SOLUTION CARD READER TRAINING: THE PURPOSE AND VALUE OF A SOLUTION

DONNIE GARCIA
SOLUTIONS ARCHITECT
SECURE TRANSACTIONS

AMF-PMT-T2778 | AUGUST 2017

SECURE CONNECTIONS
FOR A SMARTER WORLD

AGENDA

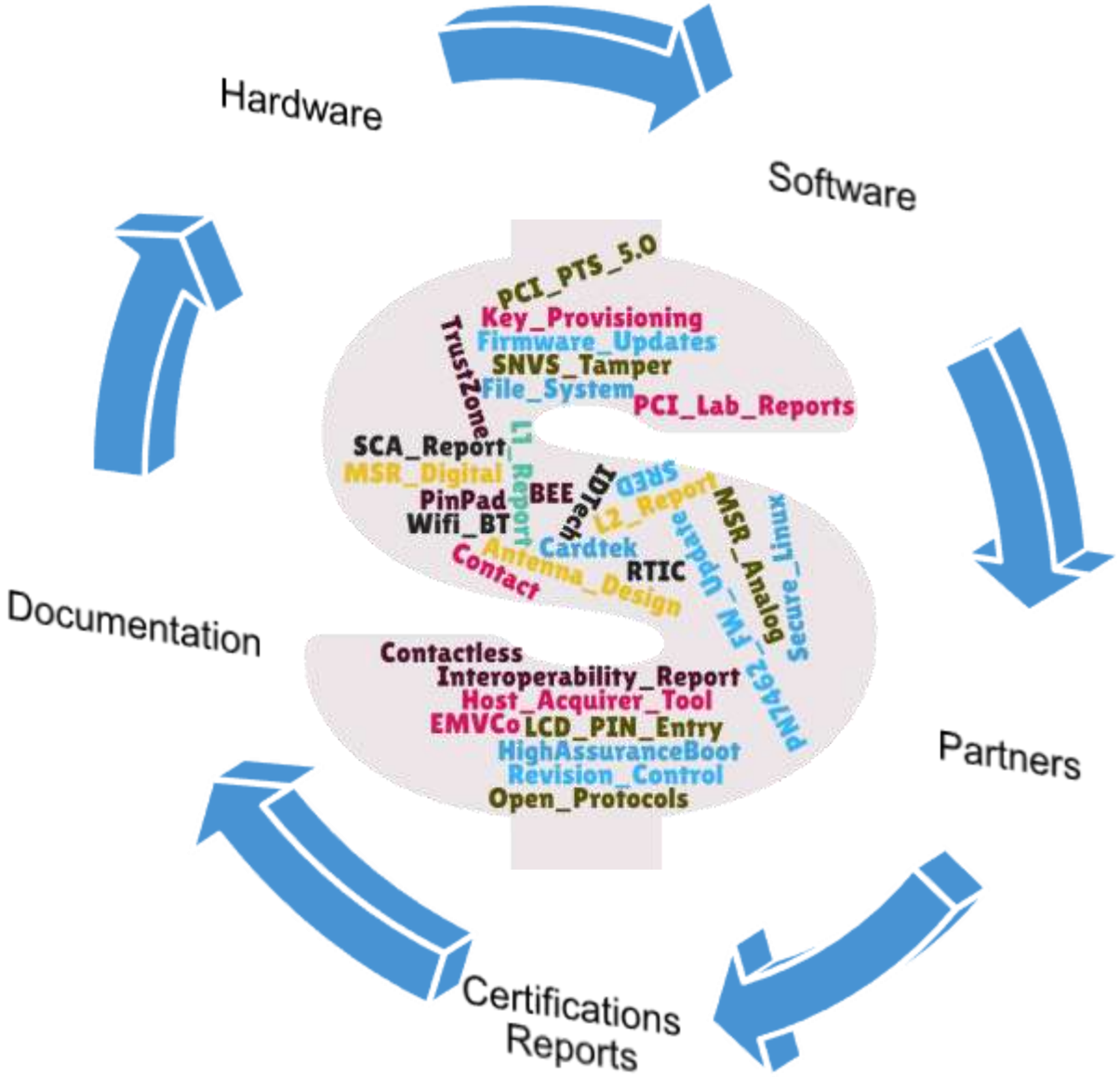
- Get to know the SLN-POS-RDR (35 minutes)
  - Details of the solution
    - Hardware
    - Software
    - Certifications
- Problems Addressed (20 minutes)
  - Security
  - Memory Expansion
  - User interface
  - Card Reading
- Hands-On with FRDM-K82F (Remaining time)
  - Secure boot
  - Execute in place, debugging and provisioning
  - Demonstration of Card Reader Functionality

01.

Get to know the SLN-POS-RDR

About a “Solution”

- **A Solution is a comprised of**
  - **The right hardware aligned to the target application**
  - **Modular software that can be repurposed for end devices**
  - **Partners where needed**
  - **Certification reports that can be leveraged by end designs**
  - **Documentation and support**



Point of Sales

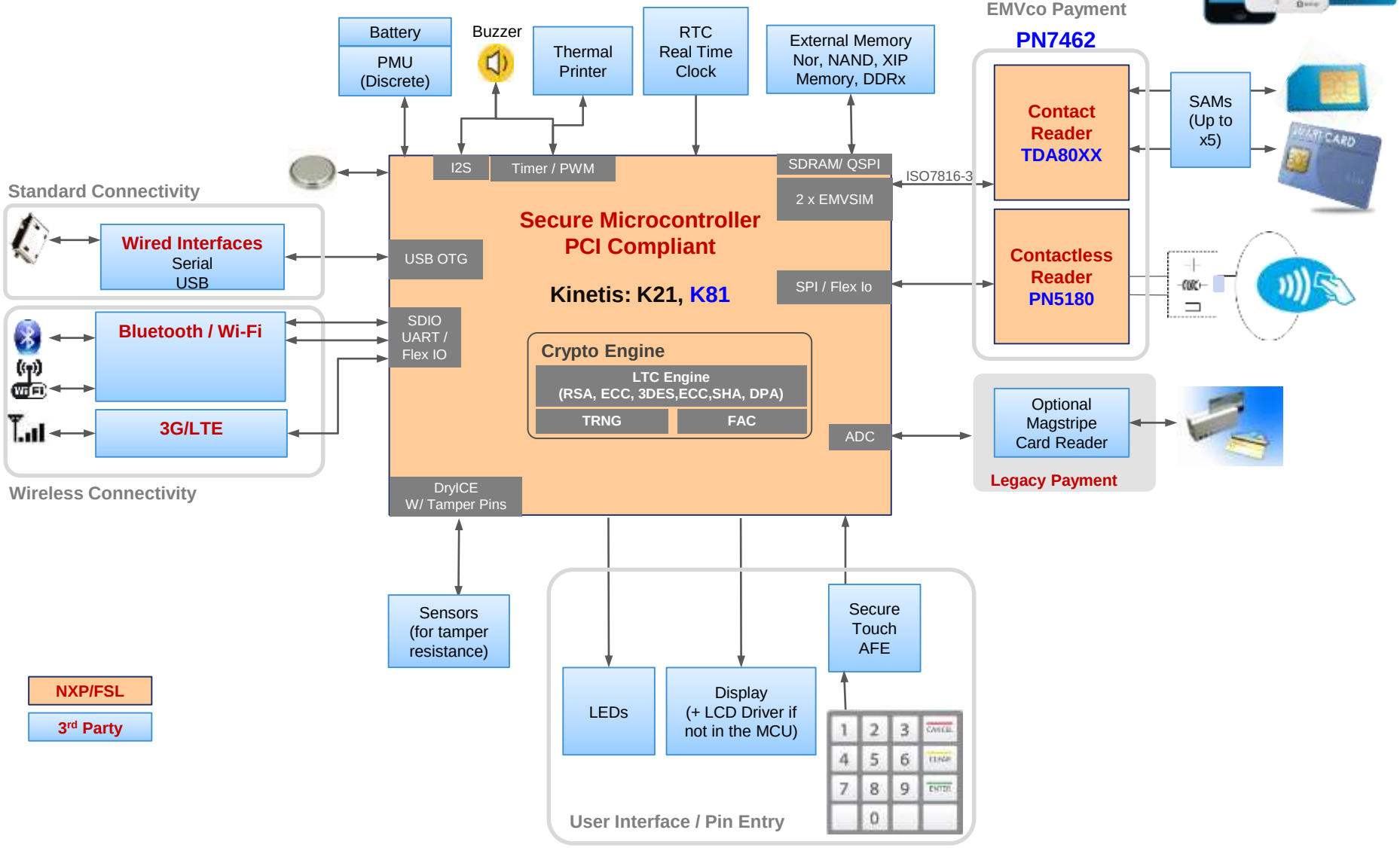
A scalable portfolio for reader interfaces and secure controllers/processors to address a wide range of POS solutions

	PinPad / mPOS	POS / Smart POS	Tablet / Counter Top POS	High End POS
				
CPU/MPU	**K21/K81/KL81**	**i.MX 6** UL-3 **i.MX7** Solo	**i.MX 7**Dual; **i.MX** 8Xseries **i.MX** 6DL/D/Q + K81/KL81	**i.MX6** DQ Plus; i.MX 8Xseries; 8series + K81/KL81/A70CM
CT reader **CL reader**	**TDA8034/TDA8035** **CLRC663/ PN5180 / PN7462**	**TDA8026/ TDA8034/TDA8035** **CLRC663/ PN5180 / PN7462**	**TDA8026/ TDA8034/TDA8035** **CLRC663/ PN5180 / PN7462**	

