FTF 2016
TECHNOLOGY FORUM

TOWER POS SOLUTION AS STRONG DEVELOPMENT SUPPORT

FTF-BAN-N1897

MICHEL BRUN AND MIKE DOW
PRODUCT MARKETERS
FTF-BAN-N1897
MAY 18, 2016

AGENDA

- Introduction
- Overview of POS Market
- Certification Challenges of the Point of Sale
- Secure Card Reader Architecture
- TWR-POS Solution
- Payment Solution Roadmap

Introduction

- NXP is a key player in the payment terminal industry as a chipset provider (card reader ICs, Smart card ICs, security controllers and processors, ESD protections…)
- NXP is providing pre qualified solutions/ reference designs/ evaluations environments as a combination of chipset building a more complete solution offering in order to improve TTM of end customers.
- NXP will be presenting here the first Secure payment solution package combining a security controller and card interfaces with the appropriate software stacks.
- The solution package will include HW boards featuring a payment terminal with keypad and display, documentation on hardware and software, pre-certified EMVL1 software stacks, PCI security assessment of security controller, recommendations for HW design to meet PCI requirements, demonstration software with a partner application.

OVERVIEW OF POS MARKET

Definitions

Traditional POS

- The traditional POS definition primarily covers traditional desktop solutions and standalone mobile solutions designed to improve POS mobility without the requirement to connect with another mobile device.
- Typically traditional POS solutions will have their own screens and PIN pads to be able to process contact, contactless, and mag-stripe payments, often with a receipt printer included or attached. Traditional POS terminals can be large-screen devices or equally smaller handheld units.

mPOS

- A mobile Point of Sale (mPOS) is a consumer grade handheld device (e.g. a smart phone or tablet) with wireless connectivity that is used for the acceptance of payment cards. An mPOS solution typically comprises:
  - A mobile device – consumer grade mobile phone or tablet device with wireless connectivity
  - Card Reading functionality (contact, contactless or both)
  - Applications supporting the payment functionality, the EMV kernel and user interface
  - Server-side software
  - CVM capture capability (e.g. PIN entry, signature capture)
- There are mPOS vendors that produce the hardware, generating revenues only from the distribution of white-labeled devices and/or payment platforms, vendors that generate revenues from the actual payments, taking a fee per transaction or standalone monthly fixed rate, and those vendors that do a combination of the two

Definitions

PINPAD

- A PINPAD or PIN entry device is an electronic device used in a debit, credit or smart card-based transaction to accept and encrypt the cardholder's personal identification number (PIN). PIN pads are normally used with automated teller machines and integrated point of sale devices in which an electronic cash register is responsible for taking the sale amount and initiating/handling the transaction. PINPAD normally implemented by POS vendor as:
  - Integrated solution to payment terminal such as mobile traditional POS and mPOS
  - Standalone PIN entry device with UART or USB interface to desktop solution
  - PINPAD module to ATM machine or vending machine

Secure Card Reader

- Secure Card Reader is the hand-held smartcard readers to support different electronic payment applications. Typical use case is:
  - Typical use case: Chip Authentication Program (CAP) uses EMV banking cards to authenticate online transactions as a phishing countermeasure.
- Most of the secure Card Reader (eg home banking readers)will integrate the PINPAD function. Below are the popular card interfaces to be integrated:
  - Magnetic stripe to support legacy bank card issued before 2015
  - Contact IC Card is the must have interface to all device that in production in market after 2015
  - Contactless NFC become more and more popular and will adopt as standard card interface in coming years

Prepaid Smart Meter

- A prepaid smart meter is a metering terminal which can accept contact or contact-less smart cards enabling to reload the meter with a certain volume of energy (water/gas/electricity) stored on the card. The card can be reloaded at a dedicated shop or using an on line using a secure card reader.

Key Uses Cases – Applications

POS

- Standard Payments (EMVCo like)
- Loyalty / Couponing
- Open Loop and Close Loop Payments
- Retail

Secure Card Reader

- Home banking
- Public Transportation (eg bus, metro)
- Parking Payment

Prepaid smart meter

- Energy payment

mPOS

- Micro-merchants, tradesmen
- Pay-on-delivery applications
- In-store shopper-assisted retail
- In-aisle check-out
- Loyalty, Couponing
- Transportation (eg taxis)
- Stadiums, events, attractions

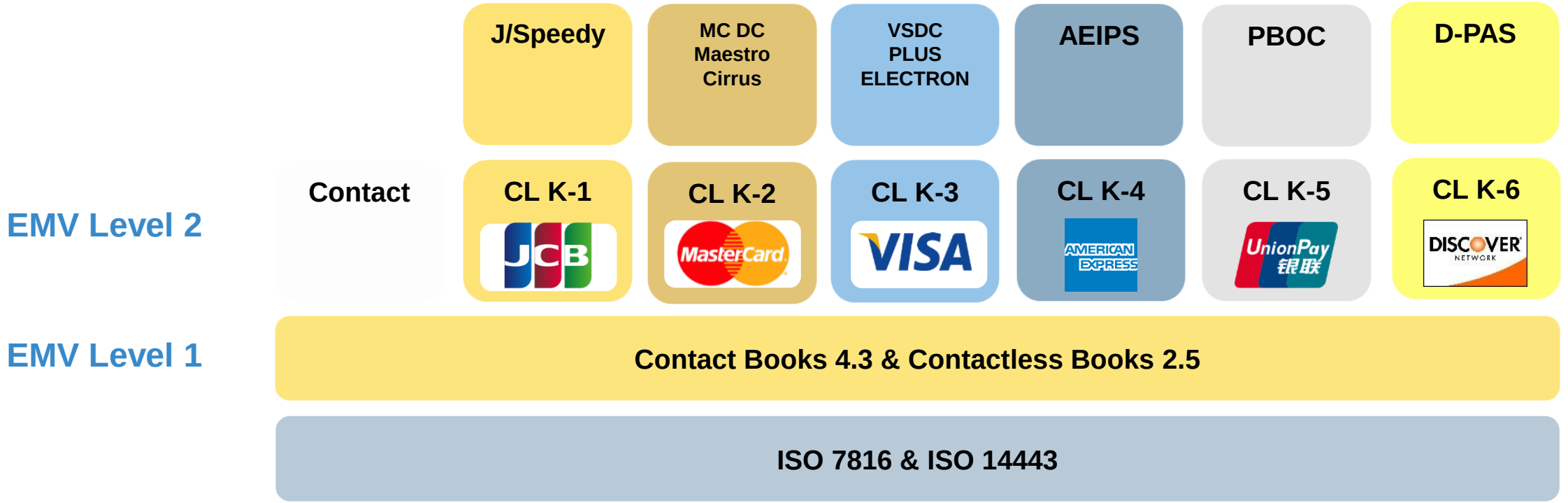
CERTIFICATION

PCI Security Standards Council

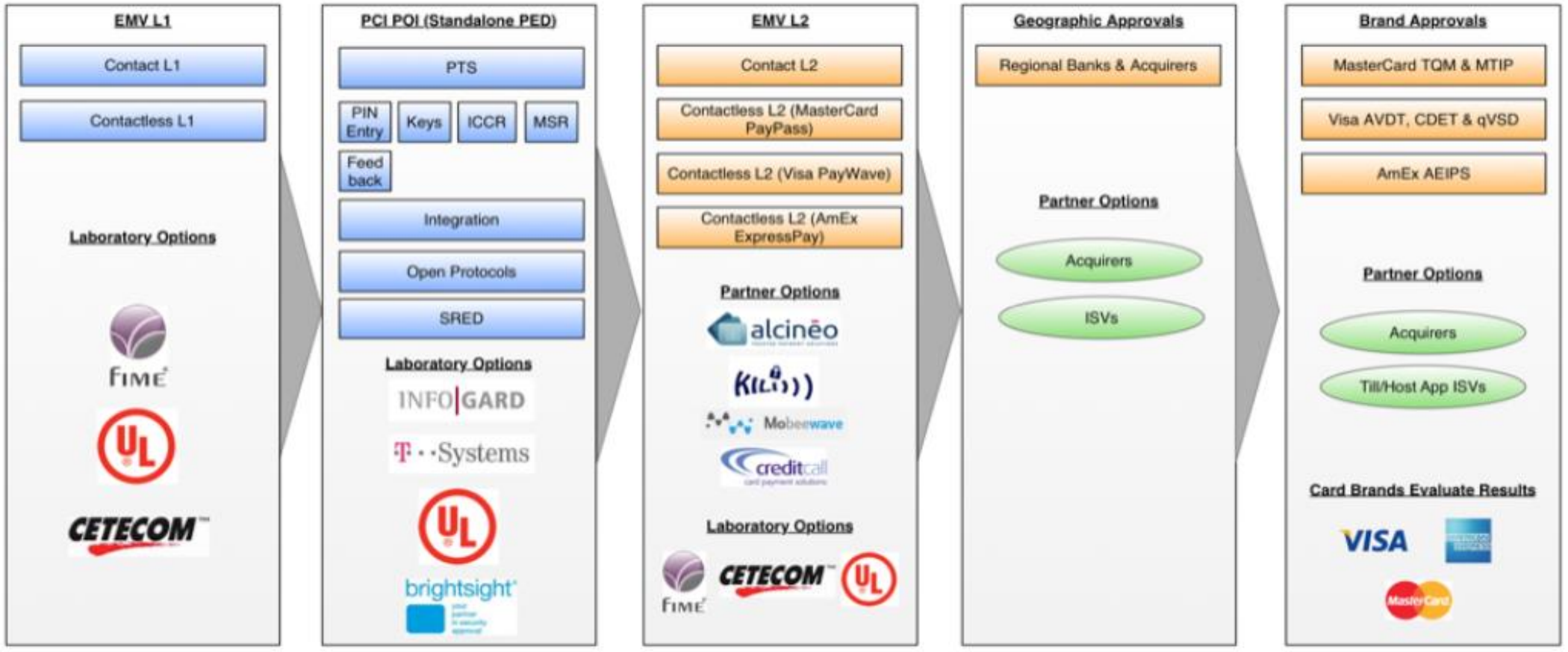
- The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.
- In general all the qualified finance payment terminals in commercial usage must get PCI certification regulated by PCI Security Standards Council
  - Website: https://www.pcisecuritystandards.org/

