HANMEGA EPP(Pinpad) KeyManagement

Rev. 1.0.0.0

5 September 2022

R&D Center S/W Team

REVISION HISTORY

Rev.	Date	Page	Description of Change
0.0.1	21 December 2020		Draft Edition
1.0.0.0	5 September 2022		Change to GUI

TABLE OF CONTENTS

SUMMARY

This document has been prepared to help understand the management of EPP encryption keys,
and is composed of basic information that users should be aware of.

This document describe how to use and control LxKeyManagement application

You can call LxKeyManagement from a Linux terminal.
If KIOSK or ATM application want to manage keys for supporting PCI standard,
implement it by referring to the LxKeyManagement source included in the libgenmegadevice package.

The KIOSK must invoke EPP_Close method of libgenmegadevice SDK and check the serial port is closed.
After close the port, invoke Key Management application with following parameters.

LxKeyManagement PORT_NAME
- PORT_NAME : Specify serial port for PinPad.

ex) > LxKeyManagement /dev/ttyS1

NOTE: Files needed to execute key management.
Executable file: /usr/local/bin/LxKeyManagement
Terminal information files: Files in the /usr/local/share/genmegadevice/terminfo directory

** It is automatically installed when installing the libgenmegadevice debian package.

1. Introduction

The EPP has two mode 'Normal' and 'Secure'.
The 'Secure' mode is for supporting PCI standard.
If KIOSK application doesn't need to support PCI key management,
Just can use 'libgenmegadevice SDK package' without LxKeyManagement appication.

If KIOSK needs to support PCI standard key management functions,
you can use LxKeyManagement to set the master key.

It can also be used when changing maintenence mode or operation mode.

1.1 Support Encryption Key

1) SINGLE DES : * It is not supported from PCI 5.x.
Single data DES encryption standard

2) DUAL DES : * It is not supported from PCI 5.x.
Dual data DES Encryption Standard

3) TRIPLE DES :
Triple data DES Encryption Standard

4) MAC, SING DES : * It is not supported from PCI 5.x.
It includes Single data DES encryption standard and MAC encryption.

5) MAC, TRIPLE DES :
It includes Triple data DES encryption standard and MAC Single encryption.

6) TRIPLE MAC, TRIPLE DES :
It includes Triple data DES encryption standard and MAC Triple encryption.

1.2 EPP Commands requiring secure mode

HM_DEV_SECURE_MODE_ERR (-4) is returned if the libgenmegadevice SDK's EPP is not in secure mode.

1) EPP_ChangeSecurePassword
2) EPP_SetKeyMode
3) EPP_SetActiveKey
4) EPP_InputKey
5) EPP_InstallKey
6) EPP_InstallDefaultKey
7) EPP_AuthorizedMoving
8) EPP_AuthorizedFixing
9) EPP_ClearAllData

** Refer to the API_Ref_for_UniversalKiosk_Standard file for an explanation of the command.

1.3 EPP Key Layout

1	2	3	D
4	5	6	E
7	8	9	F
A	0	B	C

EPP (Encrypted Pin Pad) Master Key Alpha-Numeric Key Layout

NOTE:

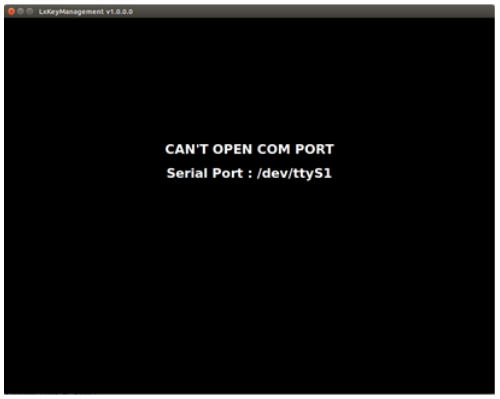
The keypad above is (EPP-B3, EPP-B5) PCI / Interac certified EPP Device.
Previous models of Genmega EPP (PCI Only) had the Enter and Cancel keys reversed from what is displayed above.
If entering keys on the PCI only keypad,
remember that the Enter key is always F and Clear Key is always E and the Cancel key is always D

2. Factory-Reset EPP installation.

2.1 Serial port connection

Invoke Key Management application with following parameter.
If there are no parameters, it connects to the default /dev/ttyS1.

ex) > LxKeyManagement /dev/ttyS1



[EPP Serial port Connection Failure]

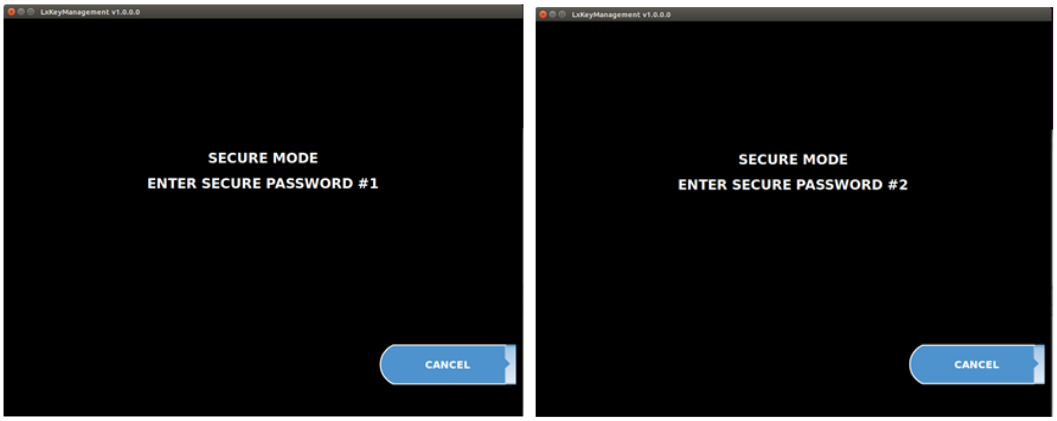
2.2 Initial screen

Select the KEY MANAGEMENT button using the mouse.