Power **E**fficient , **S**ecure & **C**onnected **S**olutions

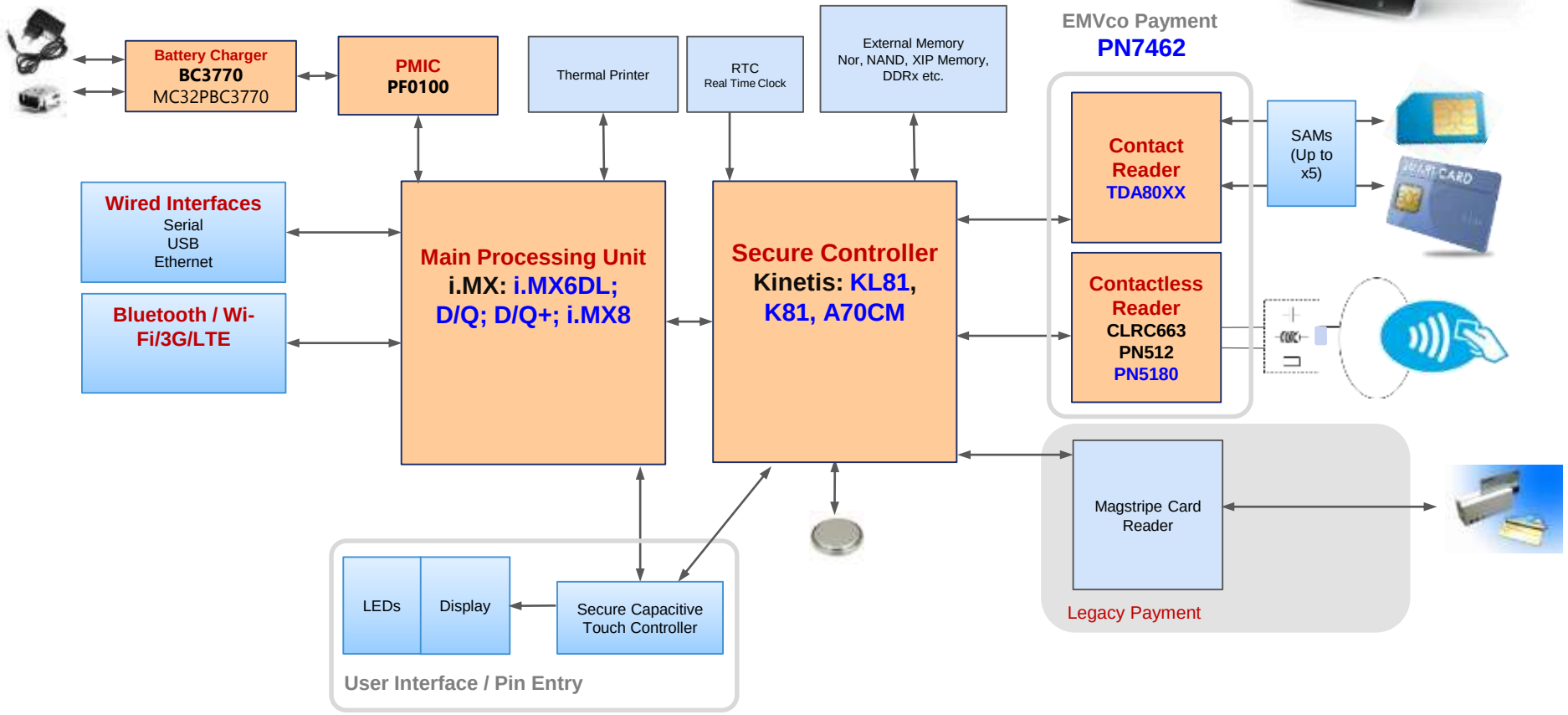
PinPad, mPOS

Architecture Block Diagram

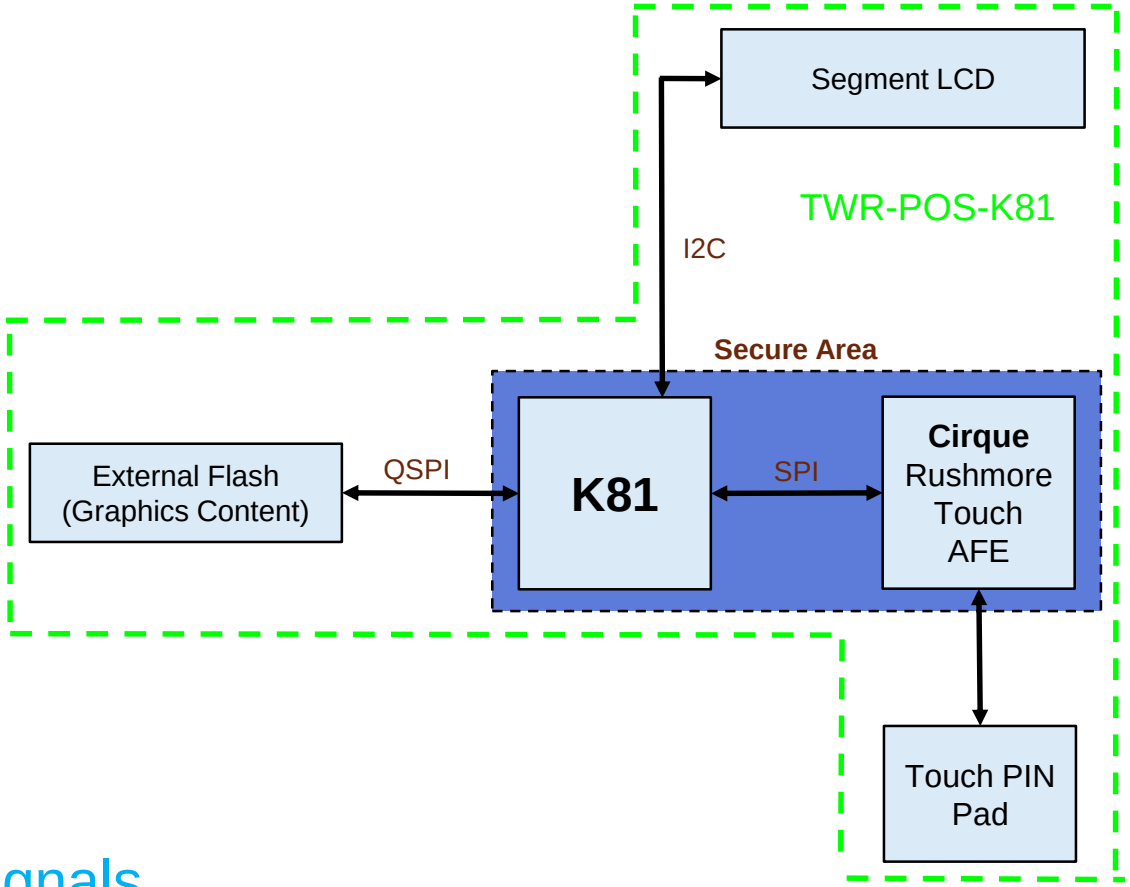


MPU/Android - Split Architecture Smart POS and Kiosk

Architecture Block Diagram



PIN Pad POS Solution



- K81 Secure Micro w/ Tamper and Crypto
- Secure Capacitive Touch (by Cirque) Pin Pad
- Tamper Header providing access to 8 tamper signals
- Chip on glass 2 lines x16 Character segment LCD
- 4 user controlled status LEDs
- Independent, battery-operated power supply for real-time clock (RTC) module
- Production Quality Software EMVCo L1
- Production Quality Documentation
- PCI 4.x Certified

Preliminary Certification report completed

New evaluation report of the NXP Semiconductor, Inc. TWR-POS-K81 against PCI PTS POI v4.1b requirements

31 October 2016

Security Evaluation of:	NXP Semiconductor, Inc. TWR-POS-K81
Reference Standard:	PCI PTS POI v4.1b (New)
Issue Date:	31 October 2016
Project:	16-3628-R-0102 v0.1

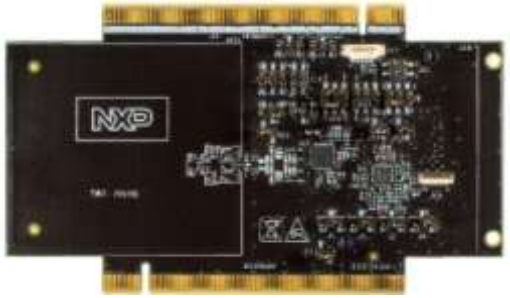
Executive Summary

UL Transaction Security was asked to study the TWR-POS-K81 and comment on its compliance with the PCI PTS POI v4.1b requirements. Under NDA, working units were provided for destructive analysis, along with wiring schematics and layouts, test data, loader application and firmware source code. We tested and evaluated the submitted samples of the device.

This report presents our findings for compliance to the PCI PTS POI v4.1b requirements, with detailed analysis of each requirement, overview of architecture and methods and cost estimates of possible attacks.

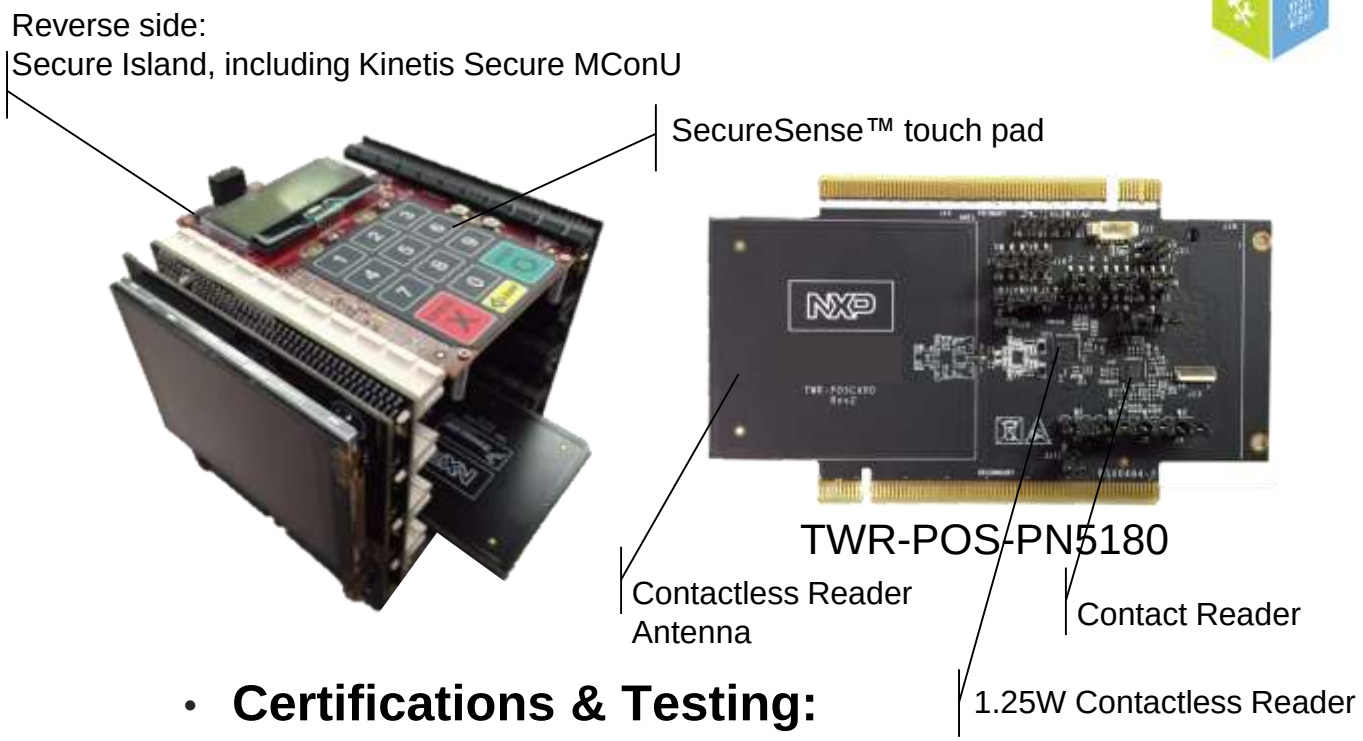
UL Transaction Security (California) concludes that the NXP Semiconductor, Inc. made TWR-POS-K81 device is compliant against PCI PTS POI v4.1b requirements.

Point of Sale (POS) Solution – SLN-POS-RDR



Point of Sale (POS) Reader Solution – SLN-POS-RDR

- POS Reader Reference Design for applications requiring Payment Card Industry certifications, supporting QVGA display
- NXP PN5180 Contactless, TDA8035 Contact card reader module with KSDK driver support
- Hardware and software, including all drivers, cryptographic libraries, NXP Secure Kinetis K81/KL81 MCUs - Pin to pin compatible, covering range of performance and price targets
- Chip-and-PIN keypad based on Cirque® SecureSense™ technology
- CardTek L2 CT/CL EMVCo Certifiable Stack
- **Target Applications:**
  - Point of Sales Terminals, Contact & Contactless
  - Automatic Teller Machine PIN Pad + Reader
  - Building and Home Automation, Secure Access Control

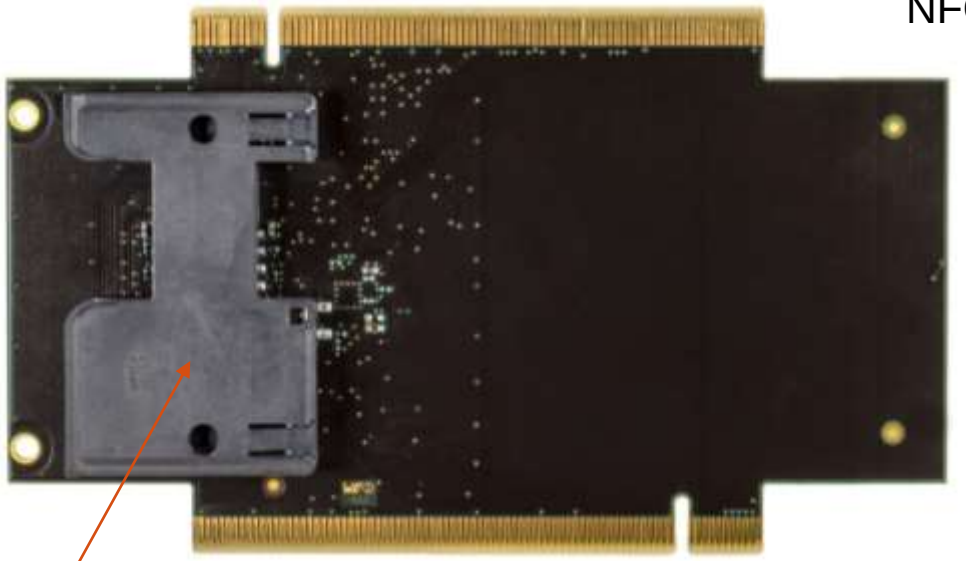


- **Certifications & Testing:**
  - TWR-POS-K81 PCI 4.1 Certified as PIN Pad *
  - PCI silicon pre-certification
  - Side channel attack testing *
  - CAVP (crypto assurance validation program) certified
  - TRNG entropy evaluation
  - EMVCo L1 CT/CL pre-certified

POS Reader Solution Features:

- Chip-and-PIN keypad based on Cirque® SecureSense™ technology
- EMVCo Level 1 CT/CL stacks by NXP
- EMVCo Level 2 CT/CL stacks by 3rd party
- EMVCo and PCI4.x Certification
  - EMVCo Pre-certification on Level 1 CT/CL by FIME
  - PCI 4.1 Pre-certification on the K81 performed by Infogard
  - PCI 4.1 PIN Entry Device (PED) Certification by Infogard (Pending)
- Kinetis K81 Secure MCU
  - Advanced physical tamper security
  - Advanced Public-key hardware w/ support for RSA and ECC
  - XIP from external Q-SPI flash w/ decrypt on the fly
- PN5180 contactless 13.56 MHz NFC front end IC
  - Dynamic Power Control for small antenna design
  - Full compliance with all NFC and EMVCo standards
- TDA8035 contact front end IC
  - 5V, 3V, 1.8V smart card supply, EMVCo compliant
  - Very low power consumption in Deep Shutdown mode
- Multiple Display Options
  - 2-line Character Segment
  - 3.2” QVGA TFT

TWR-POS-PN5180



Contact Card Slot

NFC Antenna

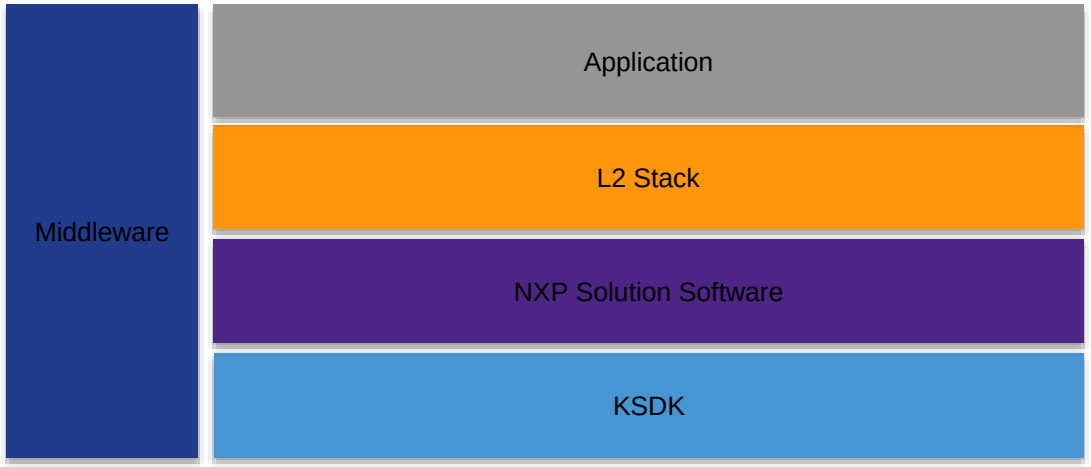
PN5180
1.25W Contactless Reader

TDA8035
Contact Reader

- Point of Sale Card Reader Board
  - PCB Antenna for contactless payment
    - ***NXP NFC: PN5180 NFC Front end***
    - ***Full EMVL1 2.5 compliant stack available in KSDK***
    - ***EMVCo L1 report from independent test house***
  - Smart Card reader PHY
    - ***NXP: TDA8035 Smart card interface***
    - ***EMVL1 4.3 compliant stack available in KSDK***
    - ***EMVCo L1 report from independent test house***

Software Layering Model

- Application layer on top contains the payment and EMV loopback application
- L2 Stack provides an API to enable upper layers implementing an EMVCo compliant payment application
- NXP Solution Software contains most of the POS-specific modules
- KSDK is the base that everything is built upon
- Middleware offer various functionality and system services



What software is provided?

