions. If voltage is lower than 1.45V or higher than 3.8V,temperature is out of range

-60℃～150℃,which will trigger the tamper mechanism and the sensitive data will be erased.

Product Firmware Security

Software Development Guidance

During the software development, the following steps must be implemented：

1. Requirements analysis
2. Software development
3. Code review、Security review and audit
4. Module test
5. Source code management and version control
6. Software test
7. Signature and release

For more development details, please refer to <Application development manual>

Firmware,Software and Configuration Parameters Update

Updates and patches can be loaded in the device. They are cryptographically authenticated by the device. If the authenticity is not confirmed, the update or patch is rejected.

Any security related firmware changes will cause firmware version update.

Signing mechanism

This device implements asymmetric algorithm for firmware authentication use. RSA algorithm with 2048bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware.

The firmware is signed by RSA-2048 bits private key which is only controlled by LANDI. And the firmware authentication is executed by signature verification using corresponding public key of LANDI.

Before firmware running every time, their integrity and validation will also be checked. If failed, the terminal will not work correctly.

The certificate and signature of the firmware code are verified. The certificate and signature are based on couples of RSA keys.

Update and patch procedures

The device supports both local and remote methods for updating or patching the software, the firmware, and the configuration parameters.

1. The patch must be Security reviewed and audited before releasing.
2. The patch must be tested before releasing.
3. The patch must be digital signed before releasing.
4. The device uses digital signature to authenticate the patch. If the patch is illegal, then the device will delete it.

Self-Tests

The reader performs start-up and periodic self-tests.

- During the power on of BOOT, BOOT verifies the SHA-256 of itself. If failed to verify, the BOOT will enter infinite loop and beep.
- If any authentication failed and usb wasn't detected in Boot, it will power down after waiting 5 seconds.

  If any authentication failed and usb was detected in Boot, the device will enter download mode.
- If the CTRL failed to verify all files included all certificates,all parameters files,user,ctrl,the CTRL will beep and enter infinite loop.
- If CTRL detected attack or failed to self-test all keys, the device will be erased all keys and be set tampered state. Then the device will be interval time to beep and the 4 LEDs will be continuously on and off.
- The device will perform self-test every 20 hours.

OEM module

For that OEM modules ,because there may be potential vulnerabilities, so the data between OEM module and secure processor must be encrypted.

System Administration

Configuration Settings

The reader is functional when received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements.

Default Value Update

The reader is functional when received by the merchant or acquirer and there is no security sensitive default value (e.g. admin password) that needs to be changed before operating the reader.

Key Management

Key Management Techniques
The reader implements key management techniques as below:

1. DUKPT: a key management technique based on a unique key for each transaction

Cryptographic Algorithms
The reader includes the following algorithms:

1. Triple DES

Key Table

Key Name	Usage	Algorithm	Size (Bits)	Origin of the key	Number	Uniqueness
E2EE DUKPT Keys (Future Keys)	Account data encryption	TDEA	128	Derived originally from E2EE DUKPT initial Key	Up to 21 future keys	Device
E2EE BPK_DUKPT	Encrypt E2EE DUKPT KEY in TR-31 FORMAT	TDEA	128/192	itself	1	Device

Key Replacement
keys should be replaced with new keys 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.

Key Loading Policy
The reader does not propose manual cryptographic key entry. Specific tools, compliant with key management requirements, shall be used for key loading.

The key loading process is implemented in a secure room and strictly protected under dual control techniques.

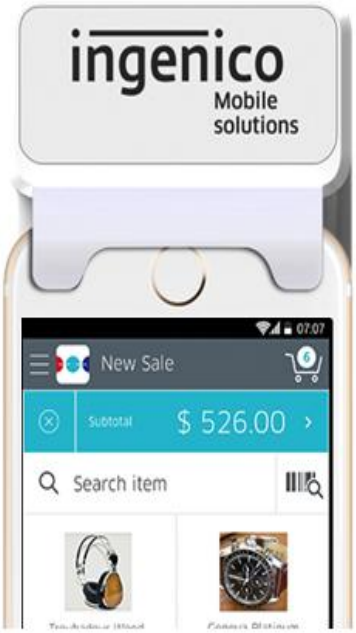
In addition to the local key injection, the device also supports remote key injection.

Installation and Operation Guidance

Installation

Three flexible uses – audio jack, Bluetooth companion, and desktop reader

Compatible with hundreds of iOS and Android smartphones and tablets.Auto-adjustable clamp to securely attach to virtually any mobile device.



Security Check

The salesperson should check the security of device every day before starting to use. The follow item should be checked:

(1) Observe the surface of device, whether there are scratches and repair.

(2) Power on the device, check whether the device is under activated mode and without any tamper event.

Roles and Services

The reader has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.