EMVCo Certification

- EMVCo defines two certification levels:
  - Level 1: physical, electrical and transport level interfaces
  - Level 2: payment app selection and credit financial transaction processing
  - Webiste: http://www.emvco.com/



POS Certification is a Long and Brutal 14 Month Process



ARCHITECTURE & NXP PRODUCT OFFERING

Point of Sales

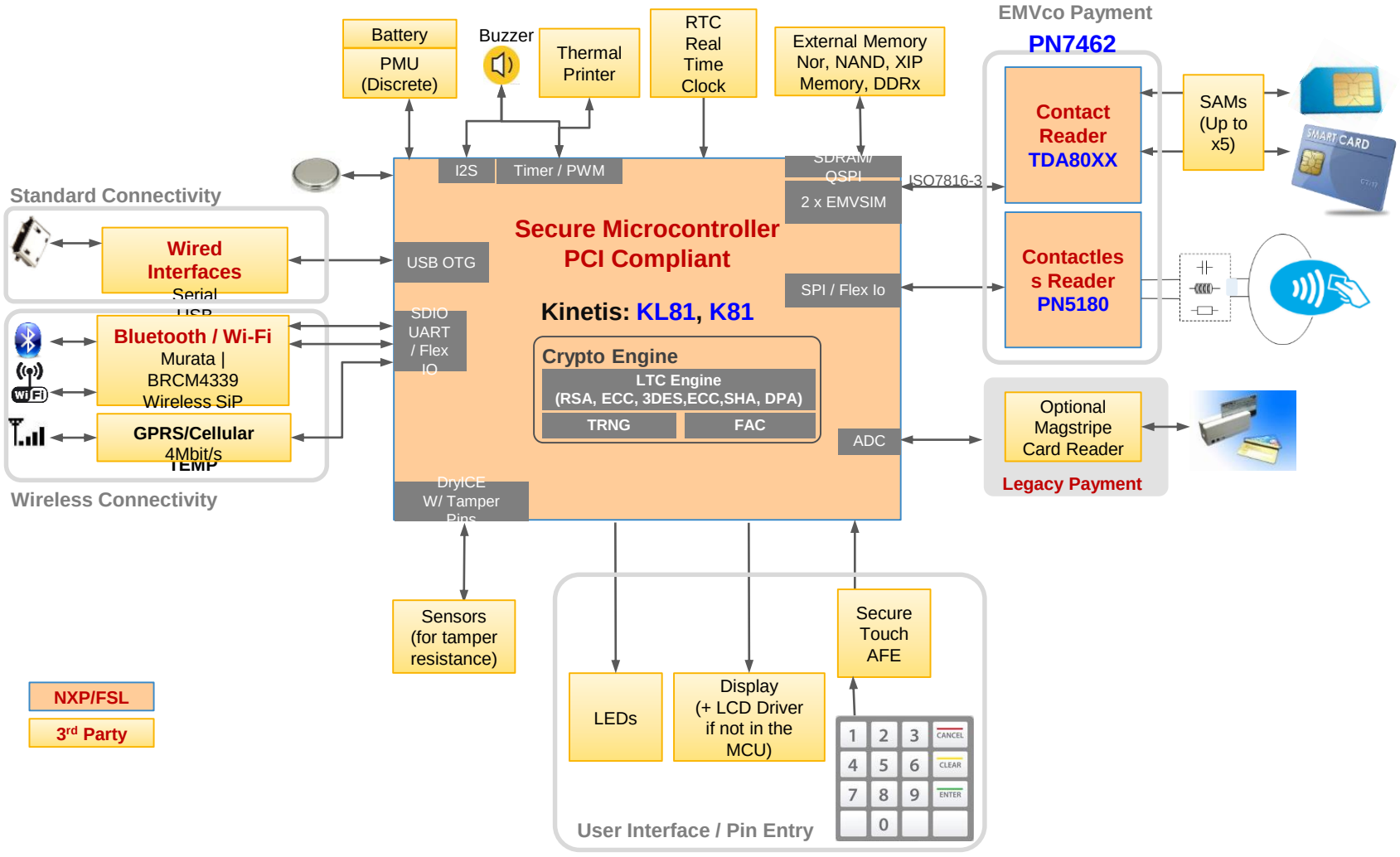
A Scalable Portfolio to Address a Wide Range of POS Solutions