- The SLN-POS-RDR software is built on top of the **K81 Kinetis SDK (KSDK)** package.
- Solution-specific software components (add-ons) fall into three categories:

Middleware:

- SPIFFS Filesystem
- eGUI
- NFC ReaderLib (CL)
- KSDK EMV L1 (CT)

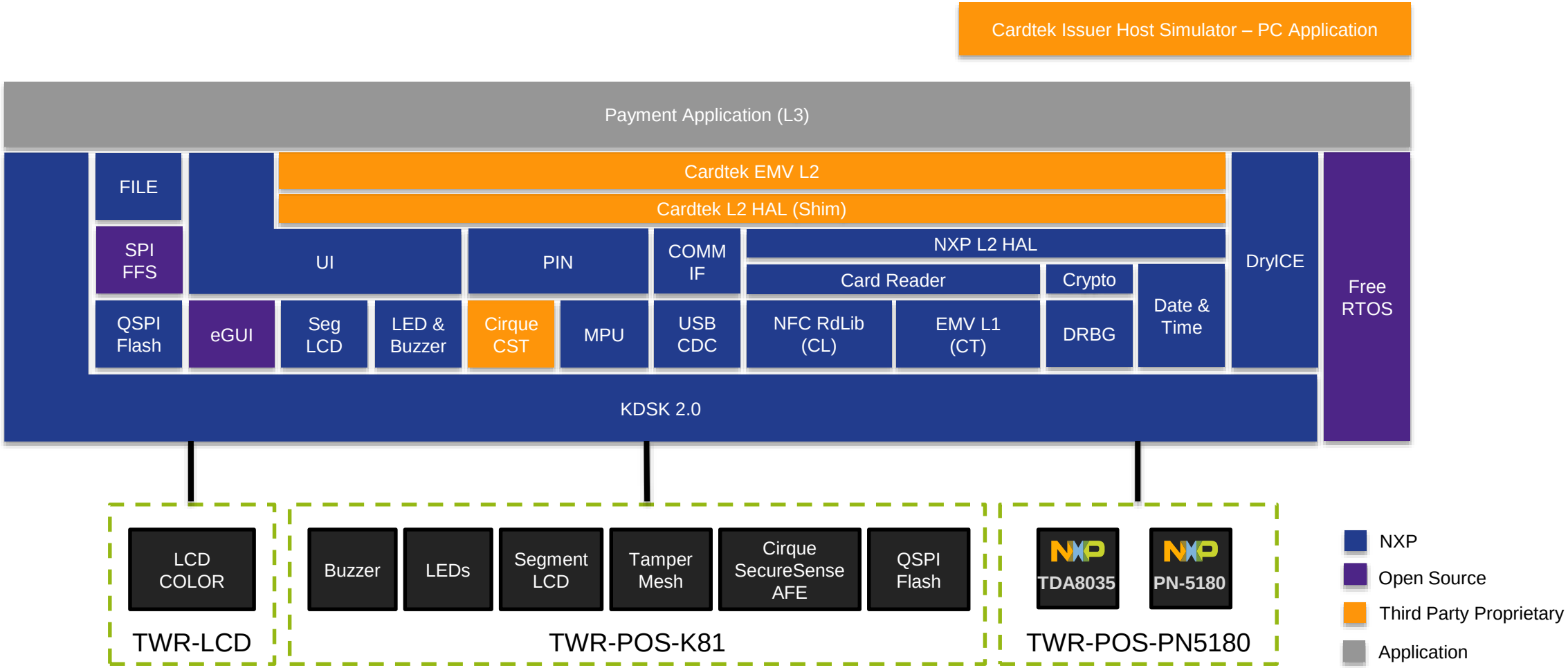
Third Party:

- Cardtek EMV L2
- Cirque Secure Touch

Point-of-Sale Add-Ons:

- L2 HAL (Card Reader, Date/Time)
- User Interface
- PIN
- Crypto
- Filesystem
- DryICE (Tamper)

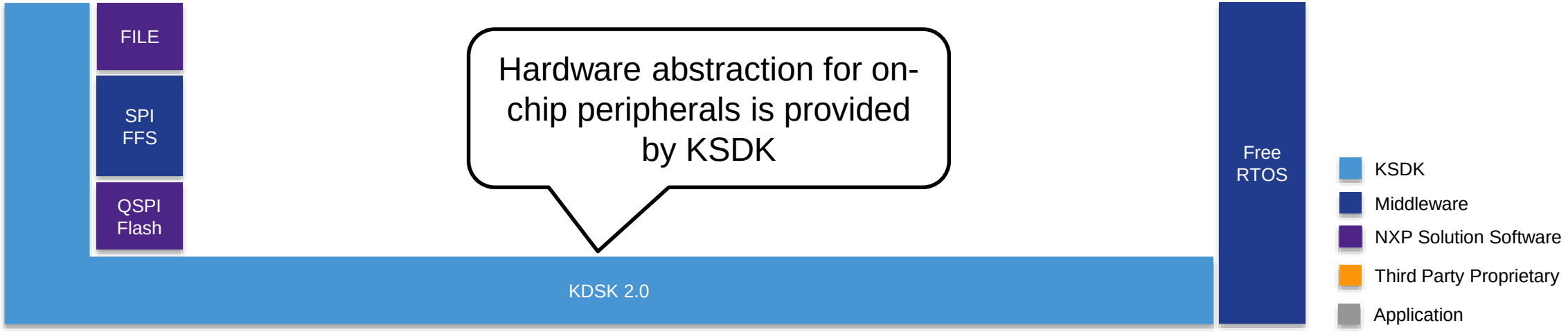
Point of Sale (POS) Reader Solution Block Diagram



Software Layering Model – System Layers

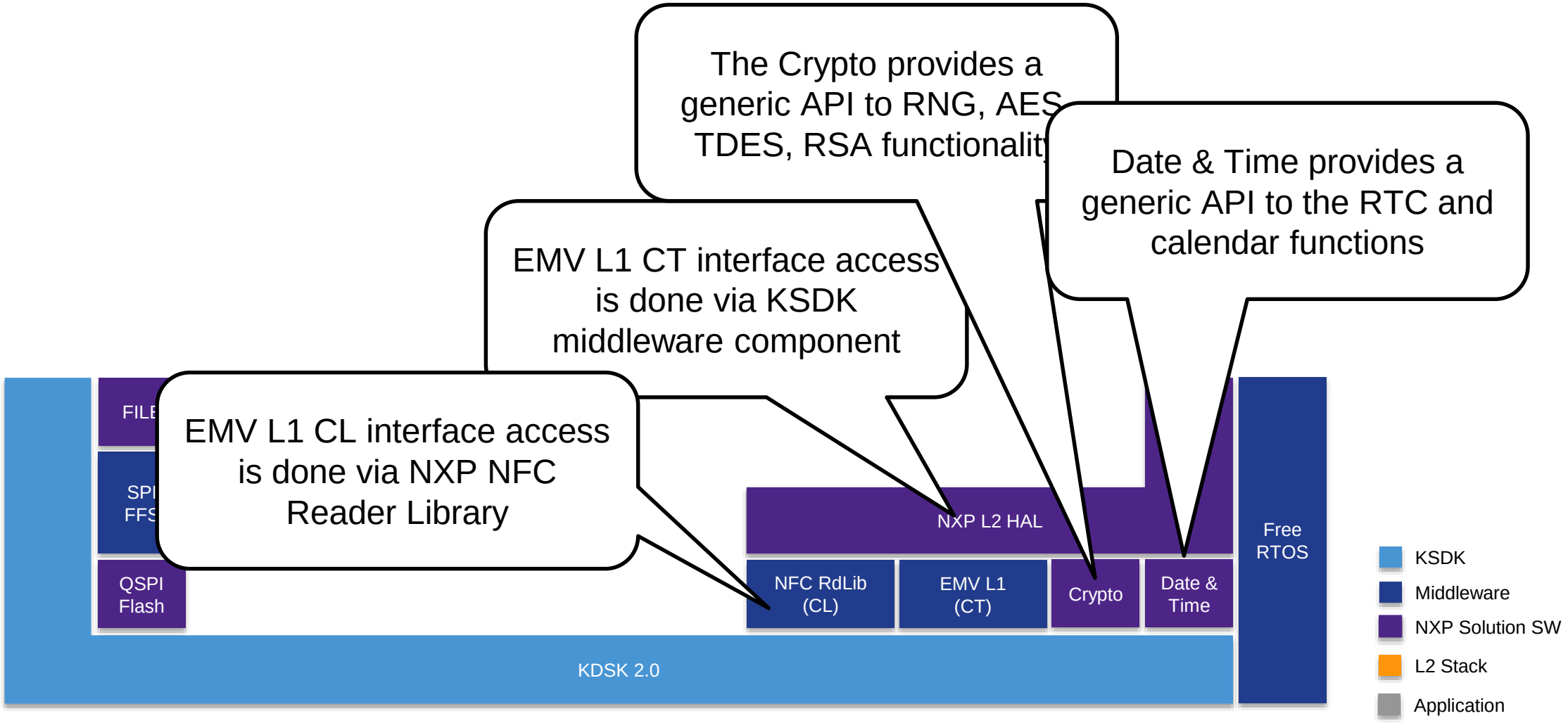
The File System is used to store configuration and runtime data in the external QSPI flash

Since there are multiple external interfaces, an RTOS is used to increase overall system robustness and enable the best user experience

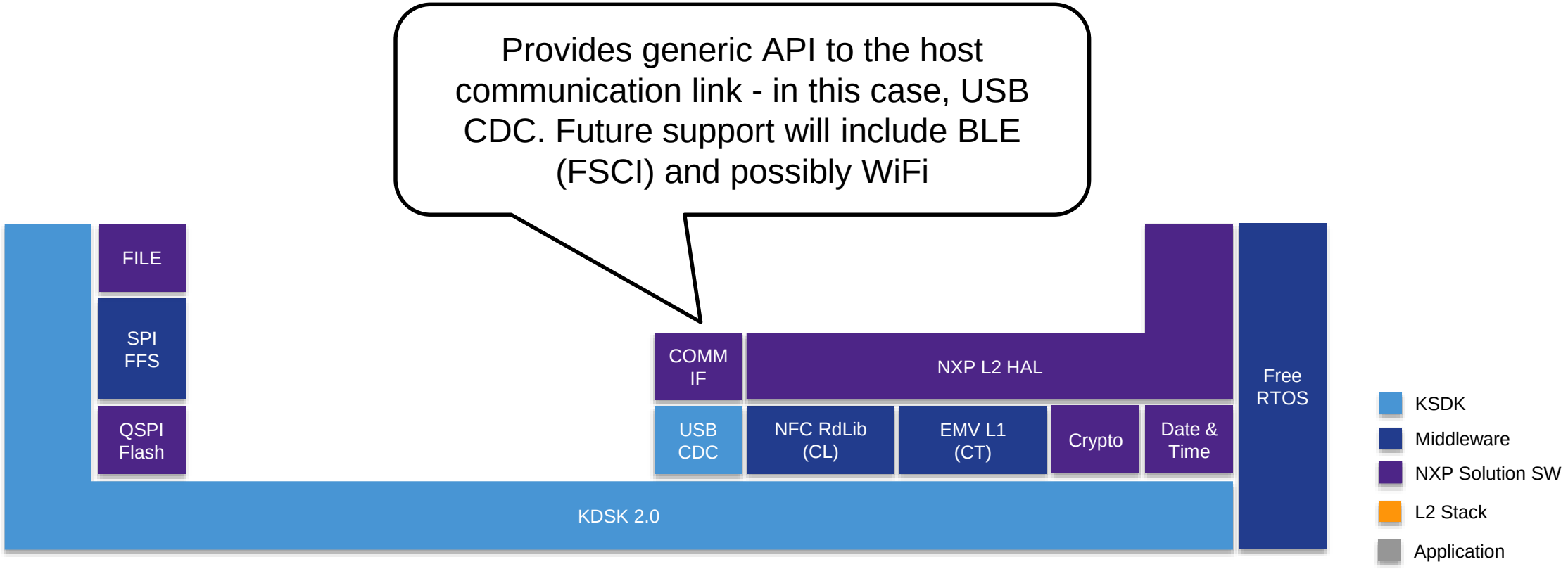


Hardware abstraction for on-chip peripherals is provided by KSDK

Software Layering Model – NXP L2 HAL



Software Layering Model – COMIF (Host Interface)

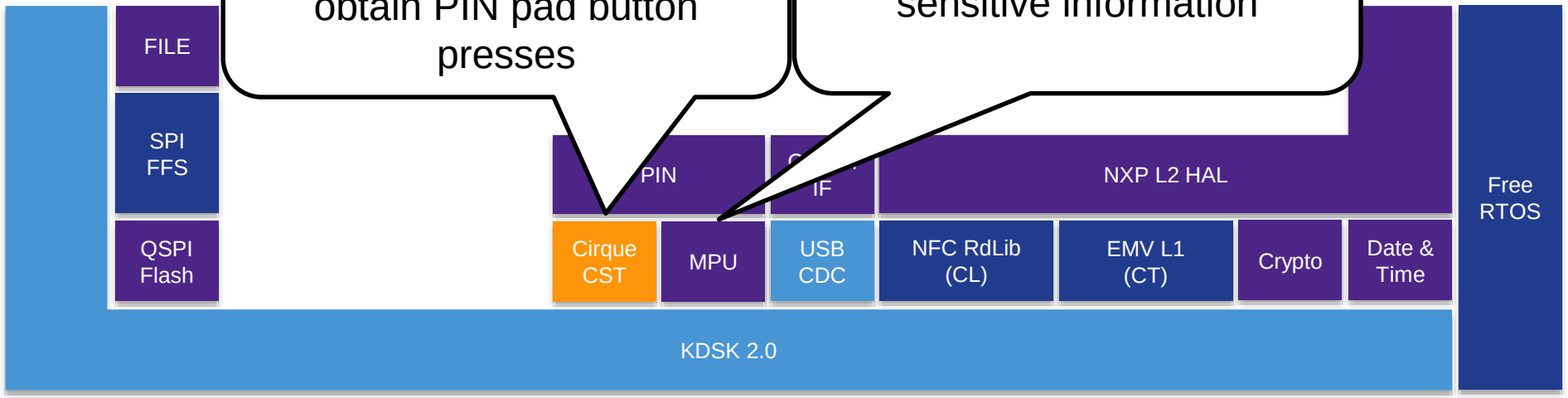


Software Layering Model – PIN Entry

Generic API to obtain PIN, button presses (navigation) and generate PIN blocks for online or offline authentication - PIN data is secured by the MPU

Third party library provided by our partner Cirque to obtain PIN pad button presses