2.3 Input Default Secure Password

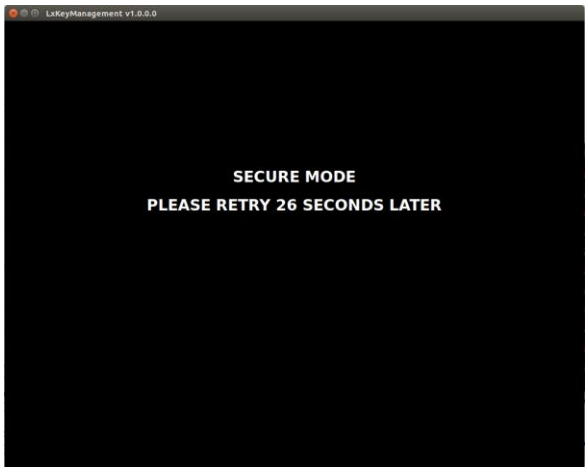
Access to Key Management requires entering a “Secure Mode” which engages additional security measures to prevent Master Key tampering. Make note of these changes as it does affect how keys are entered

Entering Key Management requires two 6-digit or 8-digit passwords (PCI v3.x : 6-digit, PCI v5.x : 8-digit)
By default these will be (PCI v3.x : "000000", PCI v5.x : "00000000") for part #1 and (PCI v3.x : "000000", PCI v5.x : "00000000") for part #2.



[Input Secure Password Screen]

If you enter the "Secure Mode" password incorrectly, you will be prompted to wait 30 seconds if you try again before 30 seconds have passed.

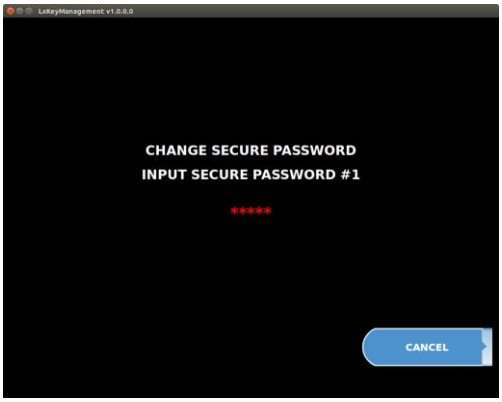


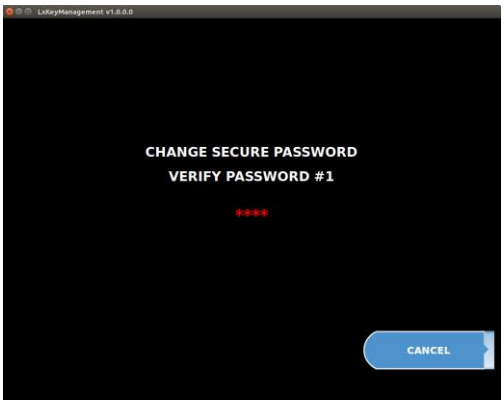
NOTE: In compliance with PCI specifications,
you must change the Secure Mode Passwords from default before any Master Keys can be entered.

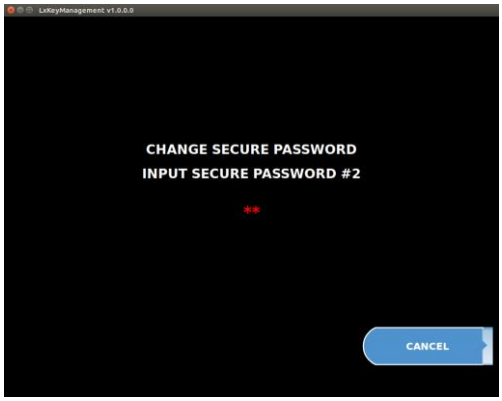
If you are ever forced to wait for the 30 second retry timer,
back all the way out of the menus and wait a full 30 seconds before retrying or the timer will not reset.

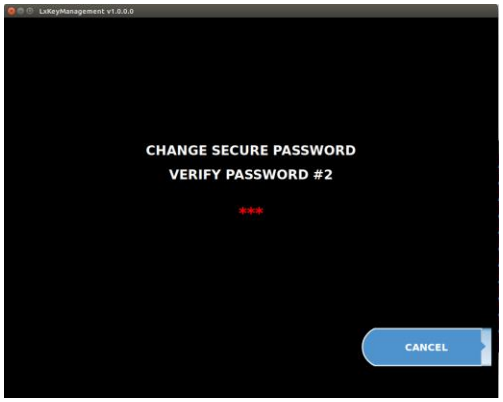
2.4 Change Default Secure Password

Enter the password to be changed.
Password change STEP : INPUT PART #1 -> VERIFY PART #1 -> INPUT PART #2 -> VERIFY PART #2