PinPad / mPOS	POS / Smart POS	Tablet / Counter Top POS	High End POS
				
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

Power efficient, secure and connected solutions

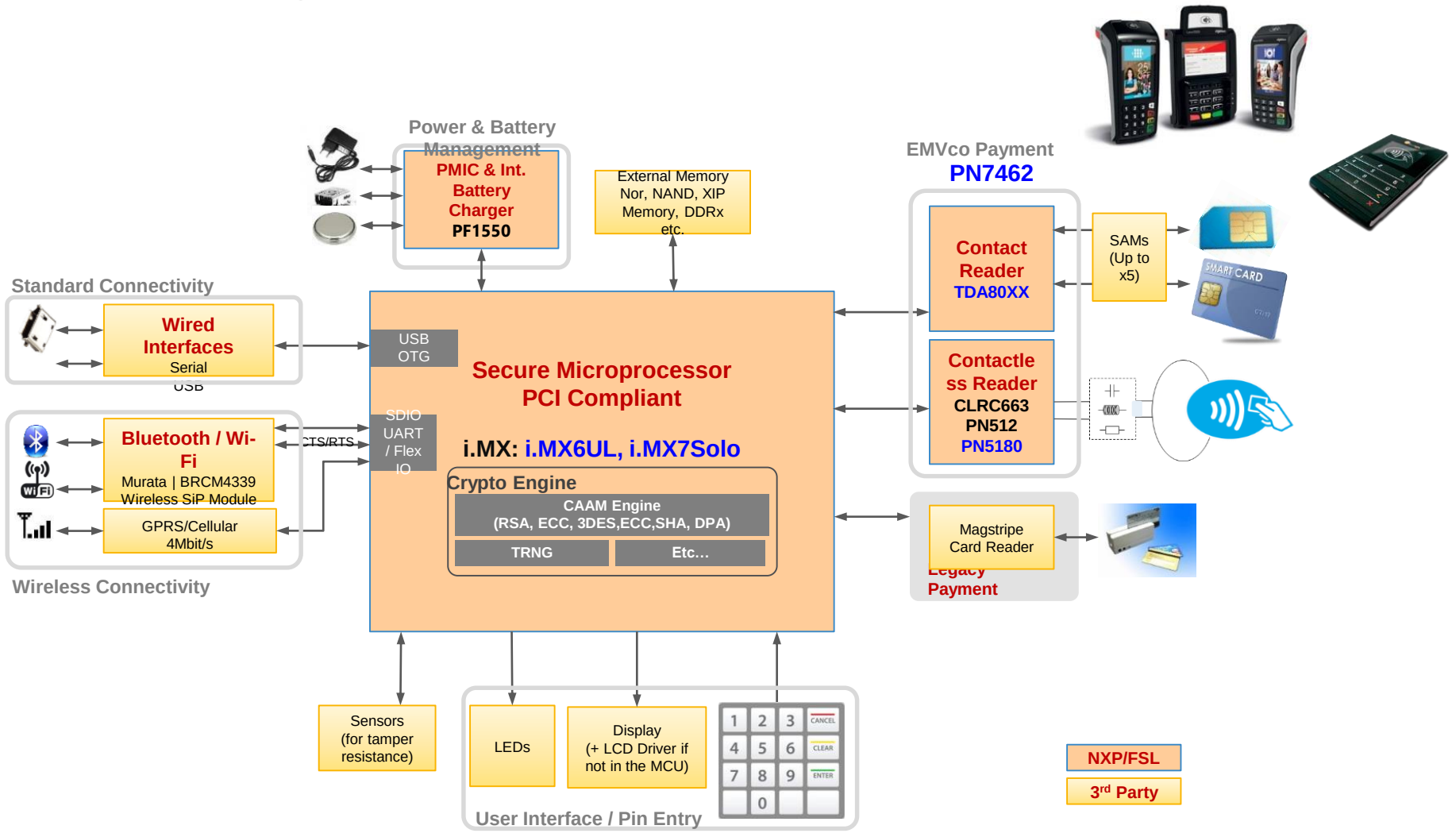
PinPad, mPOS

Architecture Block Diagram



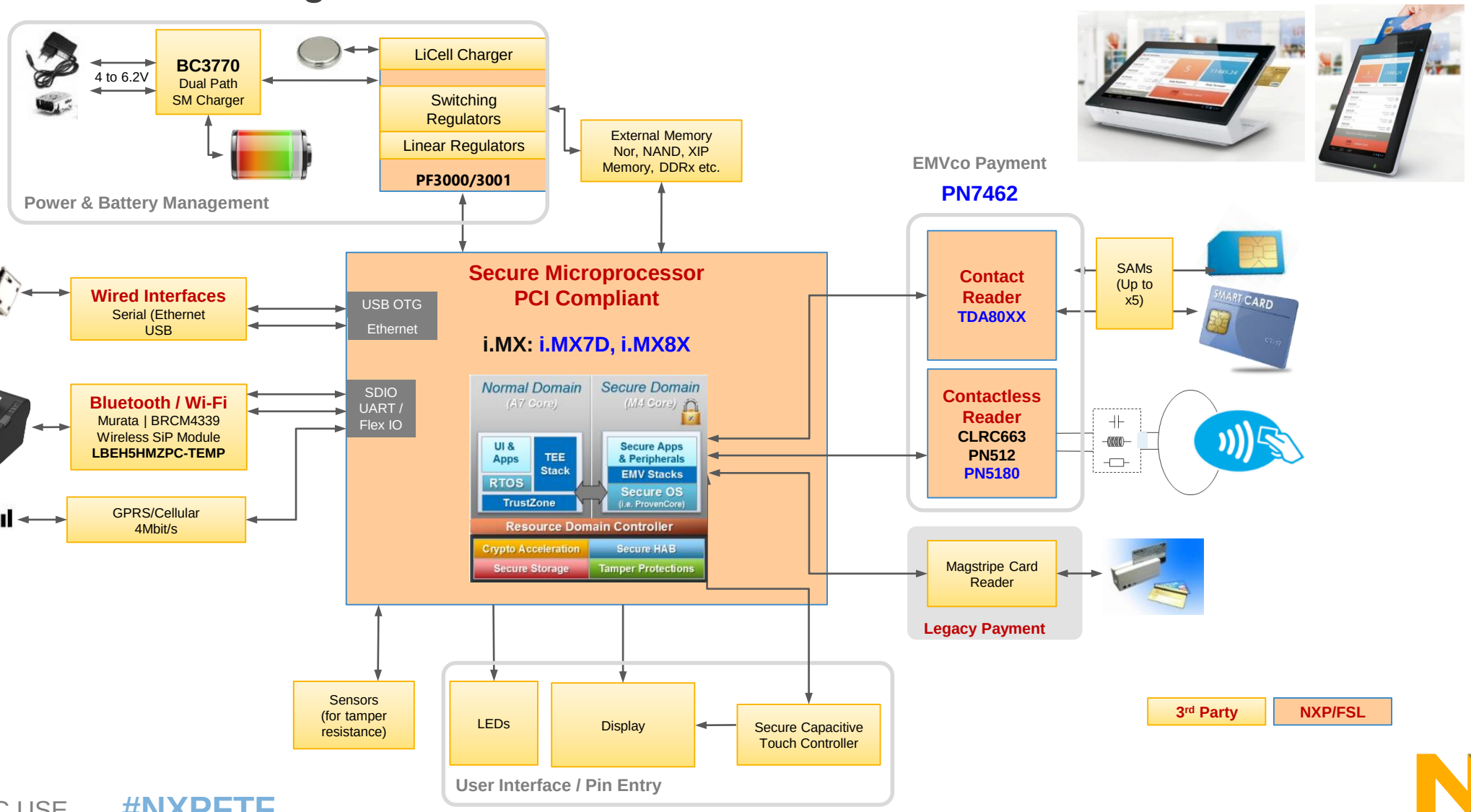
Traditional Smart Mobile POS

Architecture Block Diagram



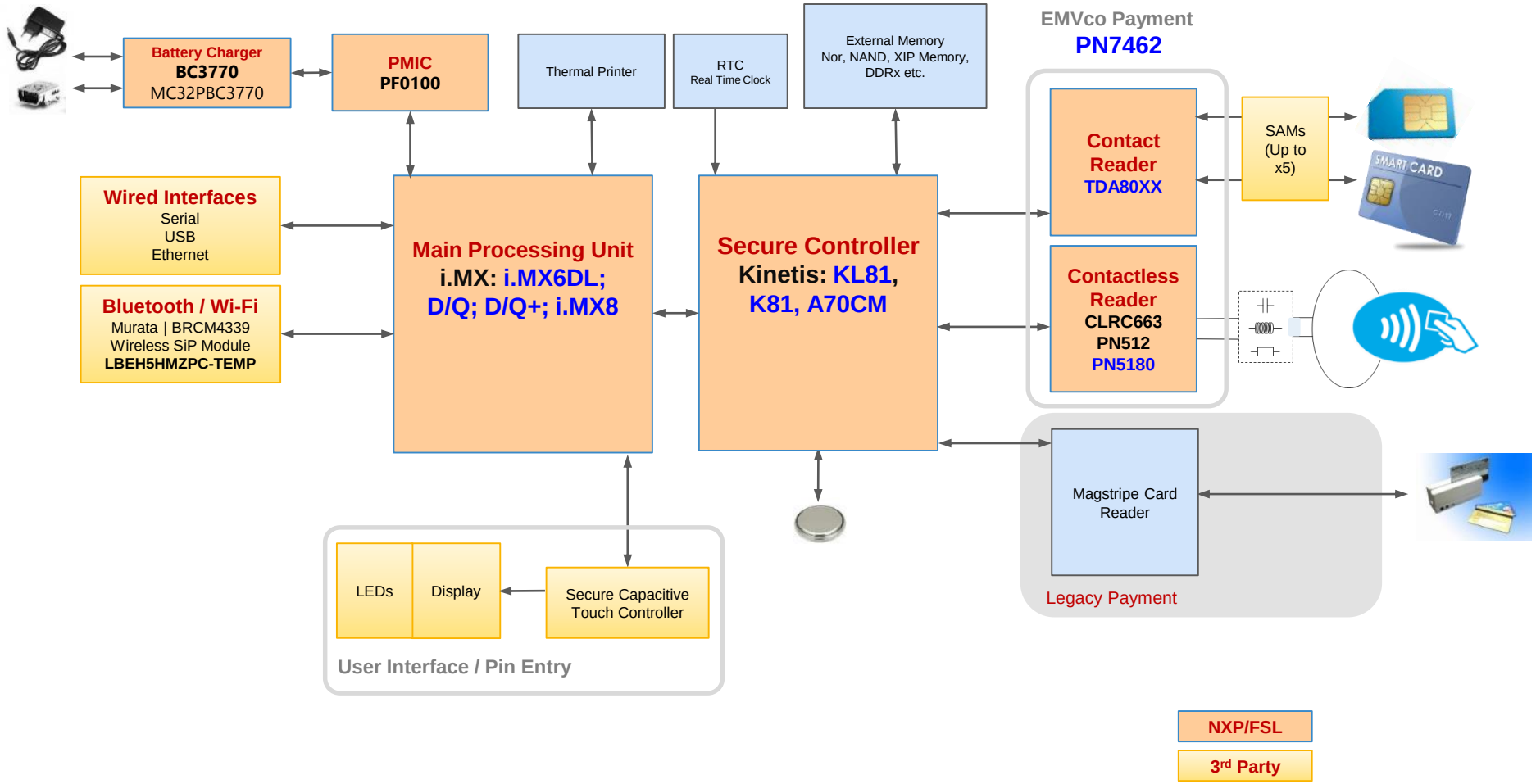
Tablet Counter Top POS

Architecture Block Diagram

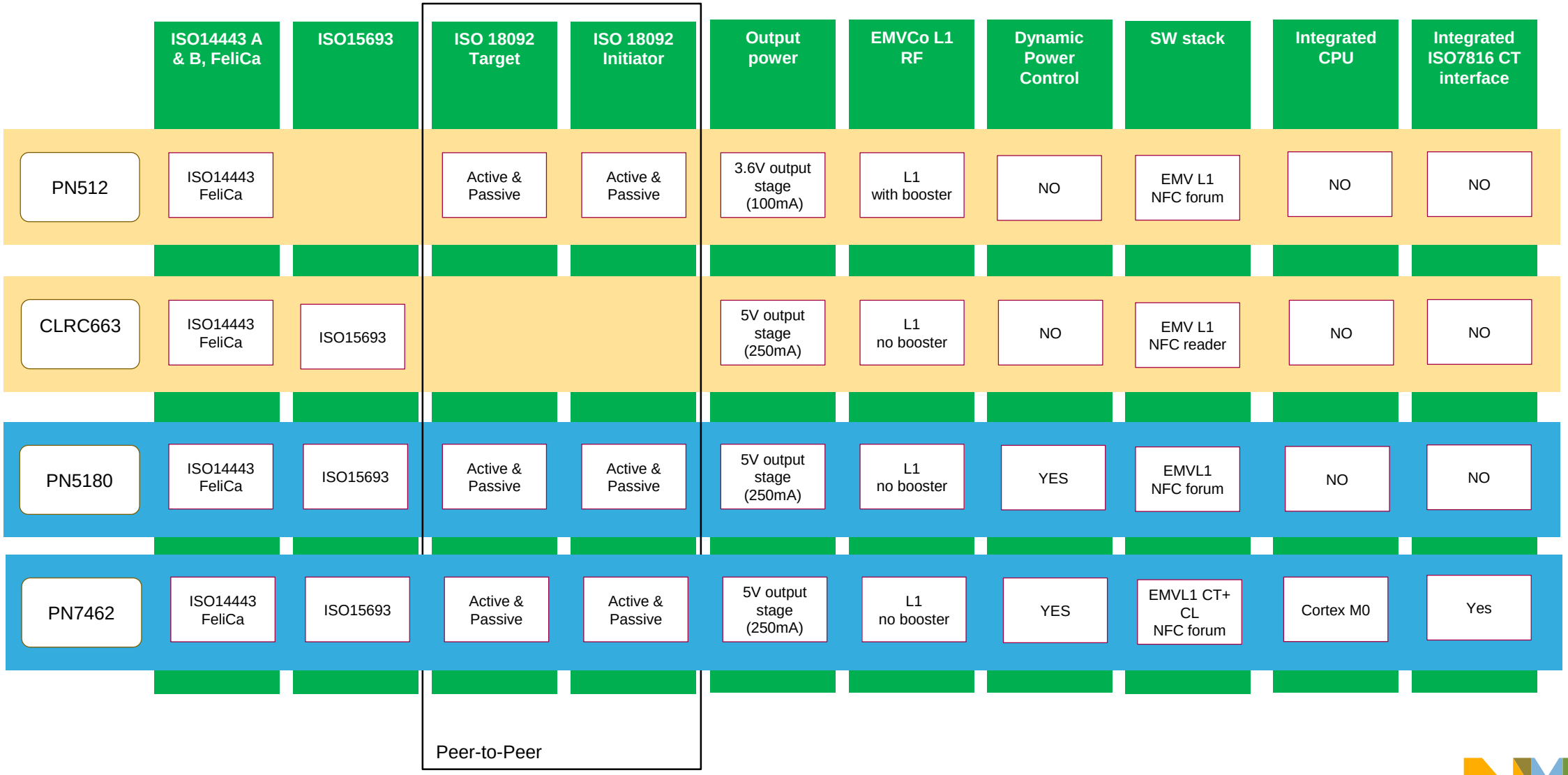


High-End Tablets & Payment Terminals

Architecture Block Diagram



NXP Offers a Complete CL/NFC Portfolio for POS/mPOS



NXP Offers a Complete CT Reader Portfolio for POS & mPOS