MPU is used to protect sensitive information



- KSDK
- Middleware
- NXP Solution SW
- L2 Stack
- Application

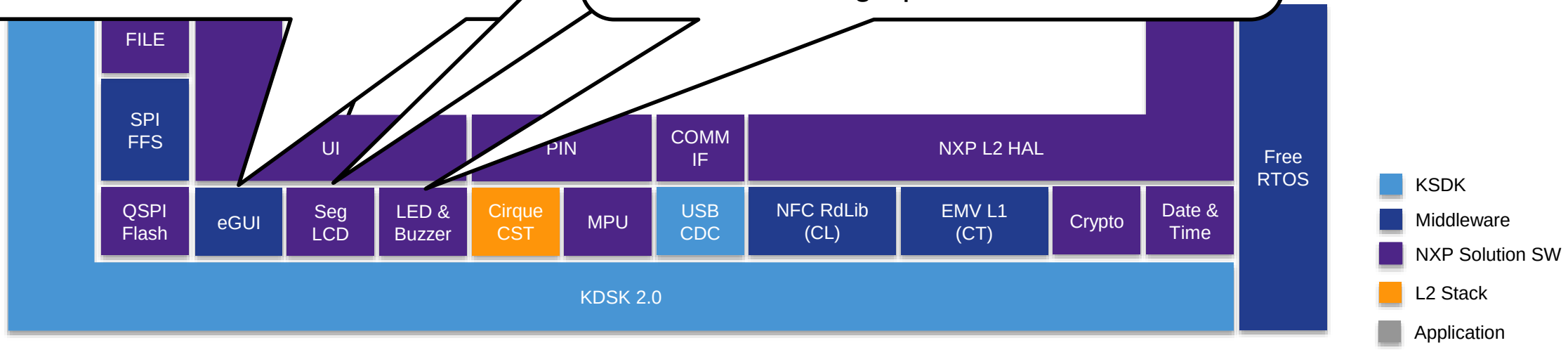
Software Layering Model – User Interface

Generic API providing access to all UI-related elements. In most applications, this would most likely be customized

The segment LCD is used to display PIN pad related messages

The graphical LCD (TWR-LCD) leverages the open source eGUI graphics package

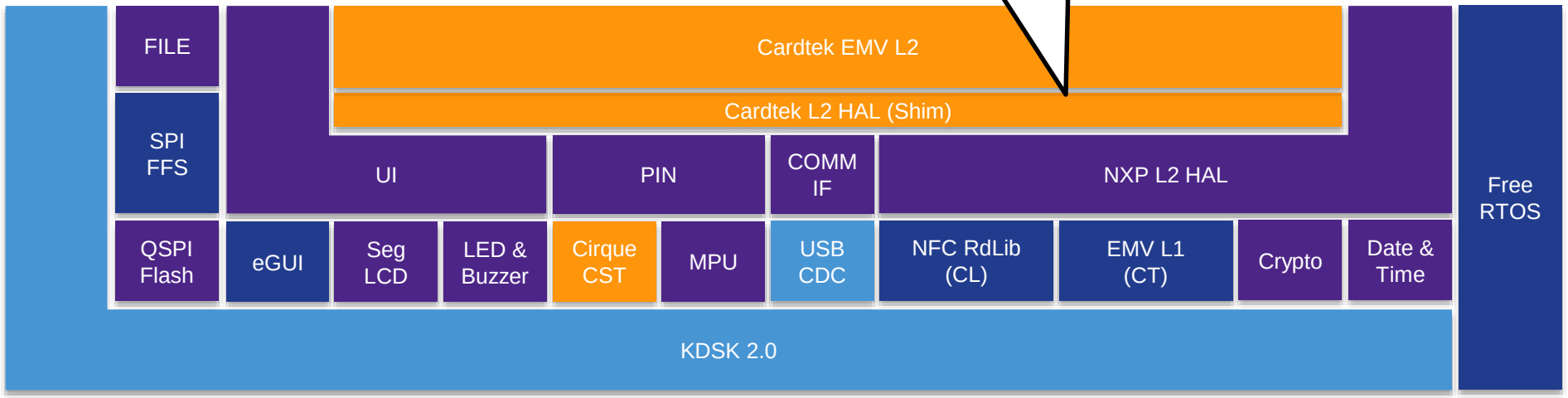
The LED and Buzzer module provides a simple way to enable/run cleanly in a RTOS environment. The LEDs are virtualized on the graphical LCD



Software Layering Model – L2 and L2 HAL Shim

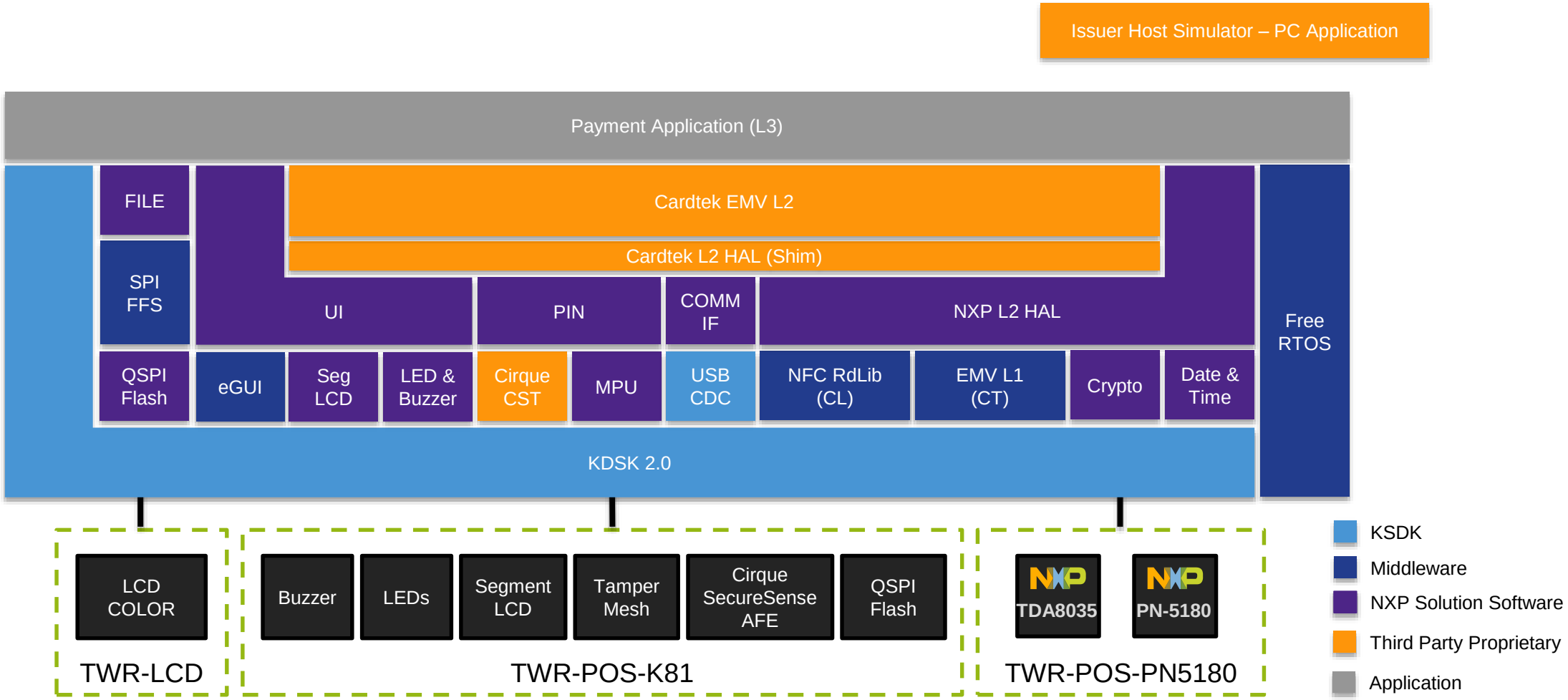
The L2 stack is provided by our partner Cardtek. It contains all L2 functionality including entry point, kernel and supports both CT (EMV 4.3) and CL (Visa) interfaces

The L2 HAL Shim is the “glue“ between the L2 stack and the rest of the system. This translates the L2 HAL API into calls to our Solution software



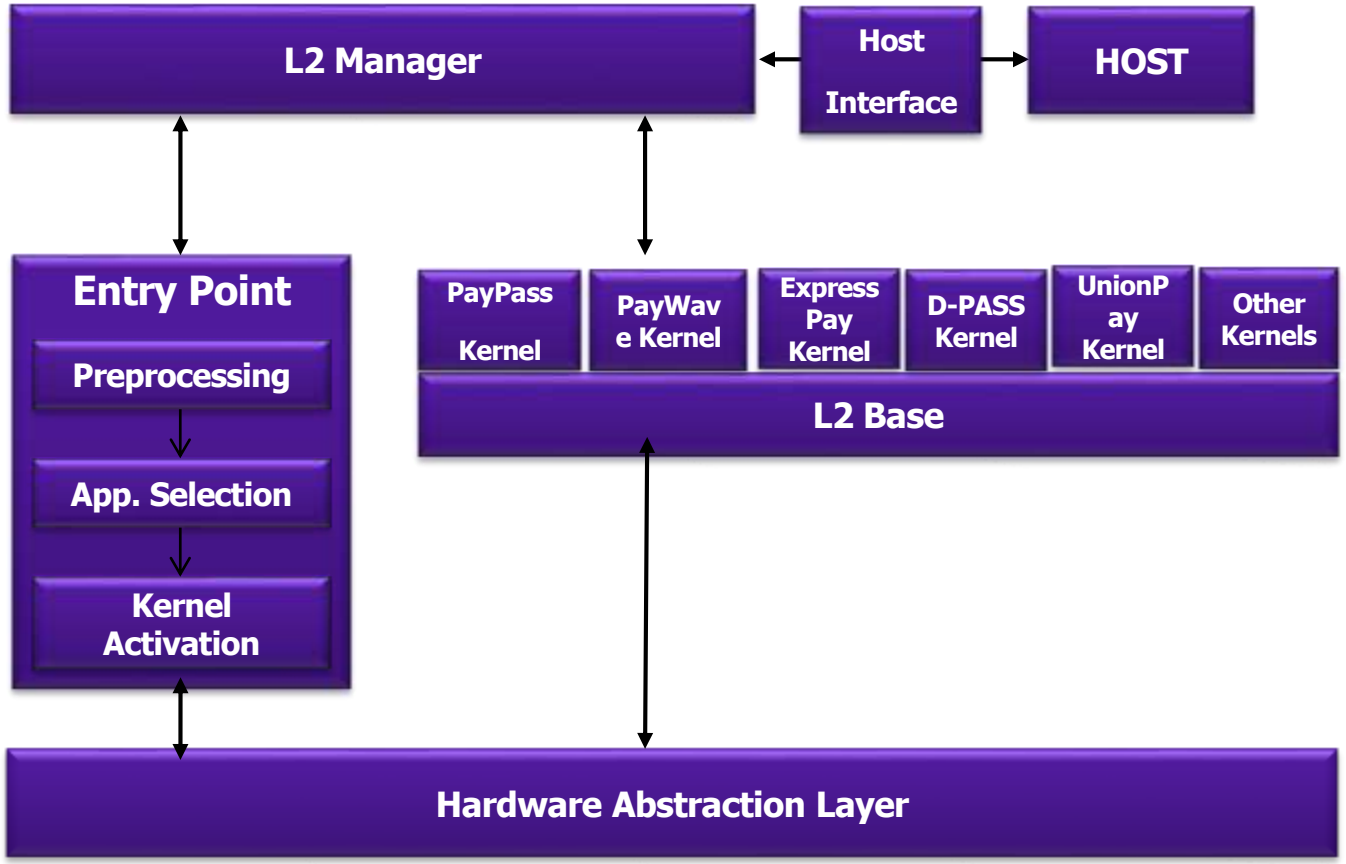
- KSDK
- Middleware
- NXP Solution SW
- L2 Stack
- Application

Software Layering (payment_demo)



Solution Modules

- **L2 Manager**
  - Provides interfaces to Payment application to get access to L2 kernel libraries. It is also a gateway to the Host.
- **Entry Point**
  - Process the configuration data, discovery and selection of a contactless application and activation of the appropriate kernel
- **Payment Schemes L2 Kernel Libraries**
  - Perform EMV related functions for different Payment schemes like MasterCard, Visa, …
- **L2 Base**
  - Shared libraries by different L2 Kernel payment scheme libraries.
- **Hardware Abstraction Layer**
  - File operations, memory operations, smartcard reader and polling.
  - Clients are able to make any change on HAL without having any impact on Kernel Libraries



