Reference:	NL_SP_ME31
Revision:	00.02
Date:	31/05/2019
Distribution:	Public

SECURITY POLICY FOR ME31 SERIES

RECORD OF REVISIONS

Revision	Date	Writer	Object of Evolution
00.01	11/02/2015	Newland E.	Initial version
00.02	31/05/2019	Newland E.	Remove page footer

APPROVAL

Name	Department	Function	Date	Visa

DISTRIBUTION LIST:

TABLE OF CONTENTS

1 GLOSSARY

PCI-PTS	Payment Card Industry PIN Transaction Security
TOE	Target of Evaluation
KLD	Key Loading Device
PIN	Personal Identification Number

2 REFERENCE DOCUMENTS

[REF01] Payment Card Industry (PCI). PIN Security Requirements. Available in www.pcisecuritystandards.org.

[REF02] Newland Key Loading And Sw Signing / Authentication. Specification.

[REF03] Newland Development Guide For ME31.

[REF04] Newland Software Development Kit Reference Documentation

[REF05] Open_Protocol_Guidance For ME31

[REF06] ME31 User Manual

3 SCOPE AND SUMMARY

This document describes the basic security policy for developers and users to ensure the proper use of FW security features in Newland Devices and for compliance with current security standards.

This document must be read in conjunction with the related Reference Documentations. The document covers the following products: ME31 series(Handheld POS).

This document is included in the SW development toolkit and is distributed only to trusted program developers, internal users and selected end users.

4 GENERAL DESCRIPTION

The device ME31 series (ME31/ME31S) is intended to be used as a Handheld POS in an attended environment, and it can't be used in an unattended environment.

4.1 Functionality

This device is a PIN entry device, it can be used as the standard POS to undertake financial transactions. Performing the PIN entry, MAC calculation, Data encryption/decryption and some other functionalities provided:

This device provides 19 buttons' keypad, contactless card reader, ICCR, MSR, LCD, thermal printer, modem. It is designed for a portable and handheld use, so that the device can be shielded by the body when in work. The power system is based on a DC 9.0V power supply or battery and the communications to the external world are based on USB, RS232, WIFI, or GPRS wireless connection.

4.2 Device Identification

4.2.1 Appearance

Please check whether the appearance of ME31/ME31S is the same as follow, including the hardware version in the label attached to the rear casing:

Figure 1. View of ME31

Figure 2. View of ME31S

4.2.2 Version information

User should check if the firmware version is consistent with vendor provided information (From mail or vendor website). To retrieve detailed version information of ME31 series, please follow below operations.

1. Power up device, the device will stay on the main menu of firmware.

2. Switch to the version item by guide function key ‘F1’ or ‘F2’, then press enter to see detailed firmware version information:

Boot version

Software version

3. For the HW version they are printed in the label attached to the rear casing.

Figure 3. The label of ME31

Figure 4. The label of ME31S

5 SECURITY GUIDANCE

Before using the device, user need to check device firstly to see if it is genuine and ready for use. Meanwhile user should also refer to the <ME31 user manual> attached within the packing case.

To inspect the received device, please check carefully of the following aspect described in the rest of this section.

5.1 Environmental Requirements

The device a Handheld POS used in an attended environment, and the use of the device in an unapproved method will violate the PCI PTS approval of the device. The device use a private shield to protect PINs during PIN entry in terms of different visual observation attacks.

The customer should be advised to take care that he is not overlooked when entering his pin code.

The environmental conditions to operate the device are specified in the device's specifications.

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

5.2 Periodic Security Inspection

The user should refer to the user manual to conduct the following daily inspection in light environment or with help of the light source:

(1) Inspect the appearance of device to make sure it is the right product.
(2) inspect whether the IC card reader's slot has untoward obstructions or suspicious objects at the opening;
(3) inspect whether the MSR card slot has an additional card reader and other inserted bugs;
(4)inspect whether the product appearance has been changed, such as the display, keypad area and so on.
(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 device and check if 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 modifications to or substitution of the terminal, or suspicious behavior of individuals that have access to the terminal.

5.3 Device Self-Test

The device will perform self-test upon startup and also every 24 hours. Periodical self-test is done by automatically reboot. This reboot period is count up once the device is powered on.

Self-Test include:

- Firmware integrity and authenticity
- Hardware security status

And if there is any kind of failure detected by self-test mechanism, the firmware will display a prompt indicating tampering status. At this situation, the device will be disabled and cannot be used. It should be sent to an authorised service centre for repair.

5.4 Decommissioning / Removal

When the device is no longer used for permanent decommissioning reason, the administrator of device need to gather the device and then erase all the key materials on it. It can be done by directly disconnecting the device to make it tampered.
For the temporary removal, there is no need to change the state of the device, as all the keys are still protected safely with the main board battery power supply

6 KEY MANAGEMENT

6.1 Key Management System

The device supports the following key management: FIXED, MK/SK, DUKPT. (Please refer to ANS X9.24 for more details of these techniques).

For the account data protection, please note that it is forbidden to load same key to multiple devices. Each device must have unique key.

The device includes the following algorithms:

- Triple DES (112 bits and 168 bits)
- RSA (Signature verification, 2048 bits)
- SHA256 (Signature digest)

6.2 Key Types / Usages

The supported transaction keys are classified into following types/usages:

- TMK: terminal master key used as key encryption key(KEK). This key is generated and distributed by the Acquirer. It is only used to unwarp and install the ciphertext working keys (TPK/TAK/TDK).