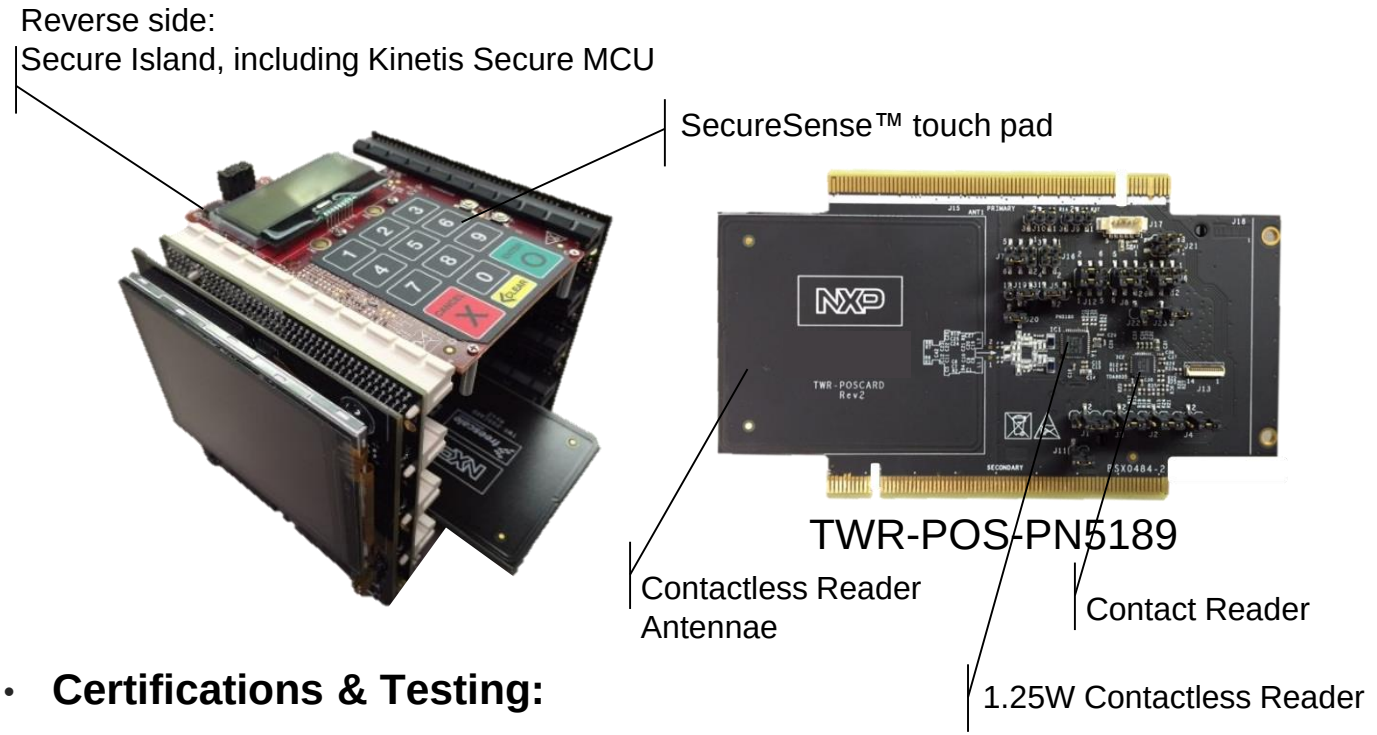
	Card Class Support	EMVco L1	Number of card slots	ESD Protection	Card Management	Package	SW stack
TDA8034HN*	Class A,B,C	Compliant	1	6kV	Sync & Async	HVQFN24	L1
TDA8035	Class A,B,C	Compliant	1	10kV	Sync & Async	HVQFN32	L1
TDA8026	Class A,B,C	Compliant	5	7kV	Sync & Async	TFBGA64	L1

* TDA8034HN has no DC/DC converter and can support Class A cards with a supply voltage of 4.80V min.

TWR-POS SOLUTION

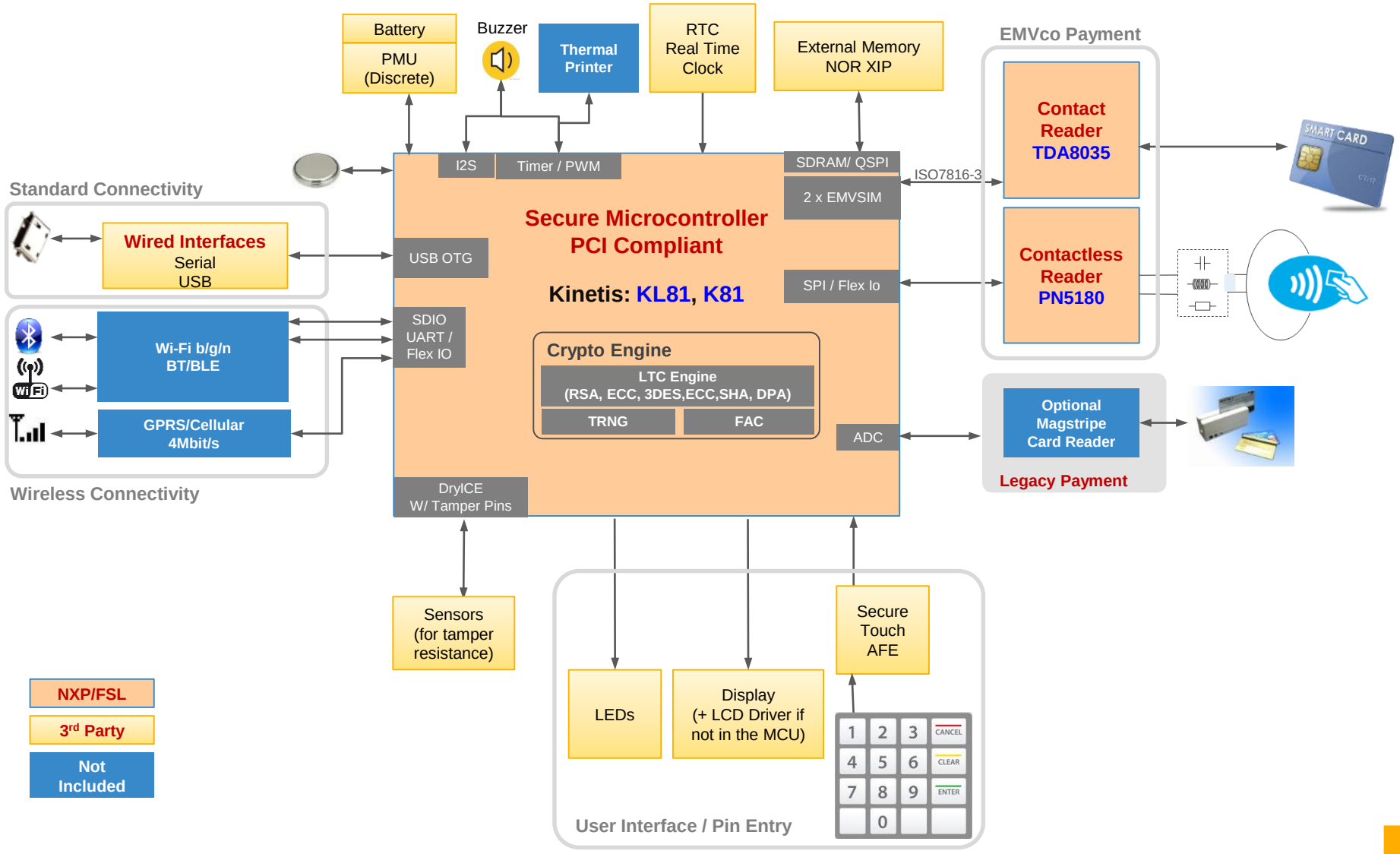
Point of Sale (POS) Reader Solution Overview

- 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
- **Availability:** Sampling now, Launch Jul ‘16