Demo Applications

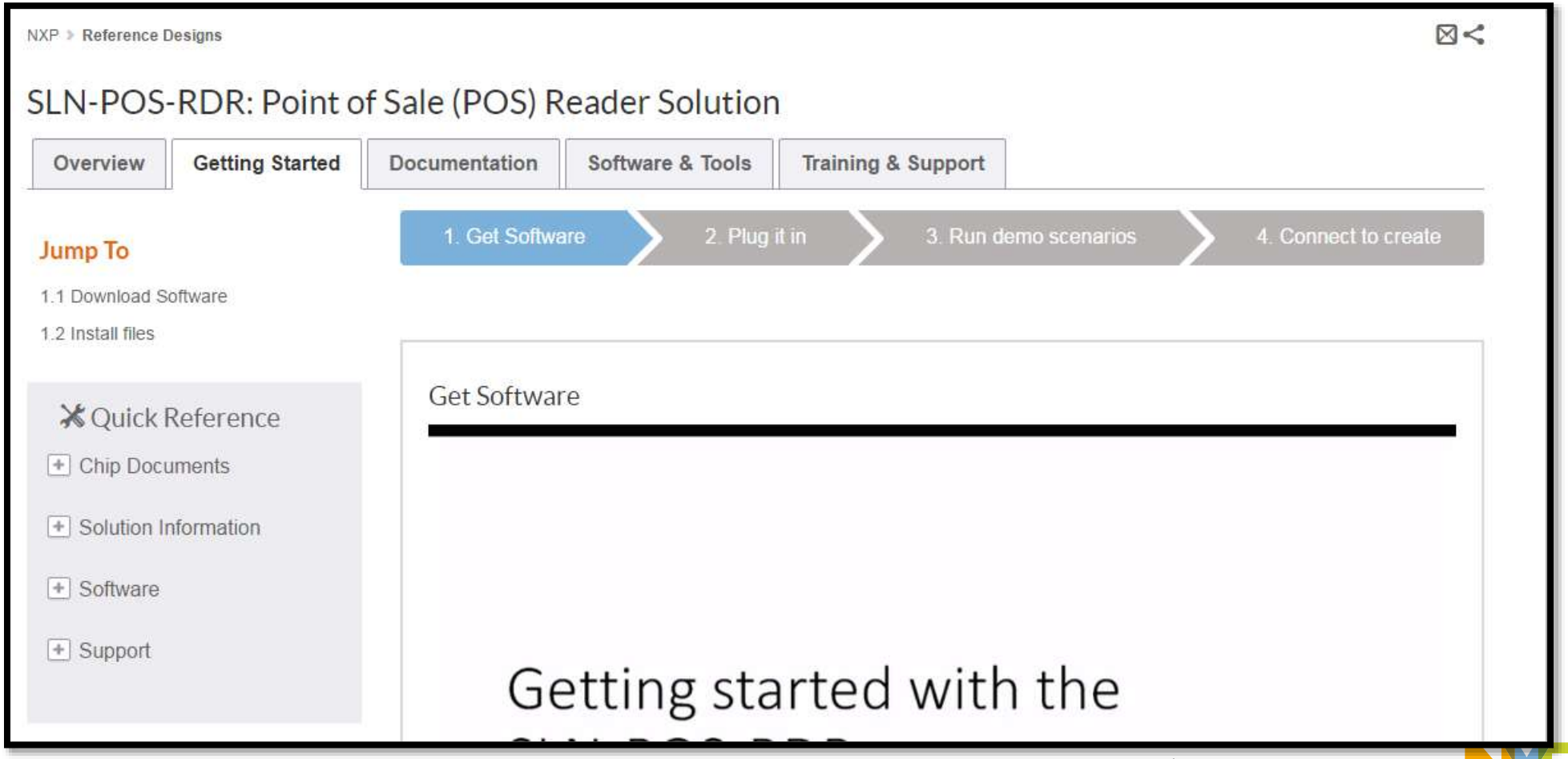
- **payment_demo:** Full payment demonstration application leveraging Cardtek's EMV L2 stack and a host simulator tool (IHS). The IHS tool can simulate online and offline transactions in addition to advanced features such as issuer scripting. All NXP Solution software modules are used in this application.

- **emv_loopback:** Provides a mechanism for customers to run CT and CL EMV L1 certification software. This demo also doubles as a reference for using the NXP Solution software modules without the Cardtek L2 and L2 HAL shim.

- **pn5180_firmware_update:**User interface and mechanisms for updating the firmware of the PN5180. Especially important for early access users of the TWR-POS-PN5180 because the **PN5180 has to be updated to support EMVCo 2.6**

Getting Started

- www.nxp.com/sln-pos-rdr/startnow



Plug it in.

1. Get Software | 2. Plug it in | 3. Run demo scenarios | 4. Connect to create

Jump To

- 2.1 Attach USB Cables
- 2.2 Install USB Driver for IHS tool

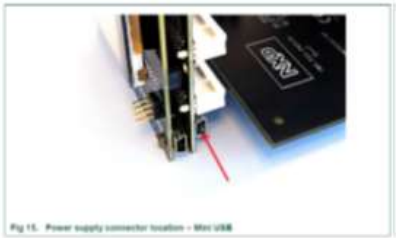
Quick Reference

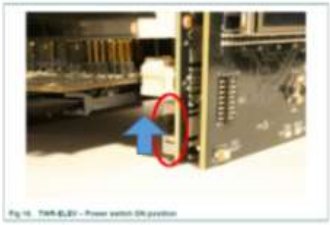
- Chip Documents
- Solution Information
- Software
- Support

2.1 Attach USB Cables

The SLN-POS-RDR requires **two** USB cables to be connected.

First connect the USB Mini cable to the TWR-ELEV as shown below. This USB connection is for power only and can be connected to a standard PC USB port or to a USB power adapter. After plugging this cable, turn on power by moving the TWR-ELEV switch to the UP position.





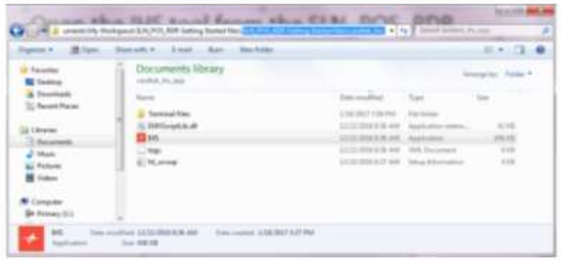
Second, Connect the USB Micro connector to the TWR-POS-K81 pin pad board as shown below. This USB connection is for communication so it must be connected to a PC that is running the IHS application. The next step will detail how to install the USB driver.

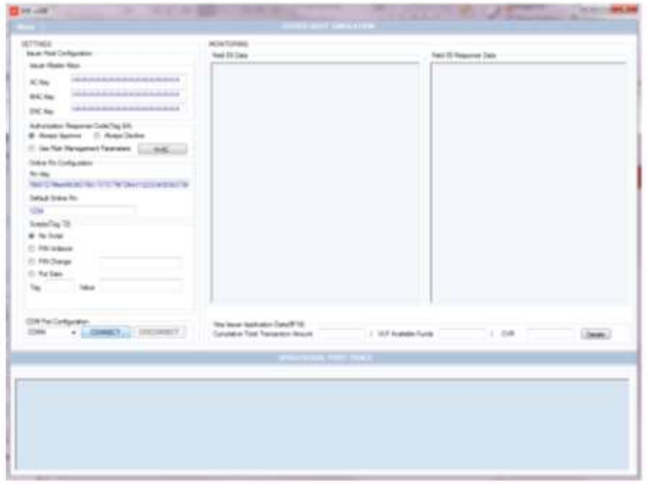
Run Demo Scenarios

1. Get Software | 2. Plug it in | 3. Run demo scenarios | 4. Connect to create

3.1 Open the IHS tool

Open the IHS tool from the SLN_POS_RDR Getting started files folder from SLN_POS_RDR Getting Started files\cardtek_ihs_app folder



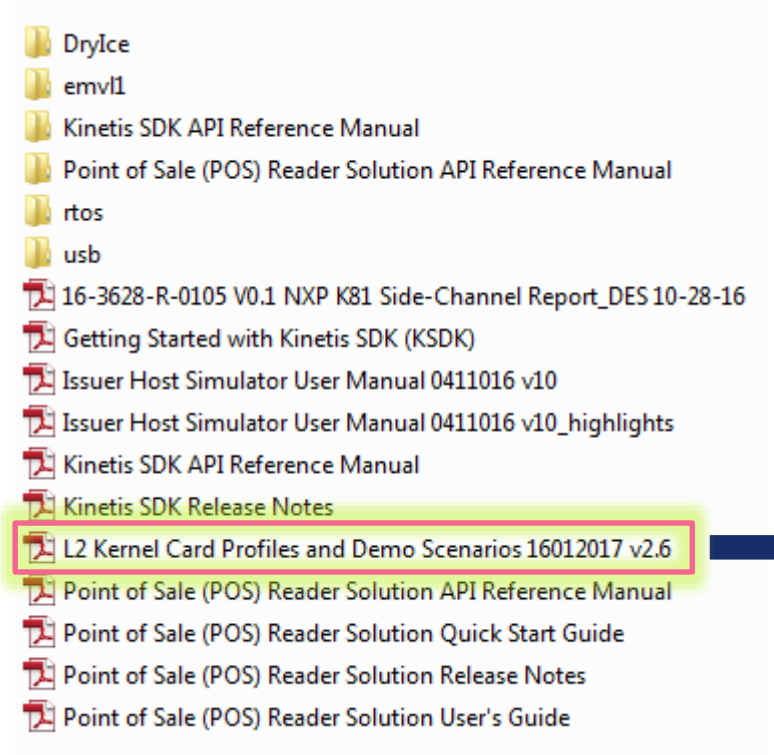


3.2 Perform Offline transaction

Perform Offline transaction for $29.99. Press Payment on the LCD screen

Cardtek documentation on Card Reader Scenarios

- K81POSCR_R_20170117\docs



Demo Scenarios done in Getting Started exercise

Other Scenarios to Highlight Functionality

Transaction with Pin Change Script

3.1.10 Transaction with Pin Change Script

3.1.10.1 1 st Transaction

- Pre-Conditions
  - Default Configuration
  - Enable "offline pin" option from board menu
  - Set "PIN Change" script option on IHS screen, and enter PIN as 1111
  - Set "Force Transaction to Online" option from board menu
- Transaction Steps
  - Insert Card
- Expected Result
  - After online processing Pin Change Script will be transmitted to the card

    (Please check Field 55 Response Data screen for the script message and please see script command on apdu trace screen)

Transaction with put data offline balance update

3.1.11.3 3 th Transaction

- Pre-Conditions
  - Default Configuration
  - Set "Put Data" script option on IHS screen
    - Set Tag value field as 9F54
    - Set Value field as 000000005000
  - Set "Force Transaction to Online" option from board menu
- Transaction Steps
  - Insert Card
- Expected Result
  - Please check Field 55 Response Data screen for the script message and please see script command on apdu trace screen

H-AC (Host Action Code) Decline when application expired

3.1.12 H-AC – Decline when Application Expired

- Pre-Conditions
  - Default Configuration
  - Update board date from board menu to any date bigger than 2025 and smaller than 2050.
  - Open H-AC screen from IHS application, then set "Decline if Expired Application" option from H-AC screen. Then Save it.
  - Set "Use Risc Management Parameters" option on IHS.
- Transaction Steps
  - Enter Amount
  - Insert Card
- Expected Result
  - Transaction will be declined online.

Registration Downloads

- Once registered the customer will have access to 2 software packages
  - Software and Collateral

Name	Date modified	Type	Size
boards	2/15/2017 8:56 AM	File folder	
CMSIS	2/15/2017 8:56 AM	File folder	
devices	2/15/2017 8:56 AM	File folder	
docs	2/15/2017 8:56 AM	File folder	
middleware	2/15/2017 8:56 AM	File folder	
pos	2/15/2017 8:56 AM	File folder	
rtos	2/15/2017 8:56 AM	File folder	
tools	2/15/2017 8:56 AM	File folder	
dryice_for_Kinetis_SDK_v2.0_readme	1/25/2017 3:13 PM	Text Document	4 KB
dryice_manifest	1/25/2017 3:13 PM	XML Document	14 KB
LA_OPT_Base_License	1/25/2017 3:12 PM	Chrome HTML Do...	146 KB
mbdetls_manifest	1/25/2017 3:13 PM	XML Document	314 KB
mbeTLS_for_Kinetis_SDK_v2.0_readme	1/25/2017 3:13 PM	Text Document	4 KB
point_of_sale_(POS)_reader_solution_readme	1/25/2017 3:13 PM	Text Document	1 KB
reportsCodeLabel	1/25/2017 3:13 PM	PNG image	51 KB
SW-Content-Register-KSDK_2.0.0_GA	1/25/2017 3:12 PM	Text Document	16 KB
SW-Content-Register-Point of Sale (POS) Reader Solution	1/25/2017 3:14 PM	Text Document	5 KB
TWR-K81F150M_manifest	1/25/2017 3:12 PM	XML Document	1,442 KB

TWR-POS-K81	2/17/2017 8:12 AM	File folder	
TWR-POS-PN5180	2/17/2017 8:12 AM	File folder	
TWR-SHIELD	2/17/2017 8:12 AM	File folder	

Supporting Documents	2/17/2017 8:12 AM	File folder	
16-3628-R-0102 V0.2 NXP TWR-POS-K81 PTS Report	11/18/2016 9:25 AM	Adobe Acrobat D...	7,539 KB

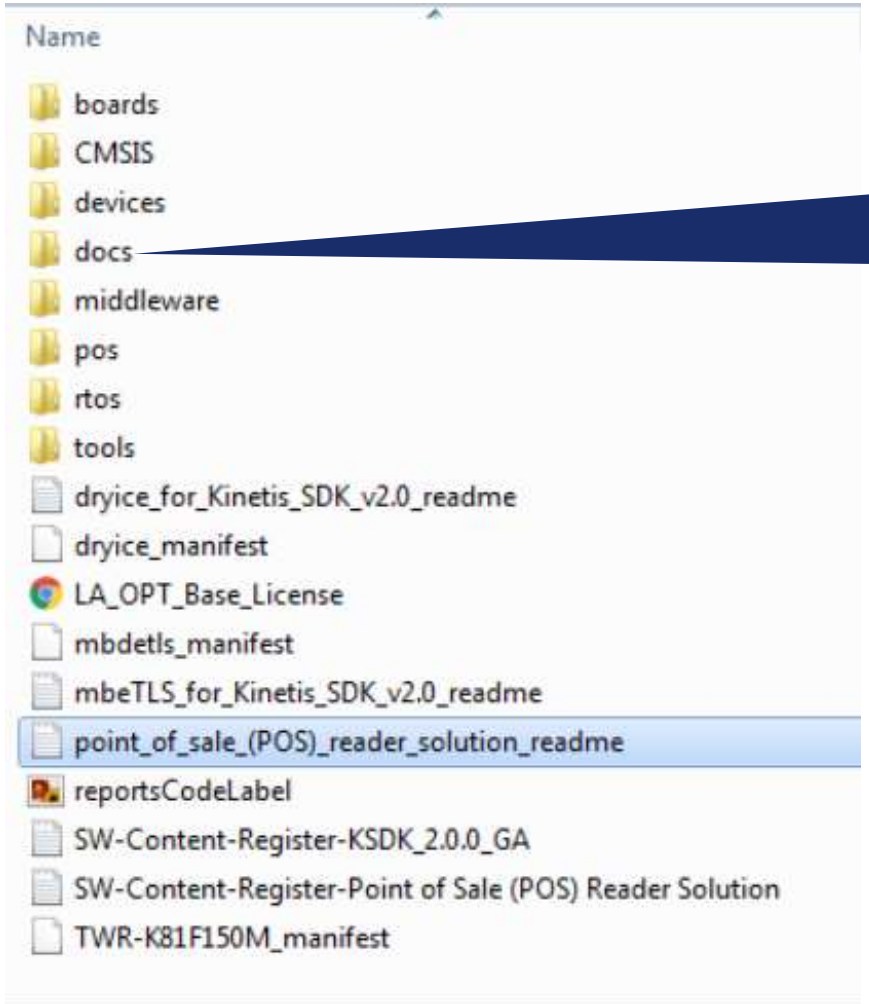
SLN-POS-RDR Software Package

Name	Date modified	Type	Size
boards	2/15/2017 8:56 AM	File folder	
CMSIS	2/15/2017 8:56 AM	File folder	
devices	2/15/2017 8:56 AM	File folder	
docs	2/15/2017 8:56 AM	File folder	
middleware	2/15/2017 8:56 AM	File folder	
pos	2/15/2017 8:56 AM	File folder	
rtos	2/15/2017 8:56 AM	File folder	
tools	2/15/2017 8:56 AM	File folder	
dryice_for_Kinetis_SDK_v2.0_readme	1/25/2017 3:13 PM	Text Document	4 KB
dryice_manifest	1/25/2017 3:13 PM	XML Document	14 KB
LA_OPT_Base_License	1/25/2017 3:12 PM	Chrome HTML Do...	146 KB
mbdetls_manifest	1/25/2017 3:13 PM	XML Document	314 KB
mbeTLS_for_Kinetis_SDK_v2.0_readme	1/25/2017 3:13 PM	Text Document	4 KB
point_of_sale_(POS)_reader_solution_readme	1/25/2017 3:13 PM	Text Document	1 KB
reportsCodeLabel	1/25/2017 3:13 PM	PNG image	51 KB
SW-Content-Register-KSDK_2.0.0_GA	1/25/2017 3:12 PM	Text Document	16 KB
SW-Content-Register-Point of Sale (POS) Reader Solution	1/25/2017 3:14 PM	Text Document	5 KB
TWR-K81F150M_manifest	1/25/2017 3:12 PM	XML Document	1,442 KB