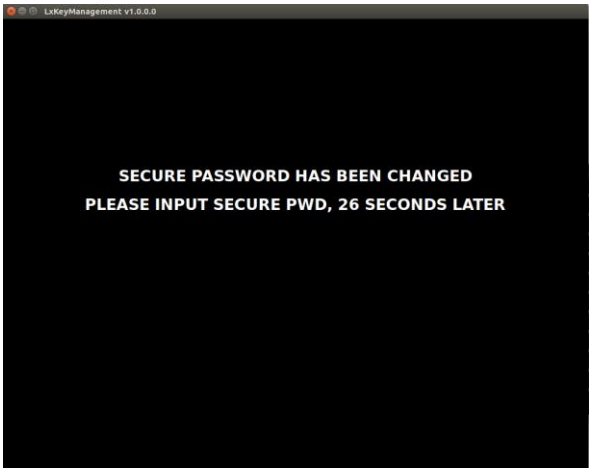








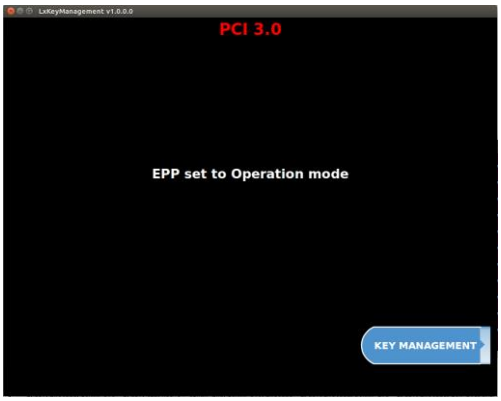
When the password change is successfully completed,
a message prompting you to enter the password is displayed after 30 seconds with a completion message.



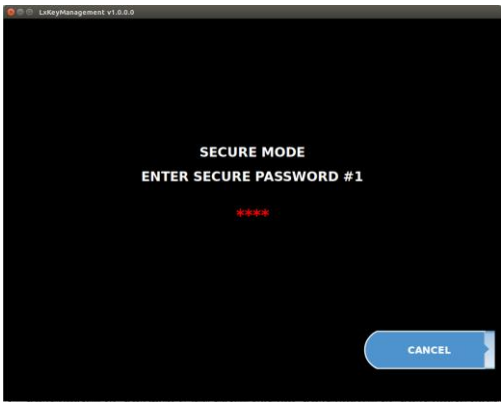
NOTE: For PCI v5.x, the password cannot be the same for PART1 and PART2, and all 8-digit passwords must not be the same number. PCI v3.x has nothing to do with this.

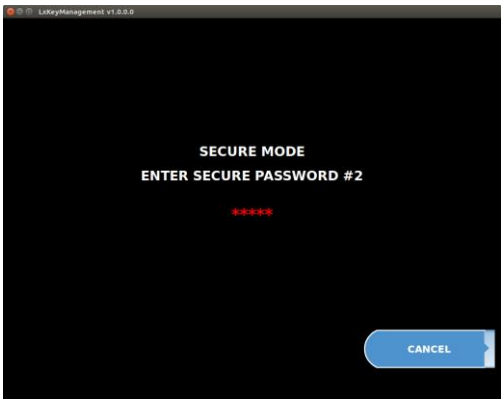
2.5 EPP Initialization processing

After the default password change is completed, the screen for set the operation mode is displayed.
Select the KEY MANAGEMENT button using the keyboard (7) or mouse.

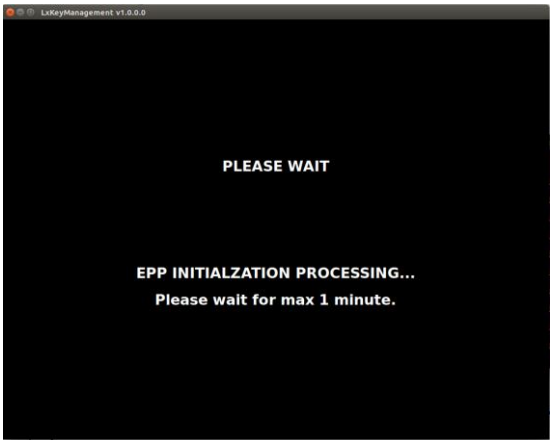


When the password input screen is displayed, enter the changed password





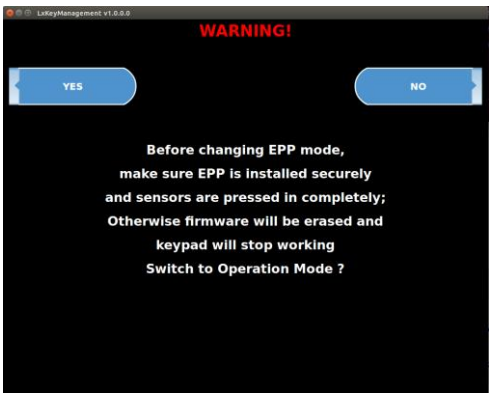
When the password input is completed, the EPP initialization processing screen appears.
Inject the default keys of EPP (Transmit Key, NON PIN Working Key, etc...)

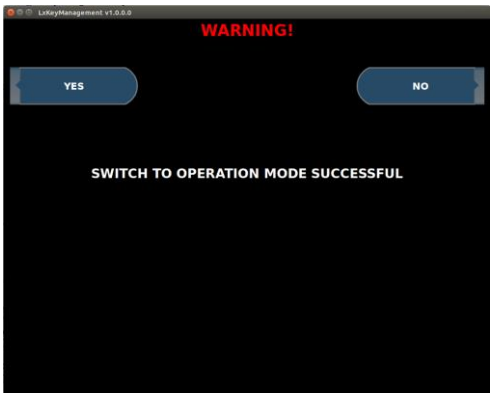


NOTE: PCI v5.x may wait longer than 1 minute.