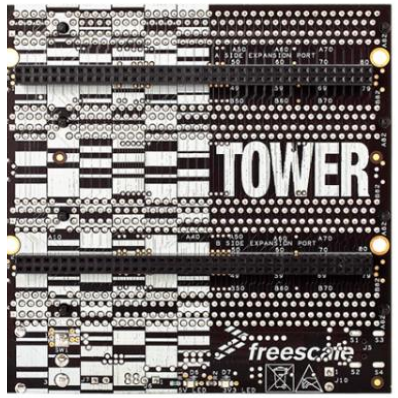
- **Certifications & Testing:**
  - TWR-POS-K81 PCI 4.1 Certified as PIN Pad *
  - PCI silicon pre-certification
  - Side channel attack testing *
  - CAVP (crypto assurance validation program) certified
  - TRNG entropy evaluation
  - EMVCo L1 CT/CL pre-certified

Point of Sale (POS) Reader Solution Architecture

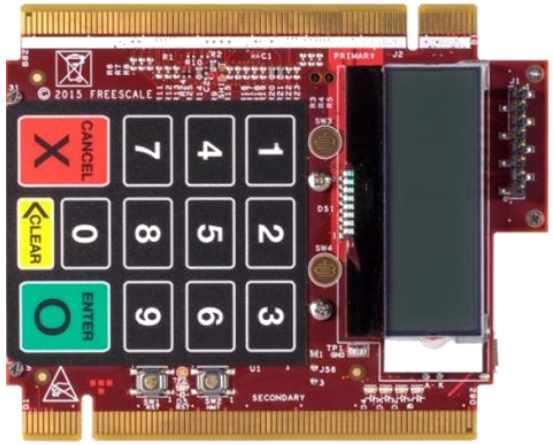


A Flexible Solution Concept Using TWR System Module

TWR-LCD

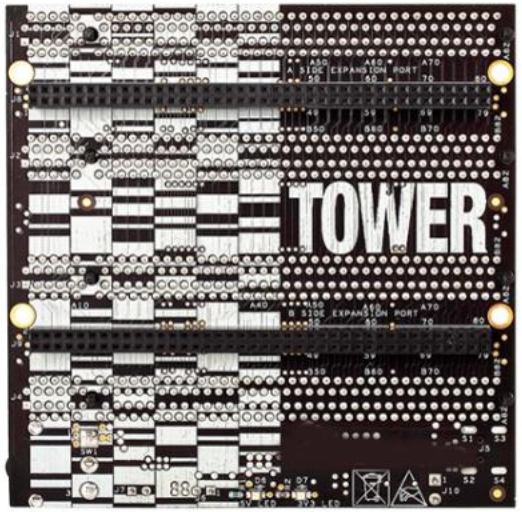


TWR-ELEV



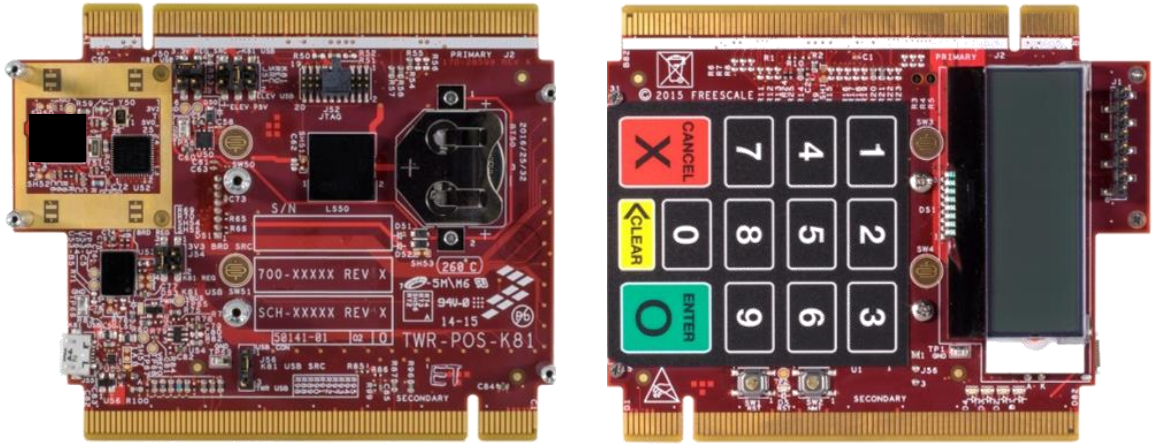
TWR-POS-K81

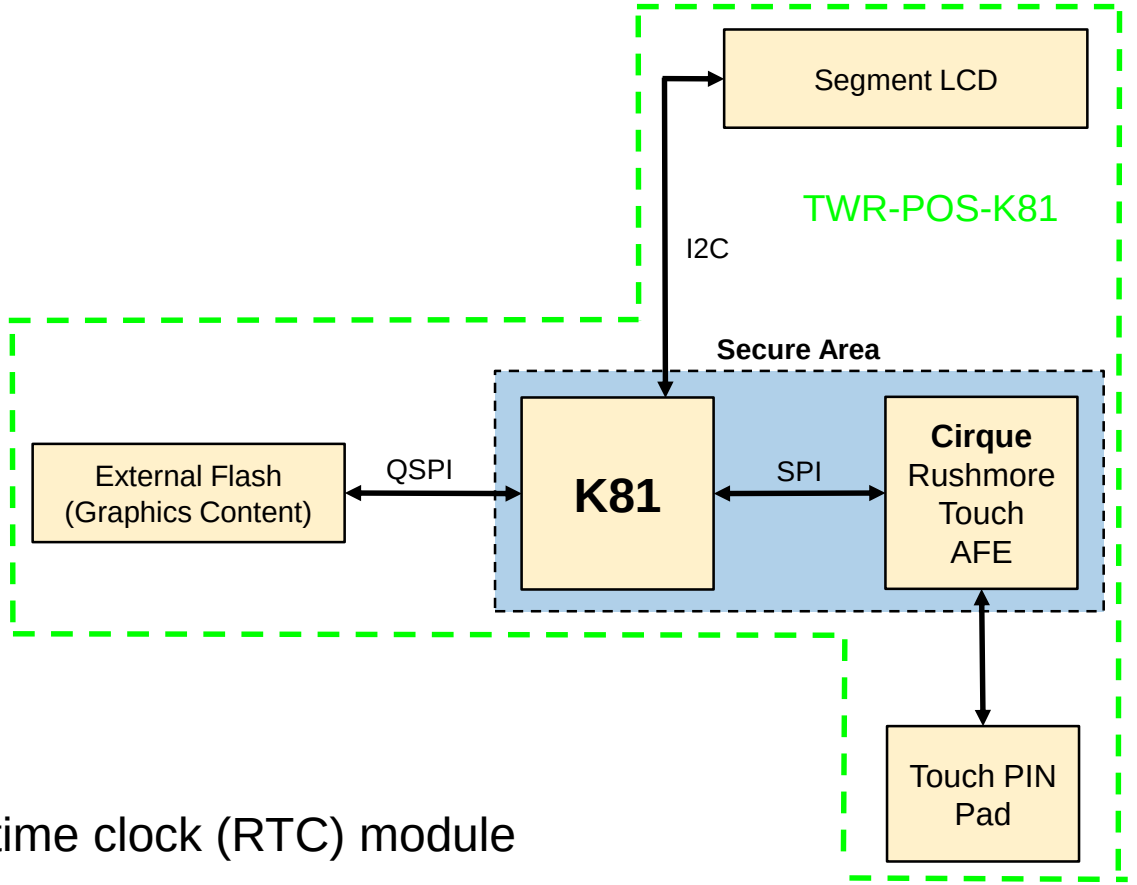
TWR-POSCARD-PN5180



TWR-ELEV

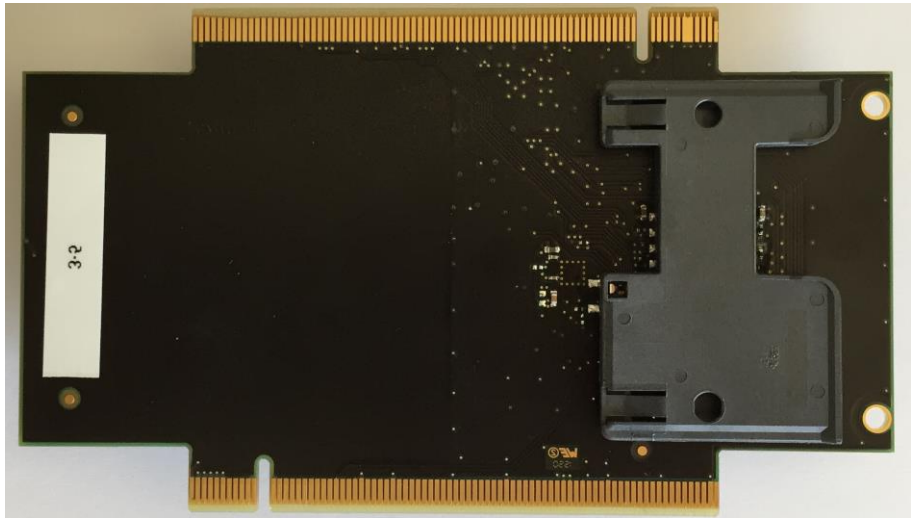
K81 Secure Touch Pin Pad Solution

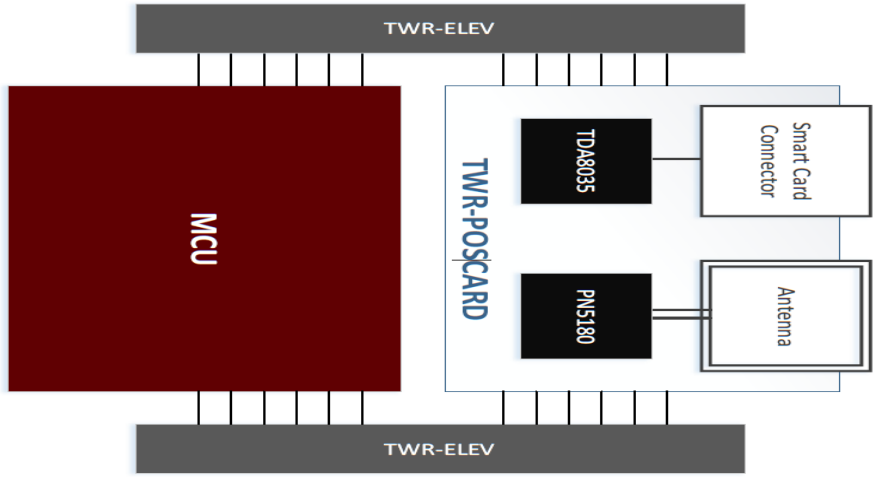




- K81 Secure Micro w/ Tamper and Crypto
- Secure Capacitive Touch (by Cirque) Pin Pad
- Tamper Header providing access to 8 tamper signals
- Chip on glass 2 lines x16 Character segment LCD
- 4 used control status LEDs
- Independent, battery-operated power supply for real-time clock (RTC) module
- Production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

