NXP Semiconductors
Solution Release Notes

Document Number: LPOSRS003SRN
Rev. 2, 04/2018

Linux Point of Sale (LPOS) Reader Solution Release Notes

Contents

1. Overview

The Linux Point of Sale (LPOS) Reader Solution SDK is based on the Linux 4.1.15_2.0.0_ga BSP release from NXP and customized for i.MX6UL TWR POS board. Most of the functional modules have been ported to OPTEE Secure OS version 2.4.0. This includes the full set of secured peripheral drivers (CAAM, PINPAD, EMVSIM, SPI/GPIO, Tamper) used to provide secure services to the payment applications running Linux user space.

2. Software Modules

The individual software components of the LPOS Reader Solution Kit are described in the below subsections.

2.1. Linux

BSP version 4.1.15 release 2.0.0 for iMX6UL TWR-POS board was used, with the RT (real-time) patch applied to satisfy performance criteria required by EMVCo L1 certifications on CT/CL secure card operations.

2.2. OPTEE OS

Version 2.4.0 was ported on iMX6UL TWR-POS board and augmented with required drivers and secure services. This might be updated latest the version (3.0 currently).

2.3. Secure LCD (secure and non-secure)

The Secure LCD driver has been ported to OPTEE OS as a core driver and associated PTA interface and shares the LCDIF with the Linux LCD driver in non-secure world. An arbitration mechanism has been created to effectively make the switch when necessary between the two OS worlds.

Features:

- [LINPOSR-6] - Ported GUI payment application from eGUI API to QT API
- [LINPOSR-18] - Implemented framebuffer sync between normal and secure world (optee)

2.4. PINPAD (secure)

PIN processing and crypto services have been ported to OPTEE as separate TA's and communicate with the hardware module through the GPIO driver.

*Note: Cancel button ('X') may function with short delay when trying to decline on-going card transaction operations. Only critical secure operations

2.5. LED, Buzzer (non-secure)

Implemented as non-secure world functionalities, using the GPIO driver in Linux OS.

2.6. AppAuth and SigVer (secure)

Application authentication and signature verification is done through OPTEE secure interface API, as a specific purpose TA, which uses the crypto services provided by the CAAM driver to compute the necessary computations.

2.7. ISDM

A secure services request (to OPTEE) monitoring system has been put in place in order to validate at runtime the sequence of operations and signal unauthorized attempts to access secured data and functionalities.

2.8. CAAM (Crypto) (secure)

Cryptographic acceleration functionality in i.MX6UL (CAAM) has been implemented in OPTEE and all specific TEE software crypto API calls have been routed to this driver. This will assure optimal performance for all required cryptographic operations.

2.9. NXP L2 HAL (secure)

API's for Card Reader and Crypto operations have been developed in secure world using the OPTEE framework. The NFC Reader Library (NFC stack and libraries) has also been ported as a submodule (TA) in OPTEE and will be serving the calls coming from normal world component - EMV L2 HAL (SHIM).

2.10. EMVSIM (CT card reader) (secure)

SIM driver for Contact interface (TDA8035) has been ported to OPTEE environment (stack, libraries) and all functionality is exercised through the NXP L2 HAL interface.

2.11. SPI/GPIO (secure)

SPI and GPIO drivers supporting PN5180 communication, PINPAD, LED and Buzzer functionalities have been ported to OPTEE in simulated IRQ mode, due to limitation in the secure OS for parallel IRQ handling (missing synchronization mechanisms in IRQ handler context) – no bottom-half processing.

2.12. COMM-IF (USB/TCPIP) (non-secure)

Currently the communication with the host application (IHS from Cardtek) is going through the TCPIP interface, but will also be supported through the USB-CDC port.

2.13. Filesystem (non-secure)

Implemented using the Linux POSIX Filesystem interface.

2.14. MSR (secure)

MSR driver has been ported to OPTEE, based on the UART

2.15. Tamper (secure)

Tamper features have been implemented in OPTEE by secure boot initialization and monitoring services. Please check the User Manual document for further details on the default pin setup behavior.

2.16. 24Hour Test (secure)

RTC driver for secure time keeping has been ported to OPTEE and an alarm service has been put in place to trigger an automatic system reset on a 24hour period. This is automatically updated upon date/time modification from the POS owner.

2.17. Secure Bootloader (secure)

A secure boot flow has been implemented following the principles of ARM chain of trust definition like:

For the first 4 images, the HAB secure keys are used for authentication, while for the Linux image a separate key is kept in OPTEE and this can be updated at image build time by the client.

3. Known issues

- [LINPOSR-195] – TEE-CORE: Failed to authenticate secure screen
  - Steps to reproduce the error:
    - Config
    - Set Date-Time
    - Payment
    - Enter amount --> after Enter is pressed the error message will be displayed on serial.
  - Workaround:
    - In order to remove the barely visible line that is painted by QT on the screen after entering a valid date and time in the "config/Set Date-Time" dialog, the line can be removed by once again entering the "config/Set Date-Time" dialog but once the "MM/DD/YYYY HH:MM:SS" text is displayed to press the "Cancel" key on the KeyPad.
    - This will remove the line and the next time the Payment is used the screens will be successfully authenticated.
- [LINPOSR-168] – CT tests failing for EMVCO L1 (1 test still failing 1709-x1)
- [LINPOSR-150] – Payment transaction with card that has PIN locked is approved
- [LINPOSR-172] – Payment transaction with expired card does not fail
- [LINPOSR-181] – Online contact transaction with Mastercard never go Online
- [LINPOSR-185] – Pin required for 4 times instead of 3.
  - Description:
    - For offline PIN validation, if the PIN is inserted incorrectly for three times, the payment-demo asks for the PIN for the fourth time, then displays the message "Approved" on the LCD, even if the PIN is wrong.

4. Release Contents

This table provides an overview of the LPOS software release package contents and locations.

Deliverable	Location
Payment demo application	/opt/payment-demo
Set IP for payment demo app	/bin/pos-set-ip.sh
Trusted Applications	/lib/optee_armtz/
Payment demo start/stop script	/etc/init.d/payment-demo
UI Module	/opt/ui2/bin/ui2

5. Revision History

Table 1. Revision history

Revision number	Date	Substantive changes
1	01/2018	Initial release
2	04/2018	Release version 3.0

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: LPOSRS003SRN
Rev. 2
04/2018