- The software package is a KSDK 2.x package
- The POS related modules are added to this package
- KSDK add ons (mbed TLS, WolfSSL) can be added to this package
  - Mbed TLS is already there

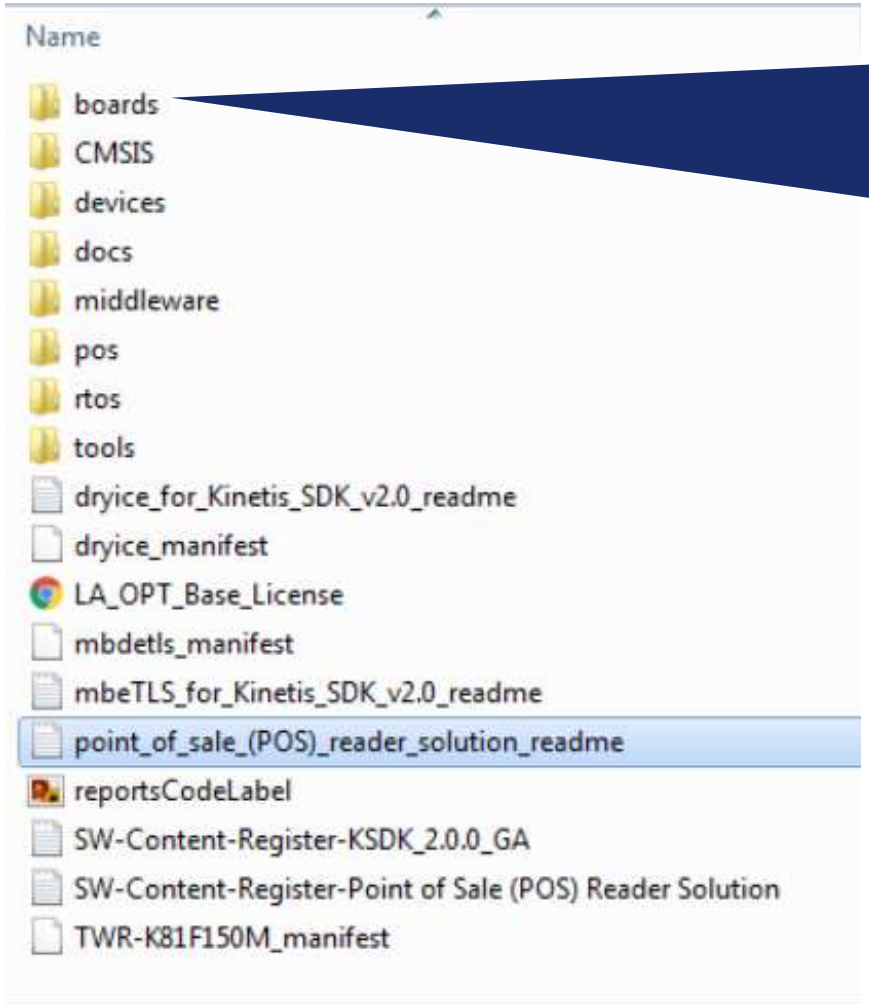
37

SLN-POS-RDR Software Package



docs -Most important folder is the docs folder. All documentation is posted here. Must read the release notes at a minimum for overview of release.

SLN-POS-RDR Software Package



Boards – Two (2) boards and 2 tool chains are supported. The TWR-POS-K81 – this is the pin pad board and the TWR-K81 (this is if a customer took the TWR-K80 board and placed a K81 IC). There are demo apps and driver examples for TWR-K81

TWR-K81 demo examples work for the TWR-POS-K81 board. Must change debugger from CMSIS-DAP to Jlink.

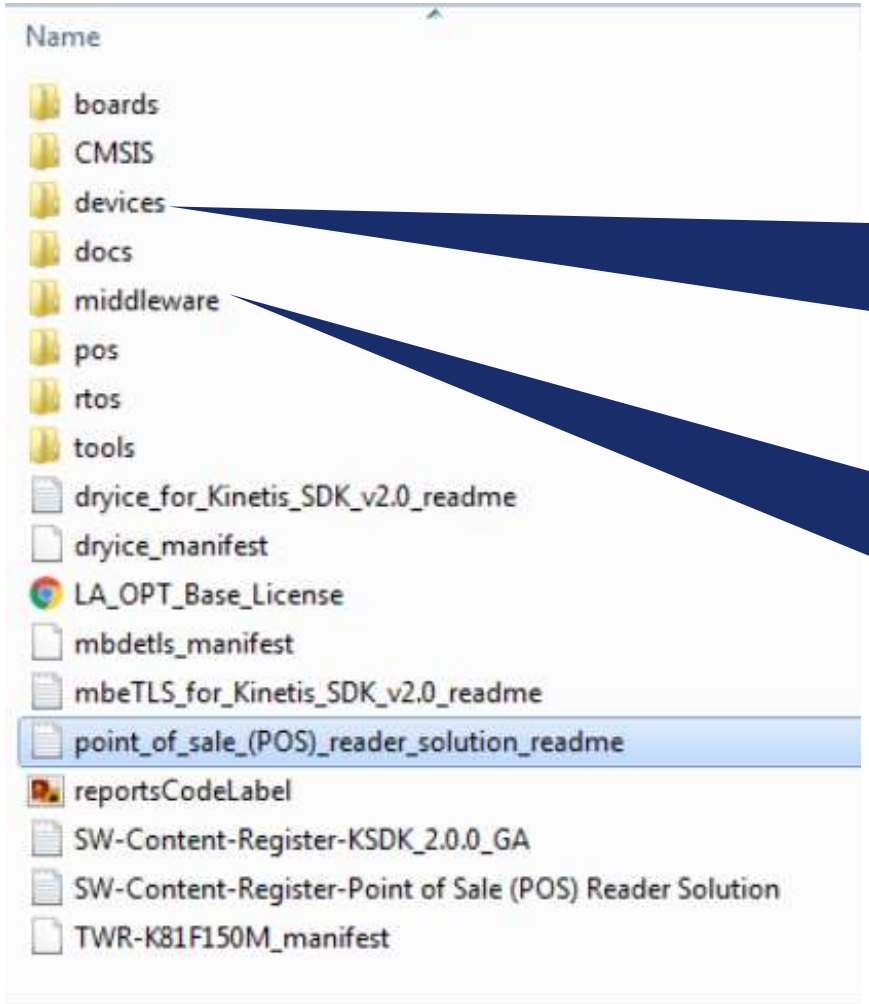
Tool Chains: KDS & IAR

- **Kinetis Design Studio:** Eclipse based Integrated development environment provided by NXP for users of Kinetis (KDS) and Kinetis and LPC (MCUXpresso)

- **IAR EWARM:** IAR product for ARM targets, fairly common among our customer. 30 Day trials are available, and limited code/function versions. Must pay for license.

40

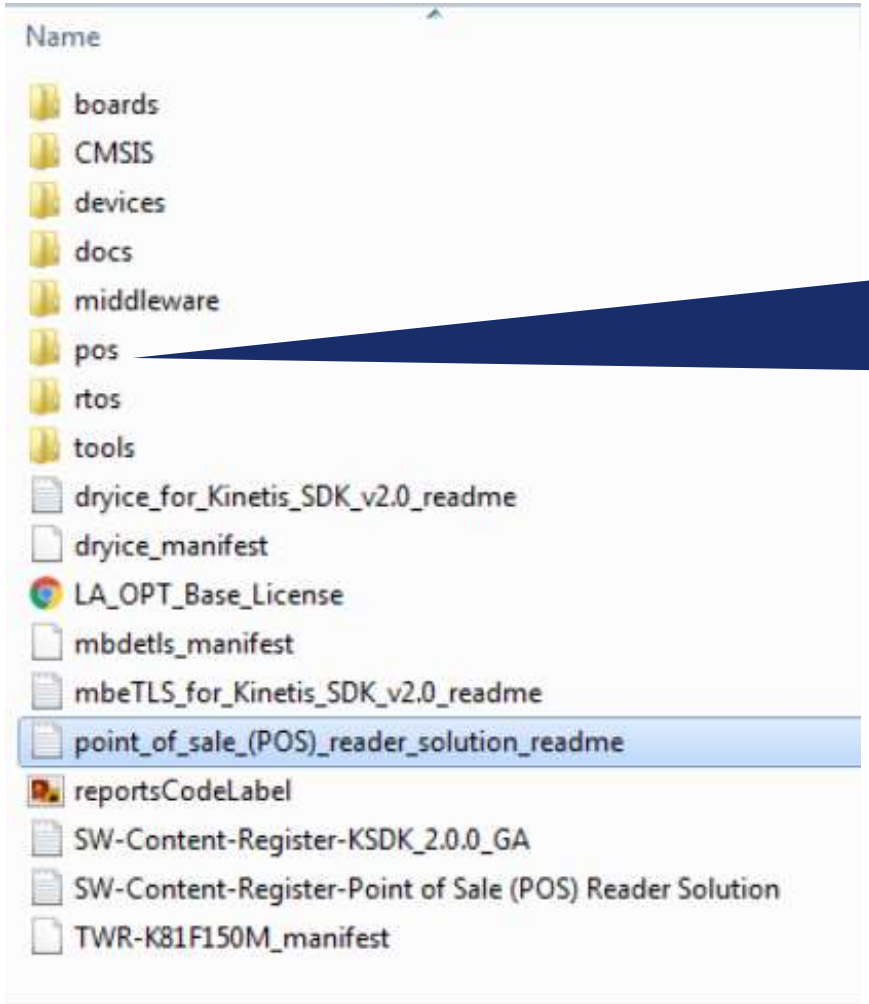
SLN-POS-RDR Software Package



Devices – Here is the device level support files for the target MCU (MK81)
If there is a peripheral driver that the customer wants to add, it can be found in this folder.

Middleware – Generic MCU SDK middleware (not related to POS)
The SPIFFS (File system) 3rd party software is here

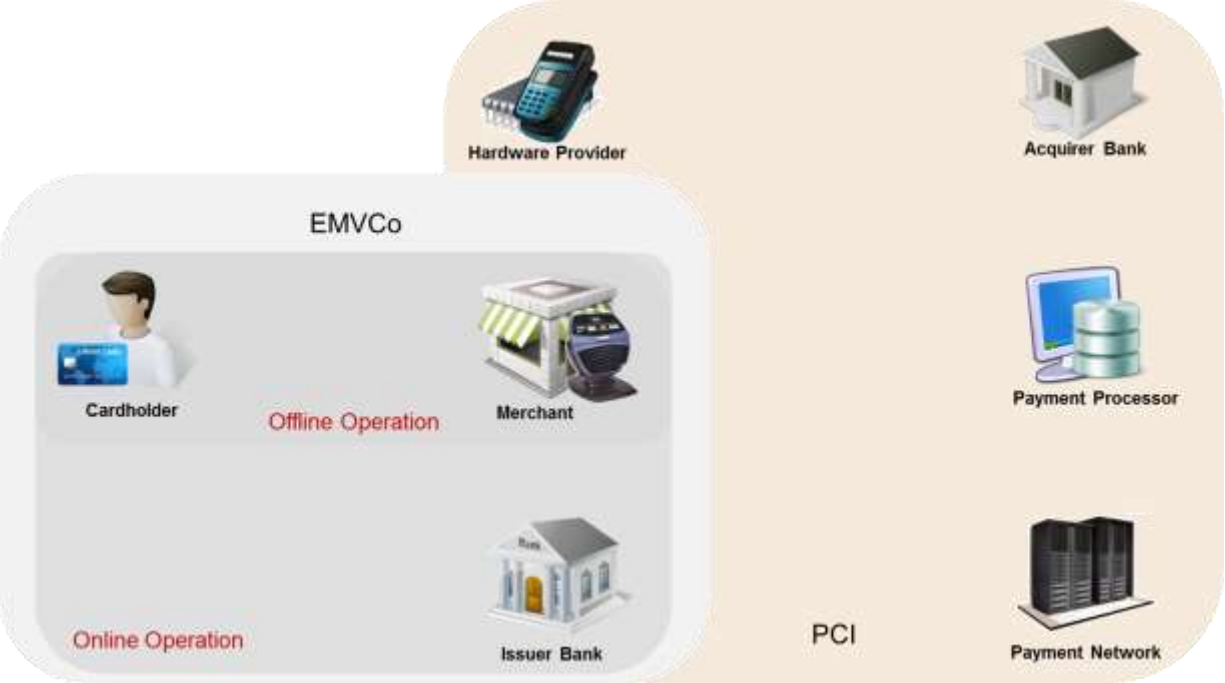
SLN-POS-RDR Software Package



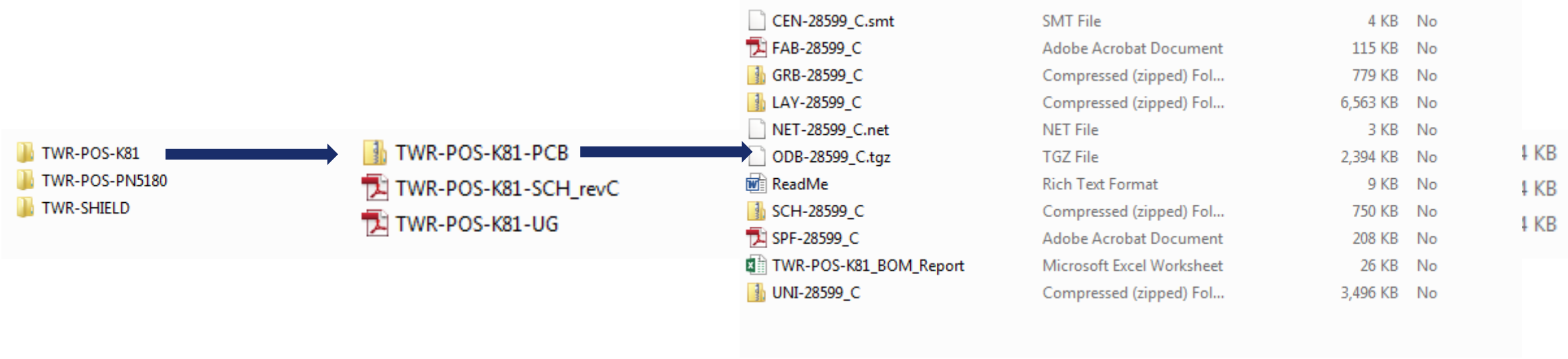
pos – Here are placed the specific software modules for Point of sale solution. This includes the NXP EMV L2 HAL, File system implementation, tamper, quadspi driver and others.