TWR-POSCARD-PN5180



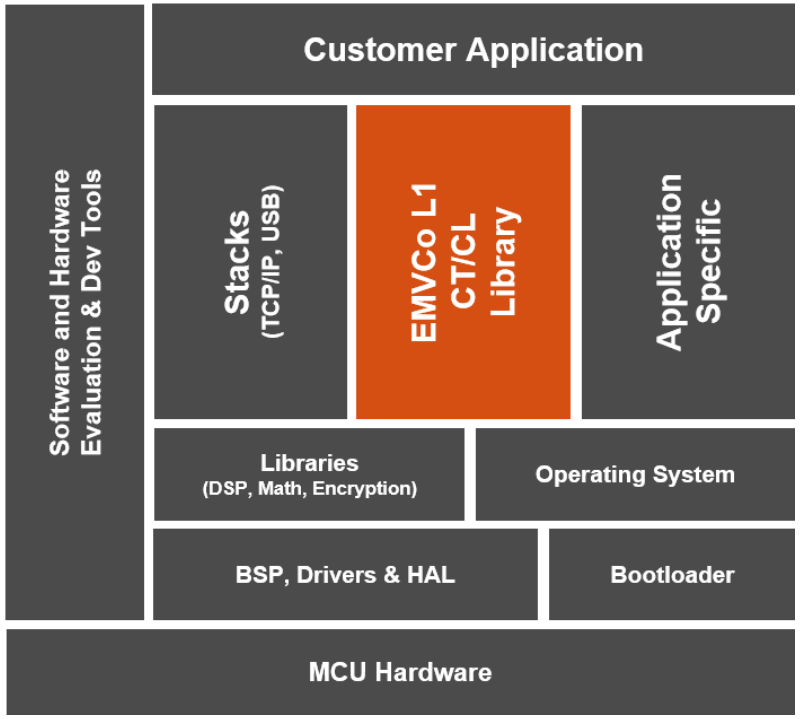


- Point of Sale Card Reader Board
  - Tower Form factor
    - Tower peripheral board for expanding capability of TWR-POS-K81 or other tower MCU boards
  - PCB Antenna for contactless payment
    - ***NXP NFC: PN5180 NFC Front end***
    - ***Full EMVL1 2.5 compliant stack available in KSDK***
    - ***Test report from independent test house***
  - Smart Card reader PHY
    - ***NXP: TDA8035 Smart card interface***
    - ***EMVL1 4.3 compliant stack available in KSDK***
  - Example part of the KSDK 1.3 & 2.0
    - Utilizes New EMVSIM peripheral of the K8x devices

Secure Card Reader Reference Solution Enablement

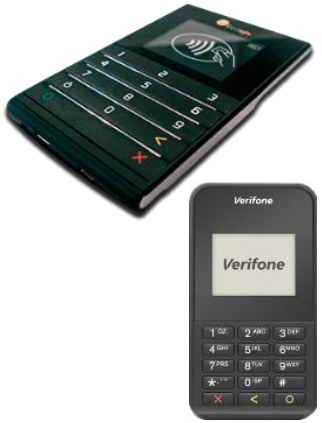
KSDK

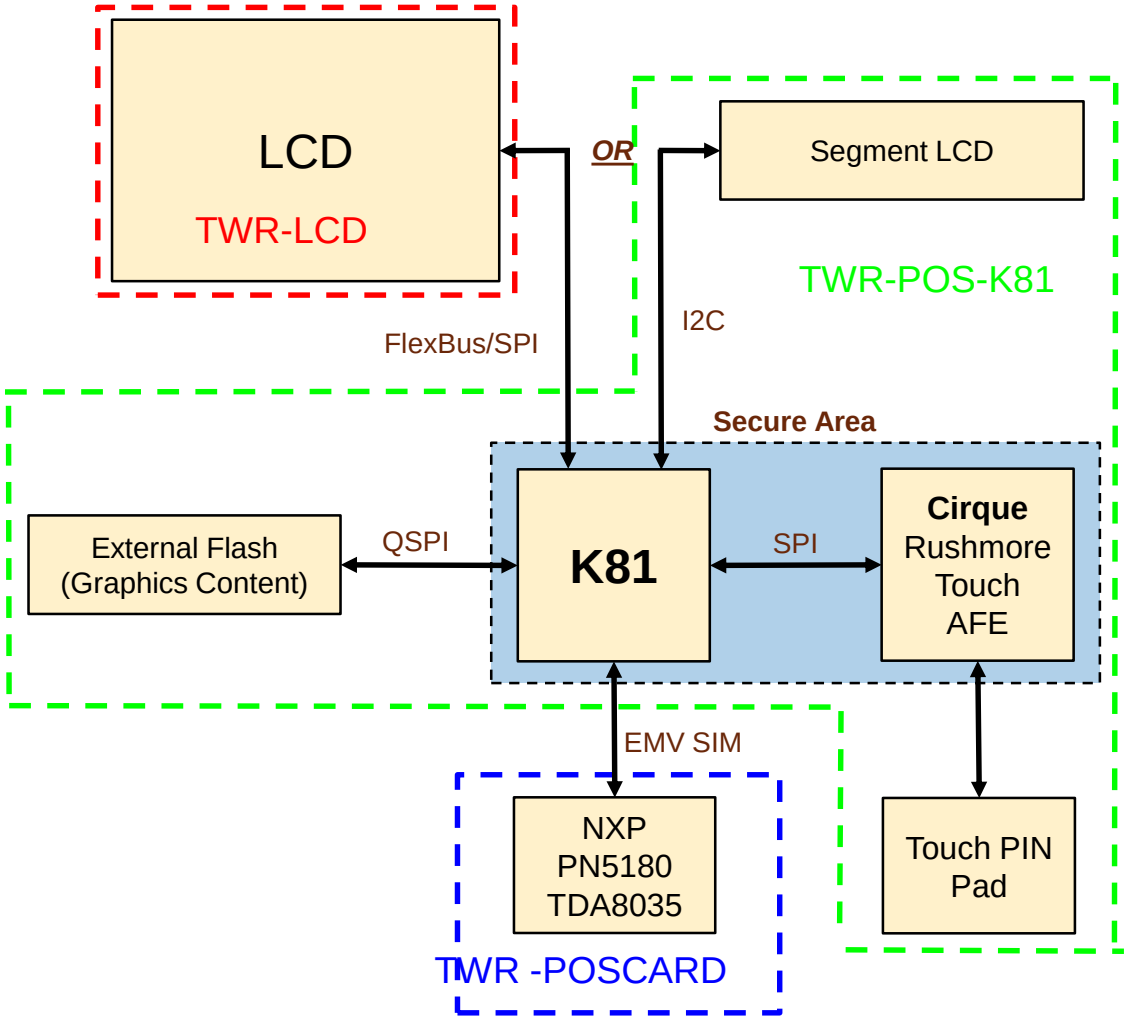
The software framework and reference for Kinetis MCU application development



- Quick Start Guide
- User Manuel
- Software
  - EMVCo L1 CT/CL Library integrated in KSDK
  - EMVCo L2 CT/CL Library integrated from 3rd parties
- Application Notes
  - AN4733 - Dry Ice App Note
  - AN4507 - Flash Security App Note
  - AN10997 – TDA8035 Smart Card Reader
  - AN11740 – PN5180 Antenna design guide
  - AN11742 – Dynamic Power Control
  - ANxxxxx –TWR POSCARD HW
- Certifications
  - Infogard PCI Silicon Pre-cert report
  - Infogard TWR-POS-K81 Pin Pad PCI 4.1 Certification Report
  - EMVCo L1 CT/CL Pre-cert report