2.6 Set to operation mode

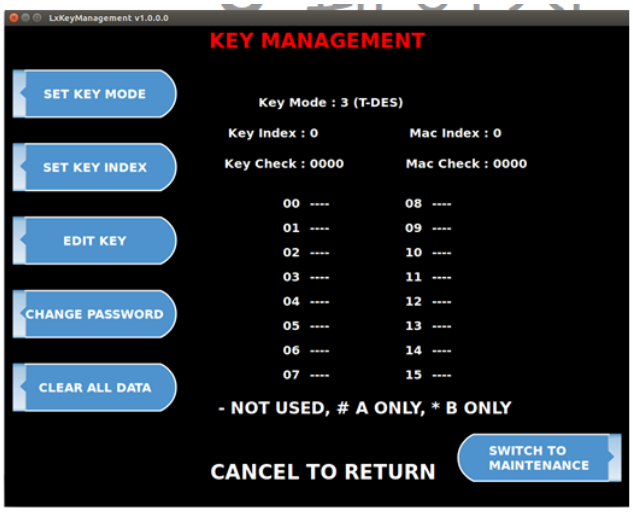
The screen for changing EPP from maintenance mode to operating mode is displayed
Select YES to change to the operating mode.





NOTE: Before changing EPP mode, make sure EPP installed securely and sensors are pressed in completely.
Otherwise firmware will be erased and keypad will stop working.

All initial processing are now complete and the KeyManagement main menu is displayed.
You can see that the default KEY MODE is set to Triple DES.

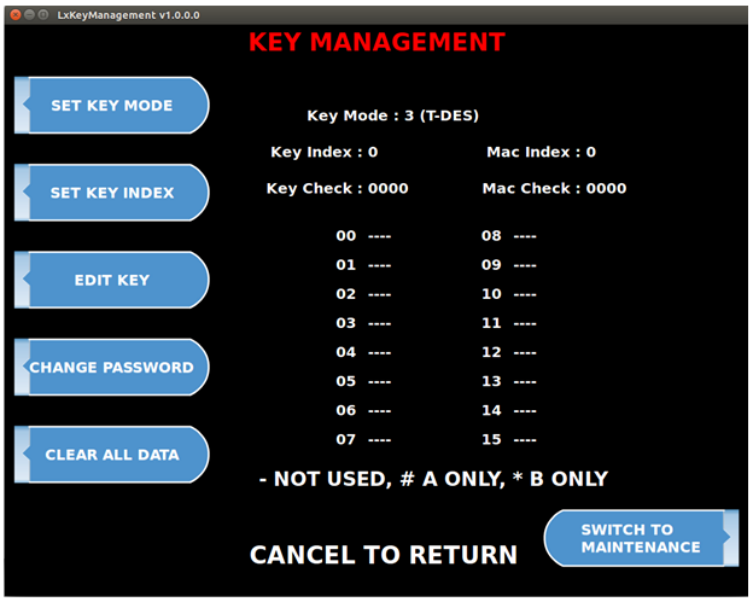


NOTE: In compliance with PCI specifications,
you must change the Secure Mode Passwords from default before any Master Keys can be entered.
After 30 seconds of changing the security mode password, you will be prompted to enter the changed password again.
After this step, you can enter Master Keys.
Successful entry of both passwords will grant access to the Key Management screen.
From the moment the Key Management area is entered, 30 seconds timer begins.
At the end of 30 seconds, regardless of what you are doing (entering a master key for example)
the Key Management area times out and LxKeyManagement will be terminaated.
Making a mistake during this process can start a 30 second reset timer.

3. KeyManagement Menu

3.1 Menu Screen

Display the menu and the key status
Press EPP's CANCEL to end KeyManagement.



NOTE: Partially entered keys will appear in the index as #### or **** which denotes that either part A or part B has been successfully entered. (PART A = #, PART B = *)

SET KEY MODE:

This option sets the type of master key you will be loading (TDES, DES, MAC etc.)

SET KEY INDEX:

The EPP will hold up to 16 individual Master Keys.
15 is used as an index for MAC or T-MAC KEY only.
The EPP will only use the key that the index is set to regardless of how many keys are installed.

EDIT KEY:

This is where enter two 16-digit Keys (PART A / PART B).
First, prompted to enter the index to store the key.
After entering the index, can enter the key.
PCI v5.x cannot enter the same key as the stored key.

CLEAR ALL DATA

Delete all keys and data stored in EPP and initialize EPP.
EPP is in the same state as factory reset.

CHANGE PASSWORD:

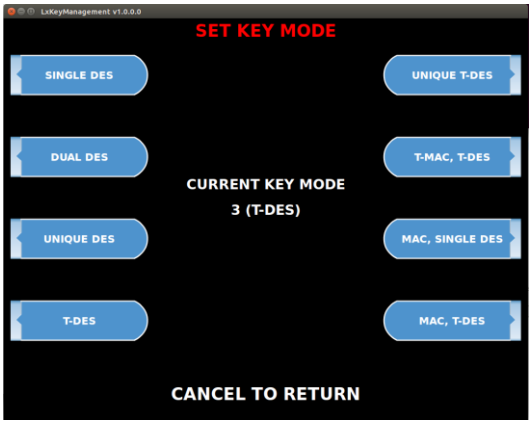
This allows you to set each part of the “Secure Mode” Password (PART A(#1), PART B(#2))
The secure password is 6 digits for PCI v3.x and 8 digits for PCI v5.x.
For PCI v5.x, the password cannot be the same for PART1(#1) and PART2(#2), and all 8-digit passwords must not be the same number.
This does not apply to PCI v3.x.