Additional Collateral

- PCI Certification collateral
- EMVCo L1 & L2 testing reports for Contact and Contactless interfaces
- ICS Forms for EMVCo submission
- Application notes for antenna design



SLN-POS-RDR Hardware Files



- Schematics and BOM information
- PCB design files for the TWR-POS-K81, TWR-POS-PN5180

SLN-POS-RDR PCI PTS Collateral

Supporting Documents	2/17/2017 8:12 AM	File folder	
16-3628-R-0102 V0.2 NXP TWR-POS-K81 PTS Report	11/18/2016 9:25 AM	Adobe Acrobat D...	7,539 KB

New evaluation report of the NXP Semiconductor, Inc. TWR-POS-K81 against PCI PTS POI v4.1b requirements

31 October 2016

Security Evaluation of:	NXP Semiconductor, Inc. TWR-POS-K81
Reference Standard:	PCI PTS POI v4.1b (New)
Issue Date:	31 October 2016
Project:	16-3628-R-0102 v0.1

Executive Summary

UL Transaction Security was asked to study the TWR-POS-K81 and comment on its compliance with the PCI PTS POI v4.1b requirements. Under NDA, working units were provided for destructive analysis, along with wiring schematics and layouts, test data, loader application and firmware source code. We tested and evaluated the submitted samples of the device.

This report presents our findings for compliance to the PCI PTS POI v4.1b requirements, with detailed analysis of each requirement, overview of architecture and methods and cost estimates of possible attacks.

UL Transaction Security (California) concludes that the NXP Semiconductor, Inc. made TWR-POS-K81 device is compliant against PCI PTS POI v4.1b requirements.

45

SLN-POS-RDR PCI PTS Collateral (Supporting Documents)

- board files
- Configuration_Management_Plan-PSDK
- Manufacturing of K81 Pin Pad
- TWR-POS-K81_management_guidelines
- TWR-POS-K81_PCI_PTS_POI_SRs_v4-1c-November_form
- TWR-POS-K81_POI_Modular_Evaluation_Vendor_Questionnaire

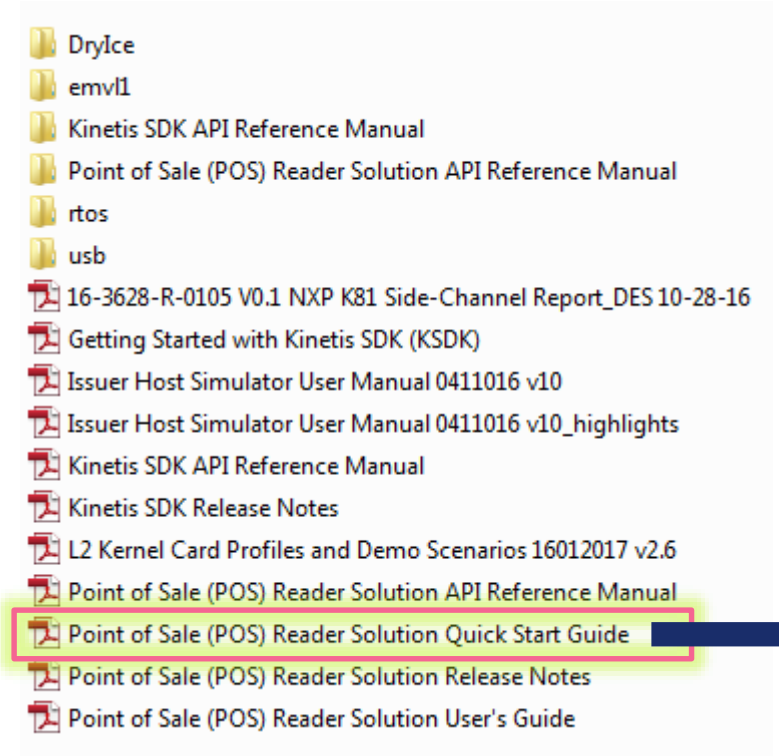
Board files includes tamper enclosure design

PCI PTS labs must certify that the firmware is protected – the manufacturing of the K81 Pin Pad details how this was done for our PCI design

All vendors must fill a questionnaire and SRs form to identify the functionality of the target of evaluation

Details provided in Quick Start document

- K81POSCR_R_20170117\docs



UM11036

Point of Sales (POS) Reader Solution - Quick Start Guide

Rev. 1.1 — 16 November 2016 User manual
406511 COMPANY PUBLIC

Getting Ready to develop with the SLN-POS-RDR

- Must have resources
  - IAR or KDS (MCUXpresso) IDE
  - Segger Jlink tool
    - Updated Segger Jlink drivers

- Recommended Resources
  - TWR-SER board for debug prints
  - If your PC does not have a Serial Port then a USB to Serial tool is needed

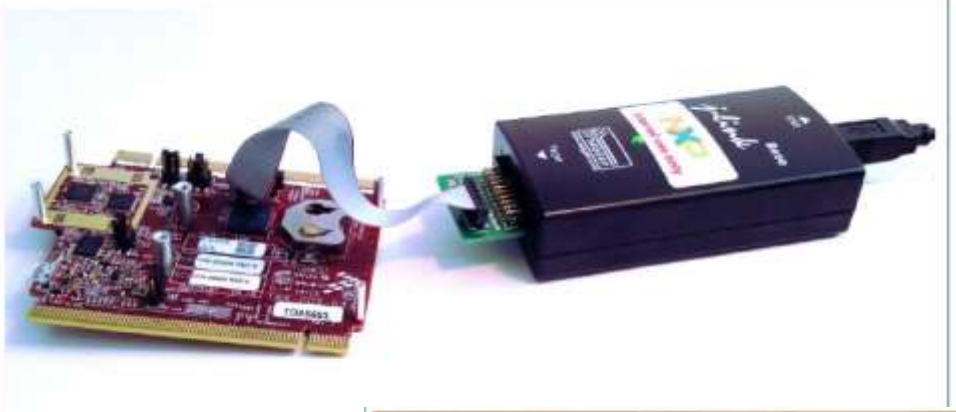


Fig 40. J-Link probe connections

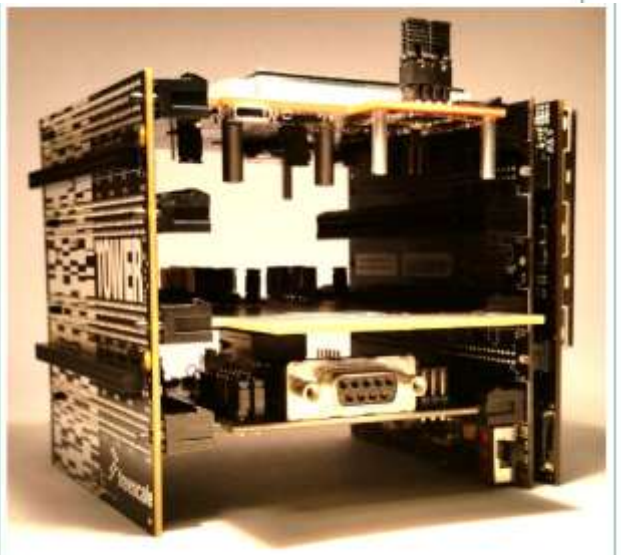


Fig 37. TWR-SER in the POS-RDR-SLN Kit

Connecting to the board (Documented in Quickstart Guide)

4.2.3 Using IAR

This chapter describes how to open and run the project Payment Application Demo.

IAR must be pre-installed with a valid license before going through these steps.

The minimum required IAR version is 7.70.0.

4.2.3.1 Open the project and compile

1. Locate the .eww file from the demo project folder:

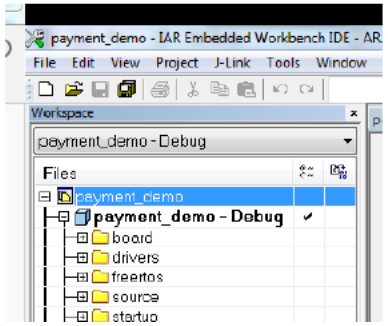
   K81POSCR_SW_Release\boards\twrposk81\demo_apps\payment_demo\iar

2. Double click on the .eww file. It will open the project in IAR.

Alternatively, if the .eww files are not linked to IAR, the following step have to be done. Otherwise, jump to step 6.

3. Open IAR
4. Select File>Open>Project and browse to the folder containing the IAR project file (extension is .eww).
5. Select the file payment_demo.eww

   The project contains two subprojects: Payment_demo and lib_pos:



4.2.4 Using KDS

4.2.4.1 Install and start KDS

KDS (Kinetis Design Studio) has to be installed first. The KDS installation can be found from NXP website:

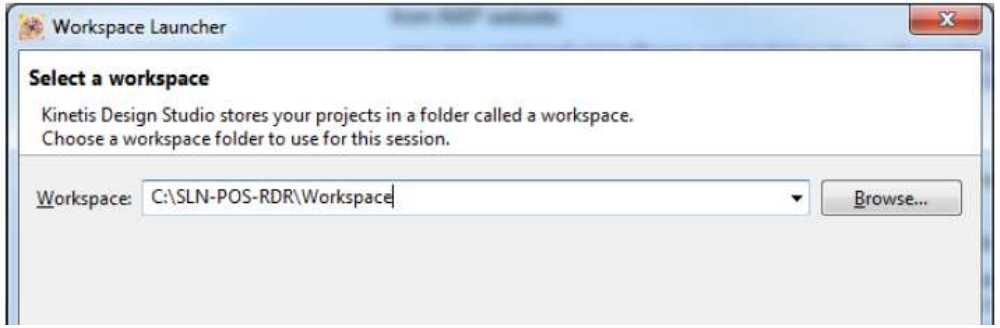
www.nxp.com/products/software-and-tools/run-time-software/kinetis-software-and-tools/ides-for-kinetis-mcus/kinetis-design-studio-integrated-development-environment-ide:KDS_IDE

The minimum required KDS version is 3.2.0.

Once KDS is installed, launch the application. KDS first asks to select a folder that will become the Workspace for this KDS session.

Select any folder on the local disk. It doesn't have to contain data at first.

Remember the folder location: next time KDS will be open, this workspace will have to be selected to retrieve the ongoing projects. The workspace will not necessarily contain source code, but it will contain all configuration and information about current projects.



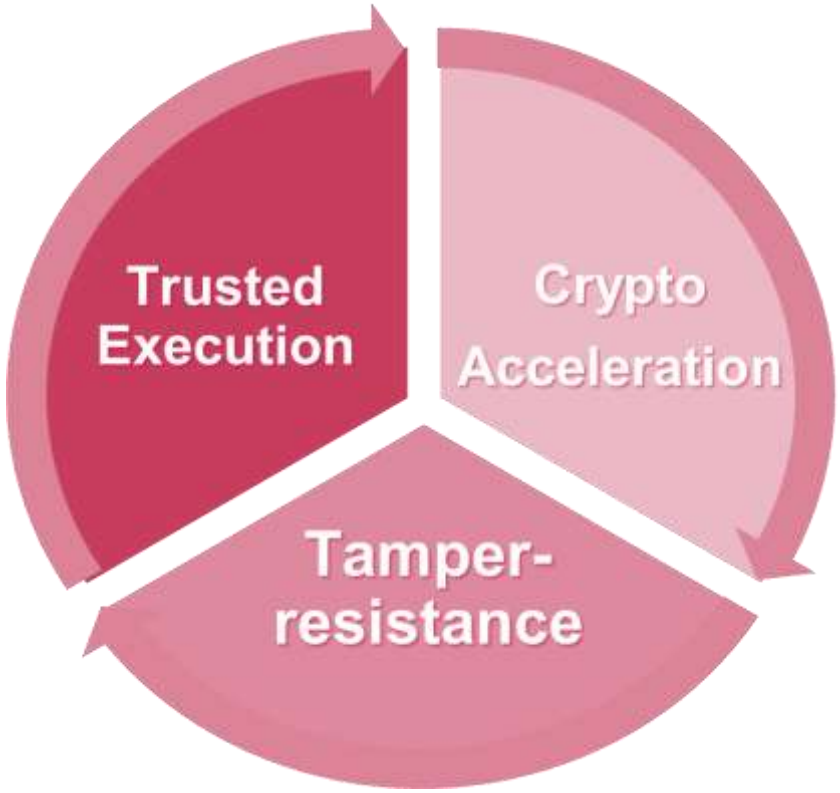
Common Solution Use Cases

- Some customers are copying our solution exactly as is (HW designs matching our schematics)
- Changing hardware
  - Serial flash from Micron to others
    - Requires updates to IDE macros
  - Changing I/O used
    - For example, different SPI pins
  - Magnetic Stripe through ADC interface/UART
- Running cryptographic benchmarks
  - Using mbedTLS
- Customize the GUI for a custom banner
- Support for secure boot and Firmware updates, OTFAD
  - Part of maintenance plans
  - Connectivity (BT, Wi-Fi, etc.)