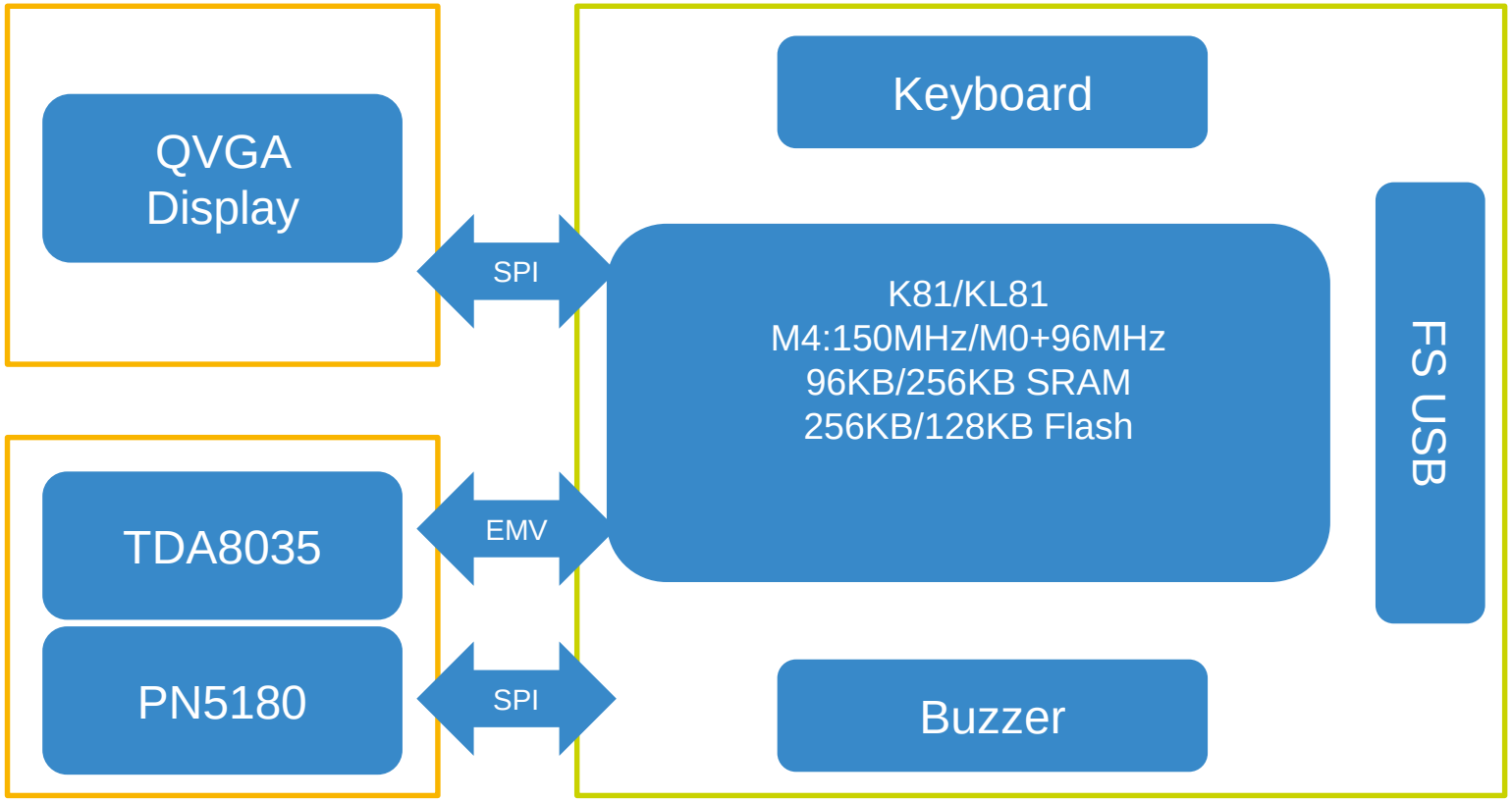
K81 POS Solution





- K81 Secure Micro w/ Tamper and Crypto
- PN5180 NFC CL Reader
- TDA8035 CN Reader
- Secure Capacitive Touch (by Cirque) Pin Pad
- Production Quality Software EMVCo L1 and L2
- Production Quality Documentation
- Great OOB Experience
- PCI 4.x and EMVCo Pre-certifications

TWR POS Demo


QVGA
Display
SPI
Keyboard
K81/KL81
M4:150MHz/M0+96MHz
96KB/256KB SRAM
256KB/128KB Flash
FS USB
TDA8035
EMV
PN5180
SPI
Buzzer


TOWER

PN5180 – Technical Product Features

Characteristics

- RF driver current up to 250mA
- Dynamic Power Control DPC
- Adaptive modulation waveform control
- RF driver supply voltage: 2,7V…5.5V
- Host interface: 1,8V or 3.3V
- Flexible low power card detection
- 4 Multi purpose Outputs‘s (only on TFBGA)
- HW support for EMVCo EMD handling
- 13.56 MHz RF clock generation from external 8, 12, 16 and 24 MHz source
- Overheat protection
- Operating temperature range: -30…+85° C

Interface to Host

- SPI up to 7Mbit/s
- IRQ and BUSY signal for improved host communication

Supported RF Protocols

Reader/Writer mode

- ISO/IEC 14443 A&B R/W support up to 848 kbit/s
- FeliCa R/W support
- R/W support for MIFARE 1K, 4K
- NFC Forum tag type 1,2,3,4,5 reader
- ISO/IEC15693 reader (I-Code SLI)
- ISO/IEC 18000-3M3 reader (I-Code ILT)
- EMVCo 2.3.1 and 2.5 compliance (L1)

Peer to Peer mode

- Passive-Initiator / Passive-Target
- Active-Initiator / Active-Target
- P2P supported for types:
  - A (106 kbit/s)
  - F (212,424 kbit/s)

Card Emulation

- ISO/IEC 14443A (up to 848 kbit/s)
- Active Load Modulation

Packages

- HVQFN40 and TFBGA64
- Part removal detection (PRD, only on TFBGA)

TDA8035

Customer Benefits

- Integrated DC DC converter
- EMV4.3 compliant, NDS certified
- Very low power consumption in shutdown
- Chip select mode for parallel cascading

Target Market

- STB, Payment terminals (POS)

Supported Cards

- 5V, 3V, 1.8V cards supported
- Synchronous cards

Standards

- ISO7816-3
- EMV level 1 compliant

Features

- Supports 5V 3V ,1.8V smart cards
- Thermal and short-circuit protection on all card contacts
- Enhanced ESD protection on card side (10kV)
- 3 specific protected half duplex bidirectional buffered I/O lines (C4, C7 and C8)
- Automatic activation and deactivation sequences
- Voltage supervision on VDD
- De-bouncing on card insertion/extraction
- DC-DC converter with capacitor
- Supply voltage from 2.7V to 5.5V
- Current limitations on Vcc,,I/O, RST, CLK on each slot

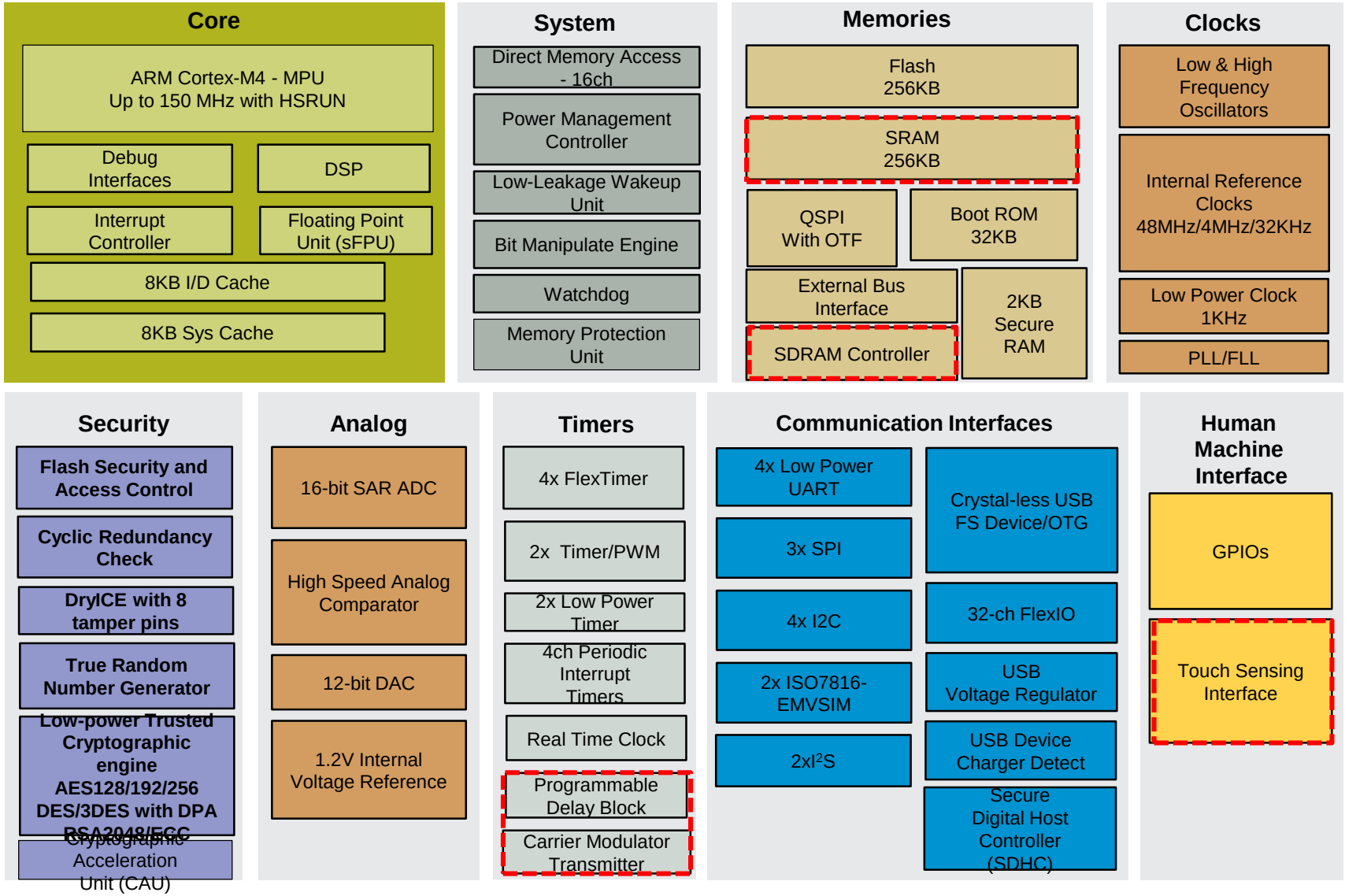
Interfaces

- GPIOs for control
- Transparent I/O lines for card communication

Package

- HVQFN32

K81



Packages

121MAPBGA 8x8x1.4/0.65mm
100LQFP 14x14x1.4/0.5mm

Temperature

-40-105C

Features Highlight

Cortex-M4 with 8KB I/D-Cache
FPU and MPU , BME
up to 256KB Flash,
up to 256KB SRAM
QSPI Flash interface
QSPI Flash interface with OTF
True Random Number Generator
Crypto acceleration MMCAU
160B(32B+128B) Secure RAM for Key storage
Enc. Engine (DES/3DES/AES/RSA)