SWITCH TO MAINTENANCE:

Uninstall the installed EPP for movement.
Use if you want to move the EPP for maintenance.
Detaching without uninstall the EPP erases all data and blocks the firmware.
After that, the EPP cannot be used and the EPP must be replaced.

3.2 Set Key Mode

This option sets the type of master key you will be loading (TDES, DES, MAC etc.)
The currently set key mode is displayed.
Press EPP's CANCEL to return to the main menu.



[PCI v3.x]

[PCI v5.x]

SINGLE DES: 16 digit master keys entered as Part A and Part B

DUAL DES: 16 digit master keys entered as Part A and Part B (a common key is entered, and then a working key is downloaded from the host).

UNIQUE DES: 2 - 16 digit master keys entered as Part A and Part B - with 10 digit unique serial number entered prior to each part

TRIPLE DES: 32 digit master keys entered in 16 digit pieces, Part A (left and right) and Part B (left and right)

UNIQUE T-DES: 2 – 32 digit master keys entered in 16 digit pieces, Part A (left and right) and Part B (left and right) - 10 digit unique serial number entered

T-MAC, T-DES: 32 digit master keys entered in 16 digit pieces, Part A (left and right) and Part B (left and right)
with 2 additianal 32 digit MAC keys entered in 16 digit pieces, Part A (left and right) and Part B (left and right) in index 15

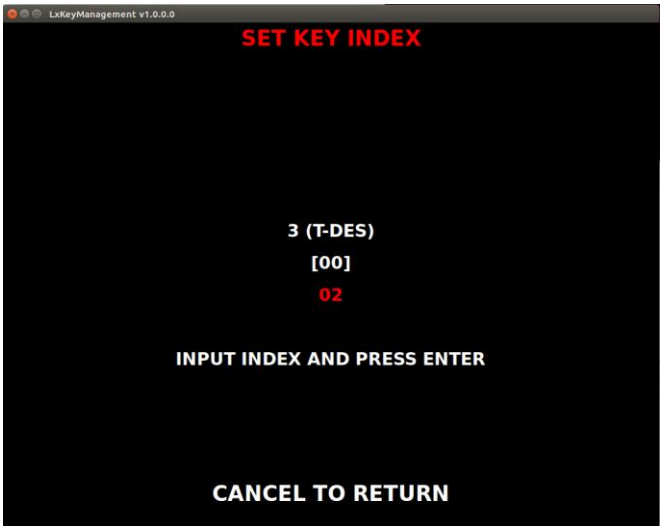
MAC, SINGLE DES: 16 digit master keys entered as Part A and Part B
with 2 additional 16 digit numbers entered as MAC Part A and Part B in index 15

MAC, T-DES: 32 digit master keys entered in 16 digit pieces, Part A (left and right) and Part B (left and right)
with 2 additional 16 digit numbers entered as MAC Part A and Part B in index 15

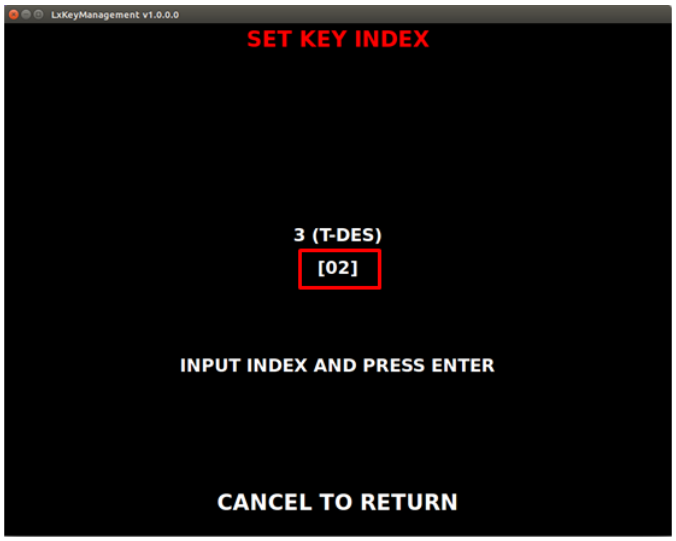
NOTE: PCI v5.x only supports T-DES for increased security

3.3 Set Key Index

Change the index of the injected master key.
Pressing the CLEAR key erases each character.



Enter the index to be selected and press ENTER to apply.

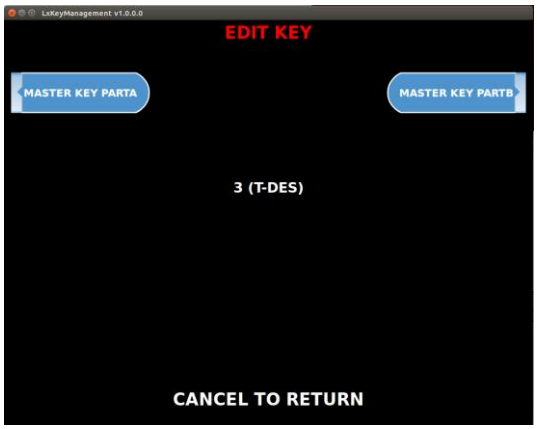


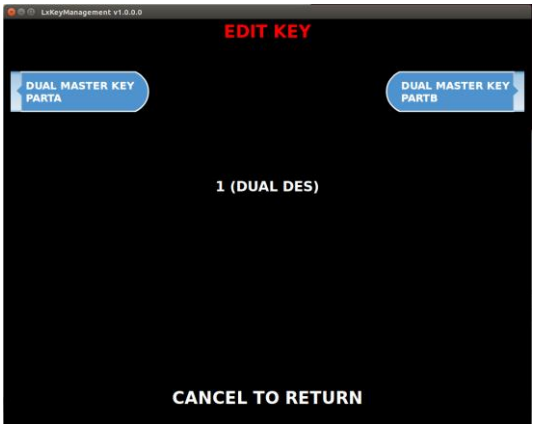
NOTE:

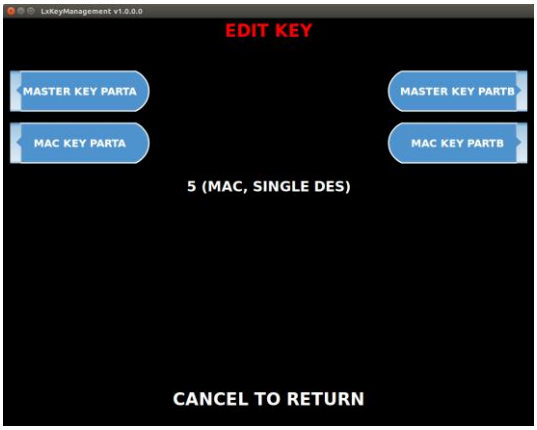
The unique master key is in position (#12-#14), the MAC key is in position #15 and the other master keys are (#00-#11).
Entering an index without an injected key will not set it.

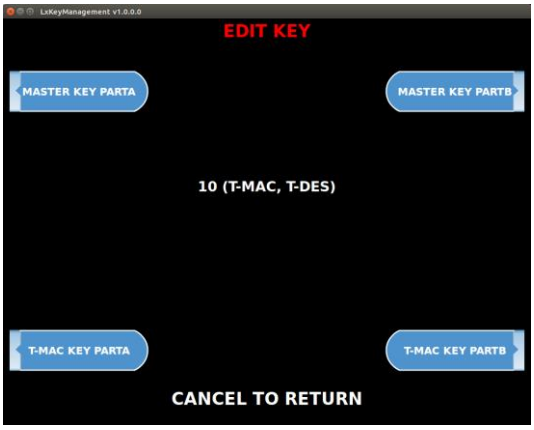
3.4 Edit Key

In the key mode that includes the MAC key, an additional MAC key button appears.



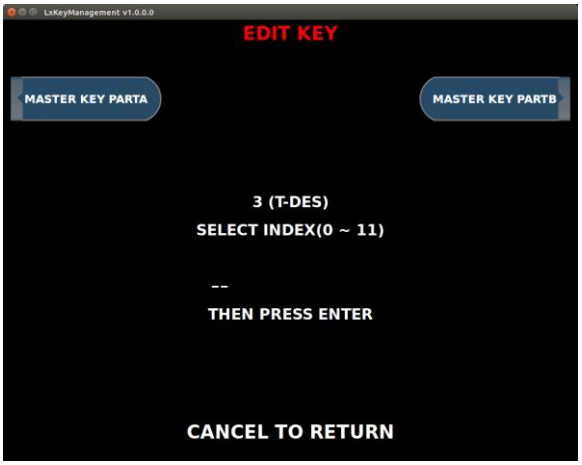






NOTE: PCI v5.x cannot enter the same key as the stored key.

Once you have selected Part A or B, you'll be prompted to enter a Key Index.
Enter the index to be selected and press ENTER to apply.
This index points to the location where the key will be stored.
There are 16 possible memory locations (0-15) available.

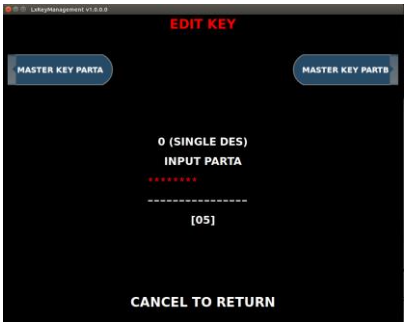


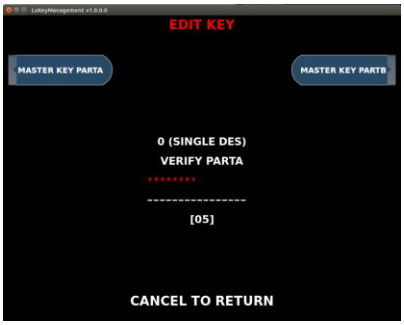
NOTE:

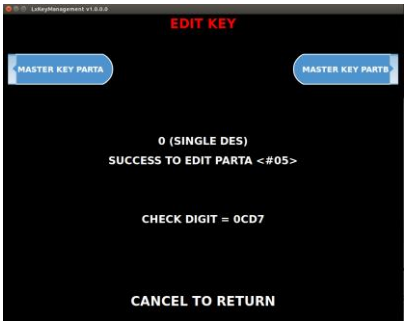
The unique master key is in position (#12-#14), the MAC key is in position #15 and the other master keys are (#00-#11).
Entering an index without an injected key will not set it.

** Master key input
Enter the key for each part (PART A, PART B)
DES is 3 steps: INPUT KEY -> VERIFY KEY -> CONFIRM
T-DES is 5 steps: INPUT LEFT KEY -> VERIFY LEFT KEY -> INPUT RIGHT KEY -> VERIFY RIGHT KEY -> CONFIRM
In the confirm step, the index and the check digit of the entered key are displayed.