02.

Problems Addressed by Solution

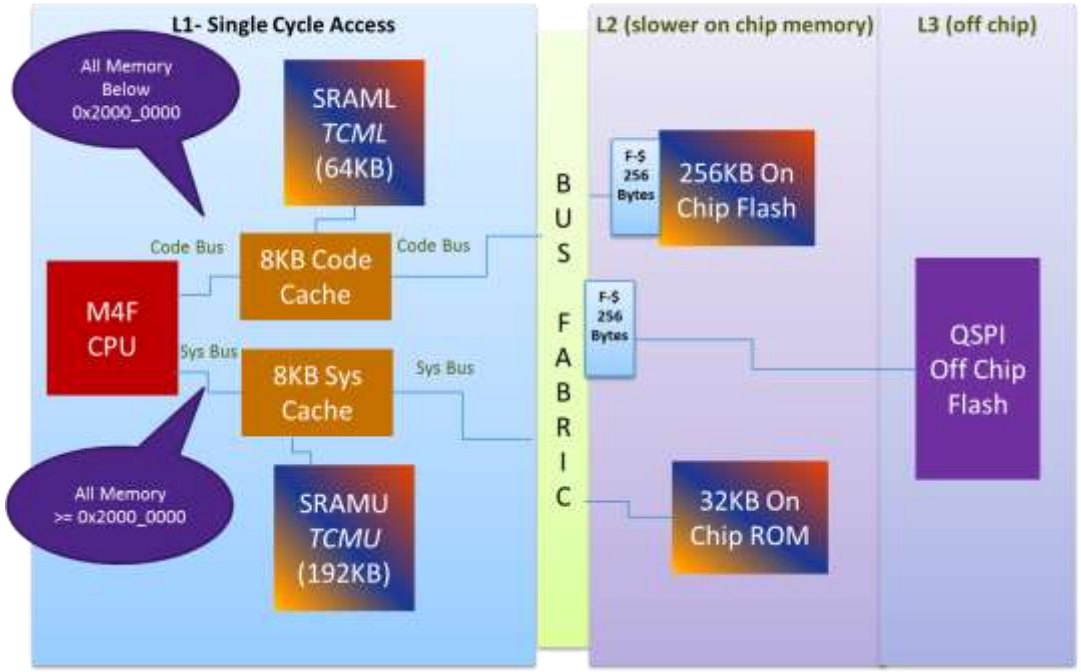
Security Technology



- **Tamper Resistance**
  - Hardware and Software implementation
  - SDK DryICE Driver use
  - Tamper demonstration part of payment demo
- **Trusted Execution**
  - System Memory Protection (MPU)
    - Configured to protect memory used for PIN
  - On-the-fly AES from XIP
    - NEW in maintenance release
- **Cryptographic Acceleration**
  - Symmetric and Public Key Cryptography
  - Side Channel Resistant MMCAU and LTC crypto libraries
    - With PCI PTS side channel reports

Memory Expansion

- Quad SPI with external serial NOR flash
  - Setting up linker files for external code and data
  - Enabling CPU cache for optimal performance
  - Debugging and development experience
  - File System (SPIFFS)



User Interface

- EGUI with SPI TFT display
  - Fonts, Text Boxes,
  - Image Converter tool

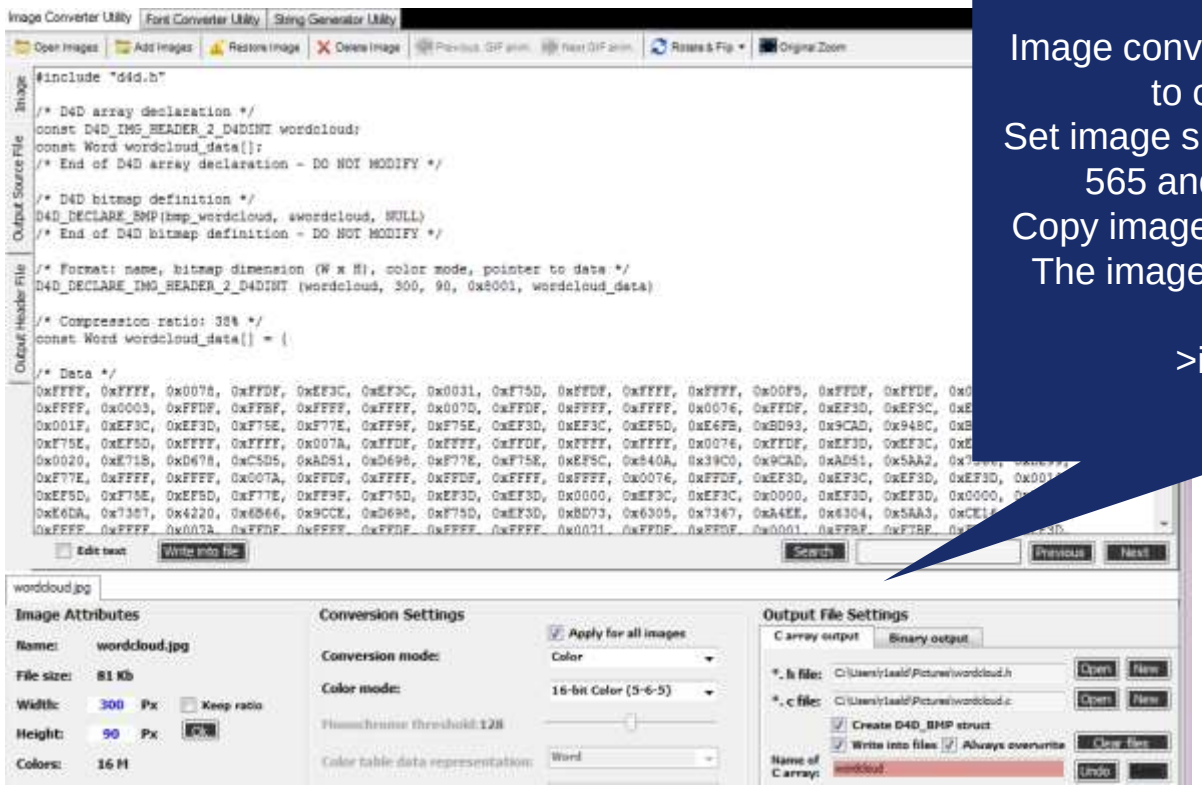
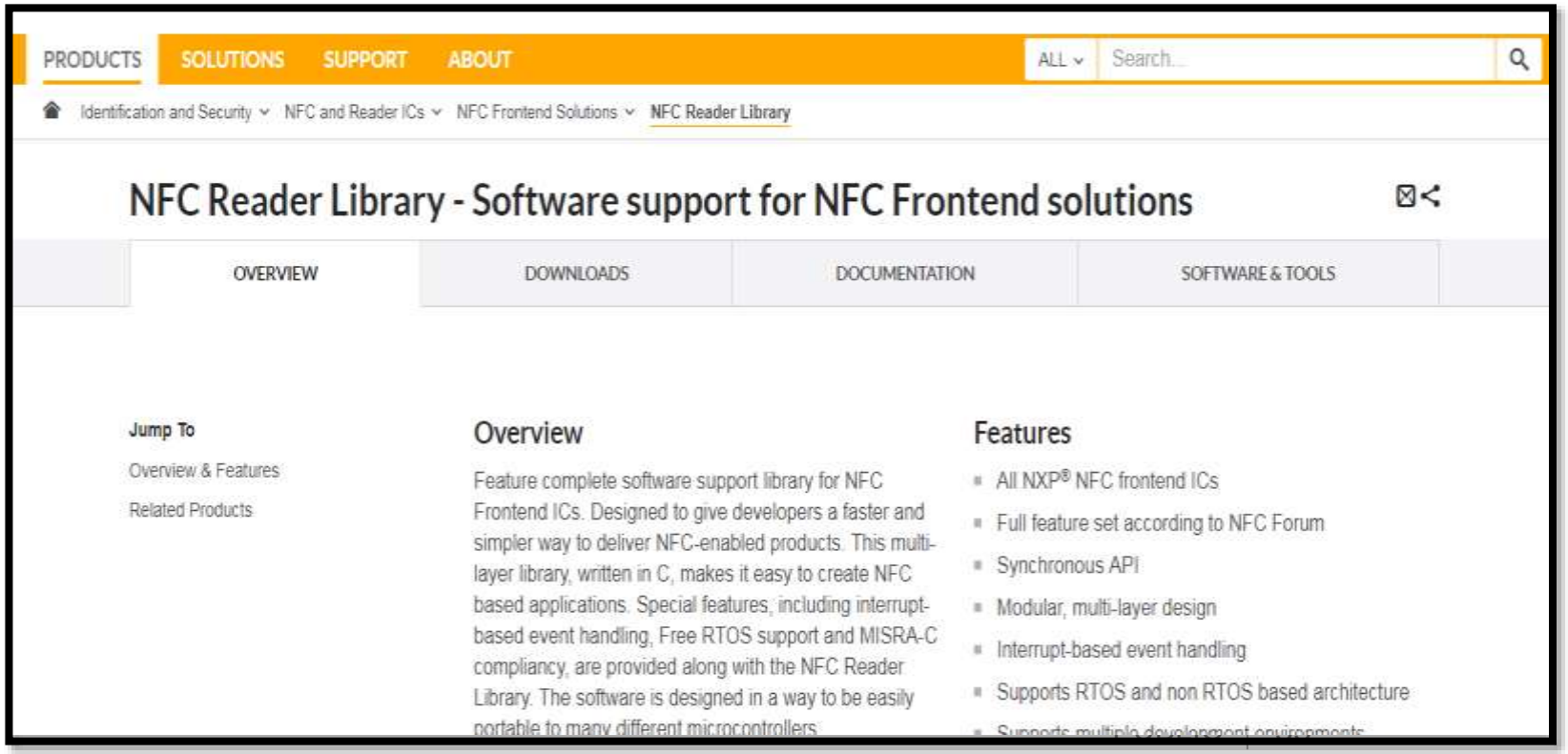


Image converter utility can be used to convert images
Set image size to banner size, RGB 565 and use compression
Copy image data to the images file
The images file is in the libpos->modules->ui->egui->images folder

Smart Card Reading

- NFC Reader Library
  - EMVCo Layer 1 stack from NXP
- ISO-7816 Communications
  - Smartcard Stack from SDK

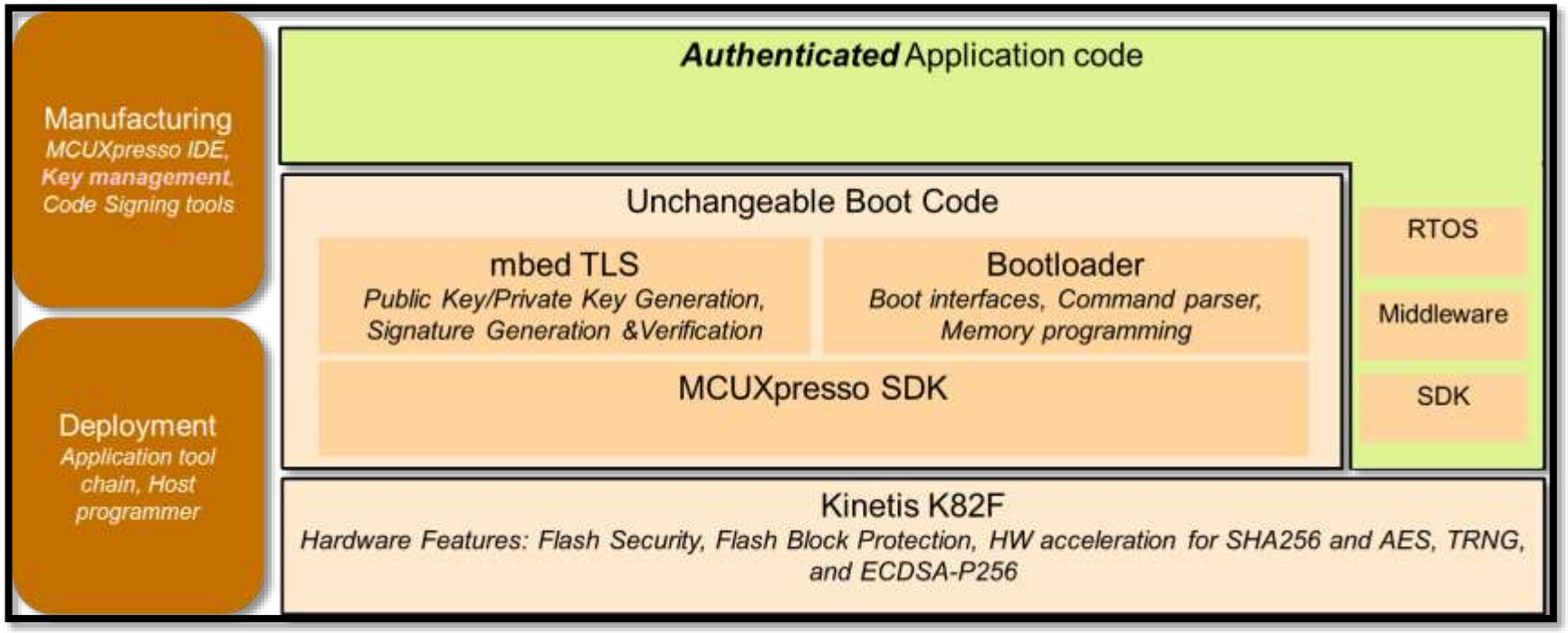


03.

Hands-On Labs

LAB1: SECURE BOOT

- Kboot bootloader
- Host tools (elftosb and blhost)
- Mbed TLS cryptography



LAB2: QUADSPI XIP

- Linker file configuration
- Flash loaders
- Automatic Downloading
- Optimization for performance
- Debugging XIP Code

SECURE CONNECTIONS
FOR A SMARTER WORLD