- TPK: PIN encryption key. Generated and installed by the Acquire. It is used to encrypt user PIN input and generate the ciphertext PINBLOCK.

- TAK: MAC encryption key. Generated and installed by the Acquire. It is used to do TDES MAC encryption.

- TDK: Data encryption key. Generated and installed by the Acquire. It can be used to do data encryption/decryption.

The algorithm used by above keys is TDES.

The transaction keys are generated by the Acquire. All keys installed on the device cannot be achieved in any way from external. Key can only be used for specified purpose through the device provided interfaces/commands.

6.3 Key Injection

The initial key include:

- TMK of MKSK system,

- TPK/TAK/TDK of FIXED system

- DUKPT Initial key.

Initial keys should be loaded to the device by an authentic Key Loading Device (KLD) in a secure environment.

For the working keys of MKSK system, they can be loaded in ciphertext under protection of TMK.

6.4 Key Removal

Once the keys are loaded to device successfully. They will be available unless the administrator wants to erase all keys for some reason like decommissioning. Or when a tamper issue is detected so that all the keys will be erased by the firmware automatically.

PLEASE NOTE THAT:

If one key has been COMPROMISED, this key and its distributed keys should not be used any more. User can use another working keys that are still safe. But if the device is tampered, it's requested to send the device to an authorised service centre for repair and re-download the new keys.

6.5 Firmware Signing / Authentication

Asymmetric cryptographic algorithm is used for the firmware authentication:

- SHA256 is used to compute the digest of firmware.

- RSA 2048bits key is used for signature verification

The firmware is signed by RSA-2048bits private key. And this signer key is only controlled by NEWLAND. And the firmware authentication is done by signature verification using corresponding public key of NEWLAND.

7 INSTALLATION GUIDANCE

Users should refer to ME31 User manual [REF06] before installation. The following requirements and recommendations are applicable during the Installation Phase.

7.1 ROLES

Terminals are delivered to end users in their ENABLED state. Terminals in their enabled state can process the PIN entry normally.

7.2 Configuration settings

No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements. And also there is no security default value that needs to be updated by the end user.

7.3 Tamper Response

In the event of tamper detection, the device will enter the DISABLED state, displaying a tamper detection message. The device will therefore be locked and no further secure function can be performed in it.

7.4 Software update

Newland terminals will only accept signed SW. The SW loading process does not need to be protected in any special way other than installation best practices. Since the device will refuse to load any unauthenticated SW, the process of Firmware loading serves to authenticate the loaded SW.

Note that tampered devices will appear as disabled, and will not allow for user SW to run even if it's authentic.

8 OPERATION GUIDANCE

The following requirements and recommendations are applicable during the Operation Phase:

8.1 PIN Entry Privacy Messages

Acquirers and merchants MUST enter the PIN safely.

For Newland devices intended to be used as a desktop POS, it is required to provide cardholders with the necessary privacy during PIN entry. The methods to ensure PIN entry privacy is through the device's private shield.

For Newland devices intended to be used as a handheld POS, it is required to provide cardholders with the necessary privacy during PIN entry. One of the methods to ensure PIN entry privacy is through the inclusion of guidance messages and logos for the cardholder as part of the payment application. Such messages and graphics must convey easy-to-understand information on how to protect the PIN from sight, such as by using the cardholder’s own body or their free hand to block the view of the keypad. Figure 8-1 shows an example of a safe PIN entry logo which could be displayed by the application prior to or in conjunction with the PIN entry prompt message.

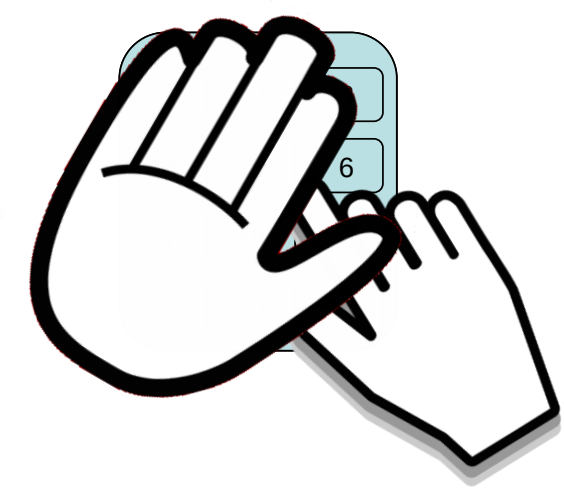

Figure 8-1. Safe PIN Entry Logo Example.

8.2 Maintenance

Devices which are detected as DISABLED through the system of requirement MUST NOT be used without further investigation of the causes of the tamper. Users are advised to seek technical support from their terminal service partners or directly from NEWLAND.

9 DEVELOPMENT GUIDANCE

Newland terminals implement the necessary security measures and functions to provide compliance with the PCI security requirements for authenticated applications.

For an application to ensure compliance, please refer to <Newland Development Guide>[REF03], which includes the following security guidance that must be observed:

- PIN Entry and Encryption
- Prompt Management
- Open Protocol Implementation guidance
- SRED Implementation guidance