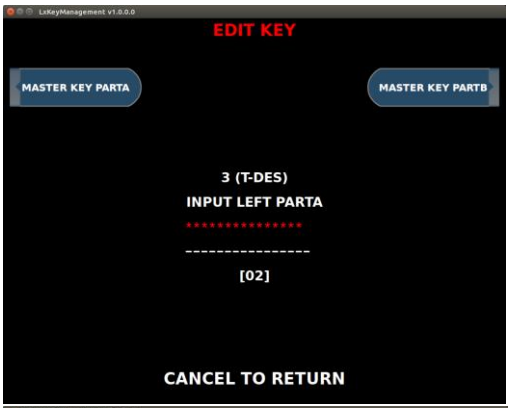
* Enter the SINGLE DES master key or MAC Key

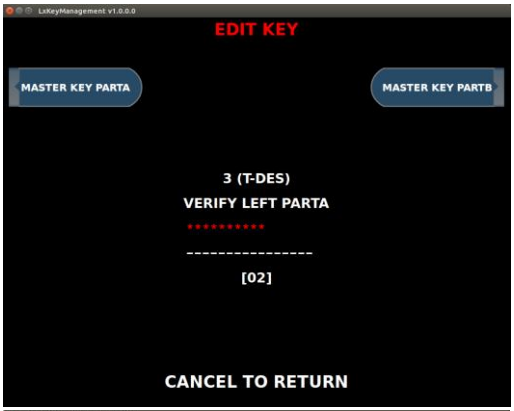


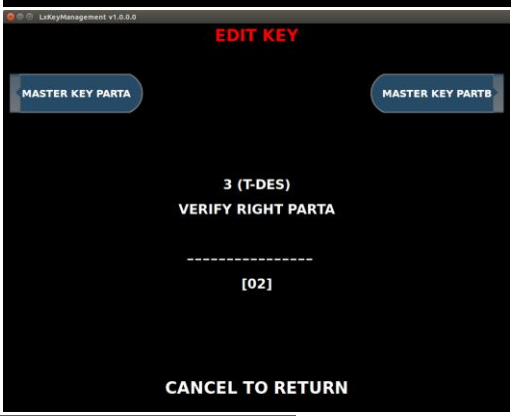


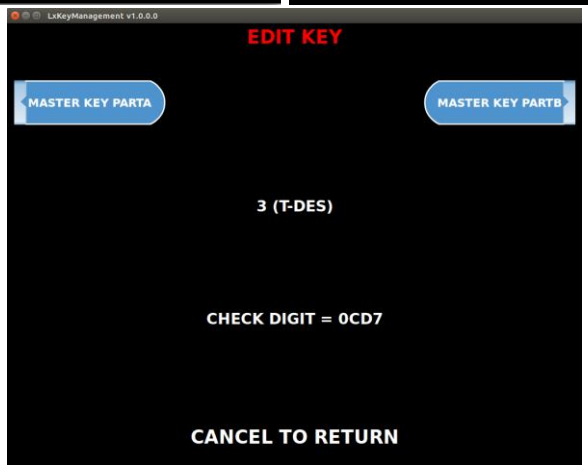


* Enter the TIRPLE DES master key or TIRPLE MAC key



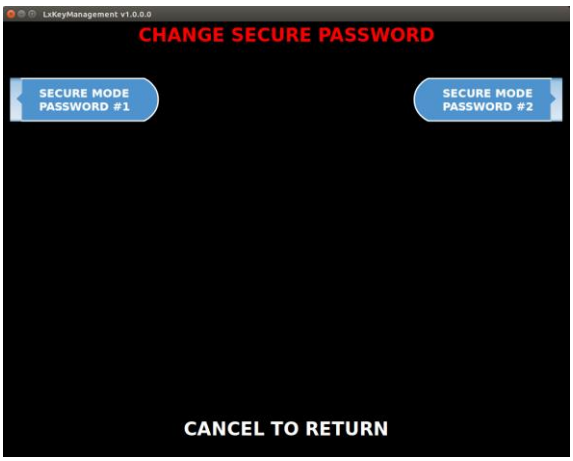




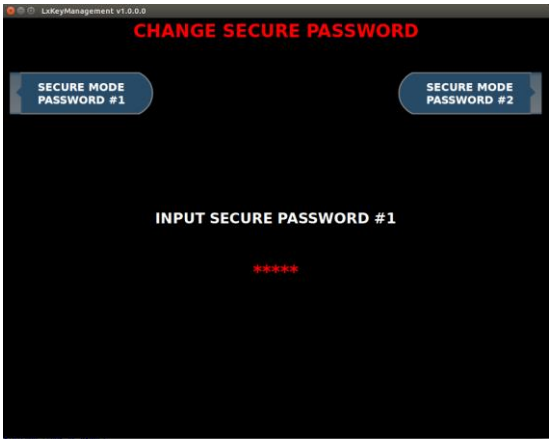


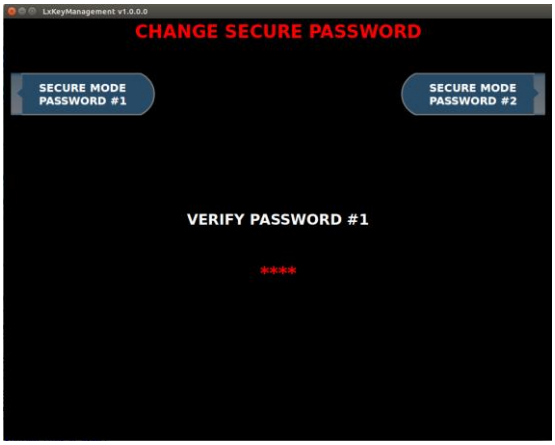
3.5 Change Password

Change the security password for each part.



Password change STEP : INPUT PART (#1 or #2) -> VERIFY PART (#1 or #2)

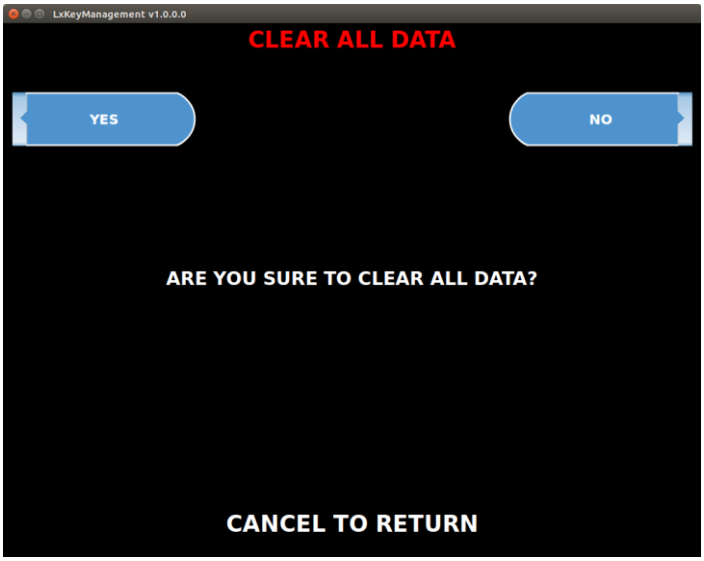


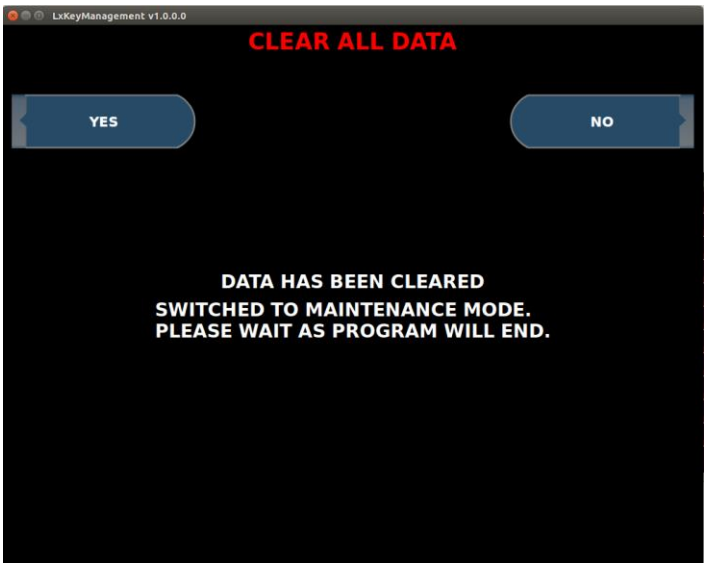


NOTE: For PCI v5.x, the password cannot be the same for PART1 and PART2, and all 8-digit passwords must not be the same number. PCI v3.x has nothing to do with this.

3.6 Clear All Data

Delete all keys and data stored in EPP and initialize EPP.
Select NO or press the Cancel key to return to the main menu

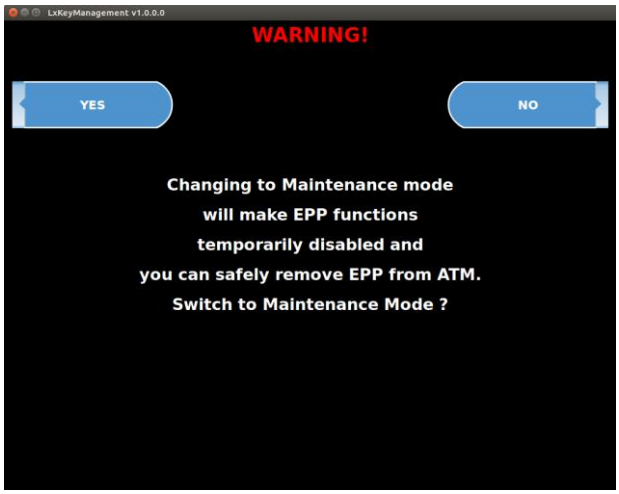


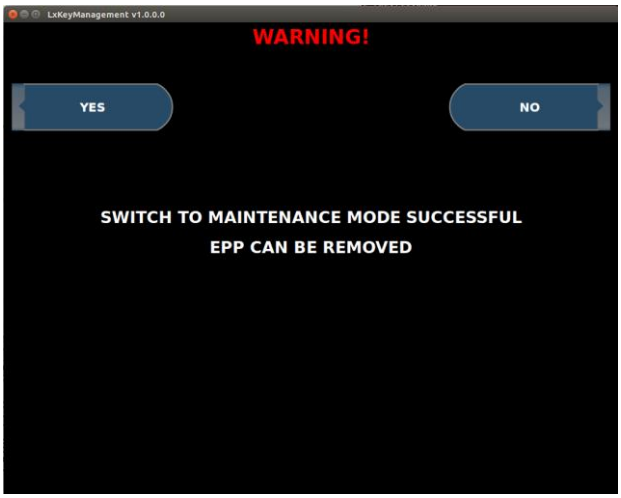


NOTE: EPP is in the same state as factory reset.
The secure password is also changed to the default password.

3.6 Switch to Maintenance

Change the EPP to maintenance mode so that it can be moved.
Changing to maintenance mode will make EPP functions temporarlly disabled and you can safely remove EPP from ATM





NOTE: The keys stored in the EPP remain, and the password remains the same.
The key and secure password stored in the EPP can be installed and used in other ATM.