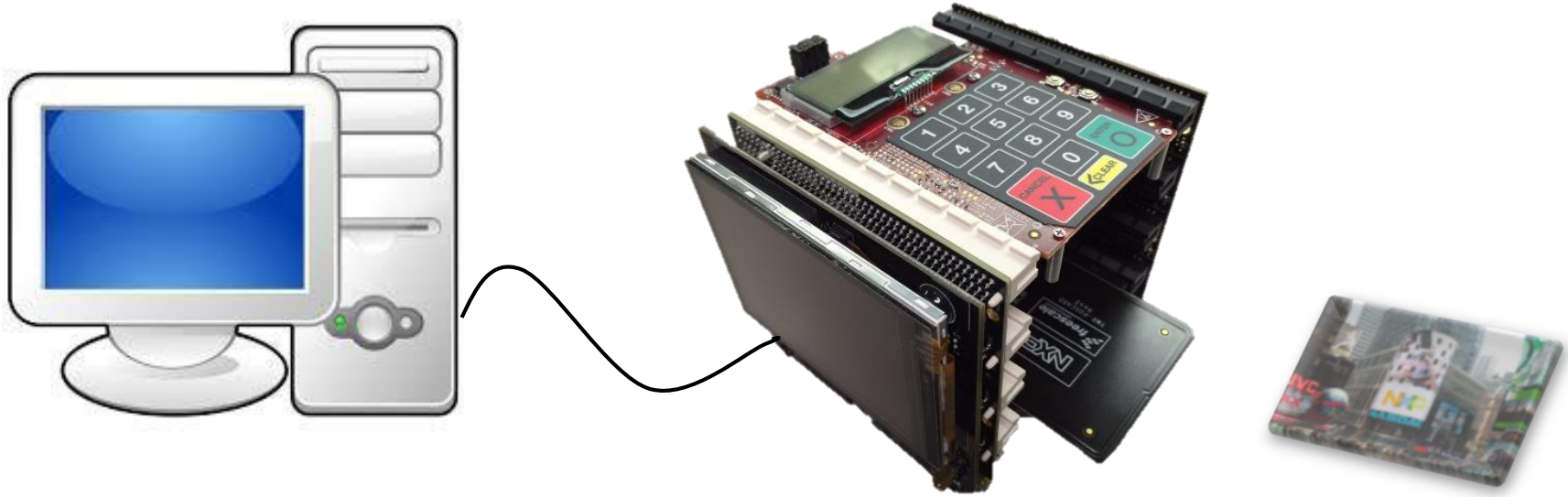
- RSA2048 support (3 decrypt and 1 encrypt <750ms)
- ECC: ECDSA and ECDH for up to P256
- DES/3DES with HW DPA
- AES256/192/128 with DPA

Up to **8** Tamper Pins
Independent Real-Time Clock (RTC)
2x EMV compatible ISO7816-3 interfaces
Crystal-less USB Device
32-ch FlexIO

Solution Outlook

- The solution includes HW and SW fundamentals for a secure payment terminal with all L1 layers and necessary peripherals (secure keypad, display) to implement the transaction layer EMVL2.
- EMVL2 stacks and payment application can be implemented by 3rd party partners or customers themselves

Payment Server simulator



SOLUTION ROADMAP

Payment Solutions Roadmap

Subject to Change

Solutions

Reader

Linux POS Reader: Integrated CT / CL, advanced GUI

Launch at FTF 2016

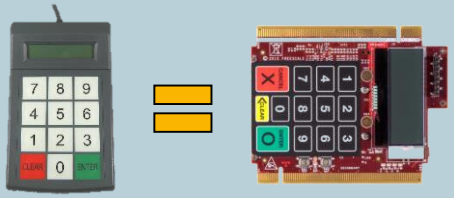
K81 POS Reader

Android POS Reader: Integrated CT / CL, advanced GUI, QR Code

Launch Nov at Trustech 2016

KL81 mPOS Reader w/BLE,MFI or USB

PINPad



K81 Secure Touch PINPad

Secure Card Reader + Integrated Secure QR Code

KL81 Cost Reduced Secure Touch PINPad

Capabilities

CL / CT — CL-1.25W NFC — CT-EMVCo 4.3 — CL-1.75W NFC

PCI3.x — PCI4.x — DPA — Cortex A7 — Multi Core — PCI 5x?

PCI3.x — PCI4.x — DPA — Asymmetric Crypto — NFC Integration — QR Code — PCI 5x?

KSDK — DPA — EMVCo L1 — EMVCo L2 — Linux CT/CL Stack

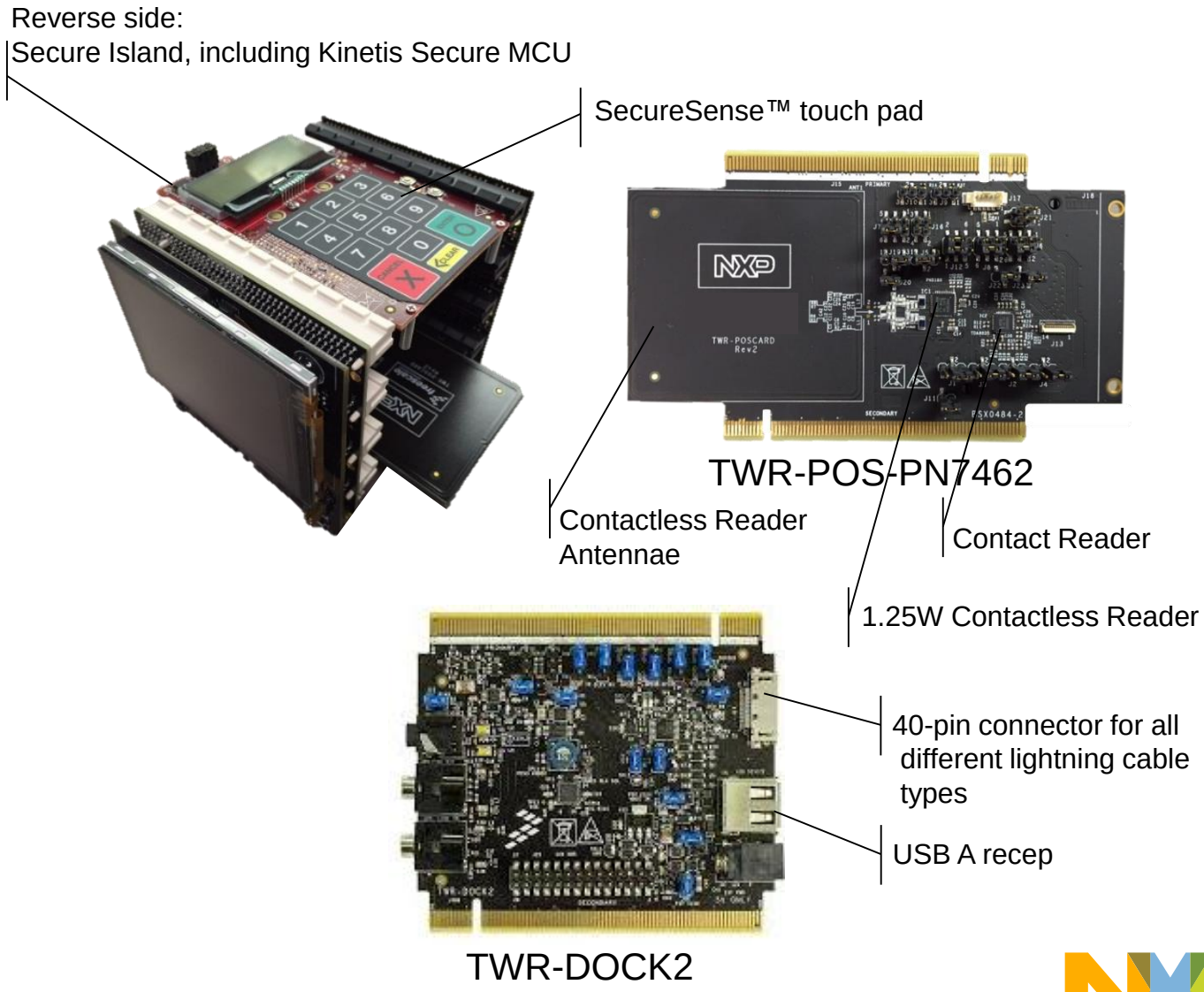
2015 | 2106 | 2017 | Future

Foundational IP Development

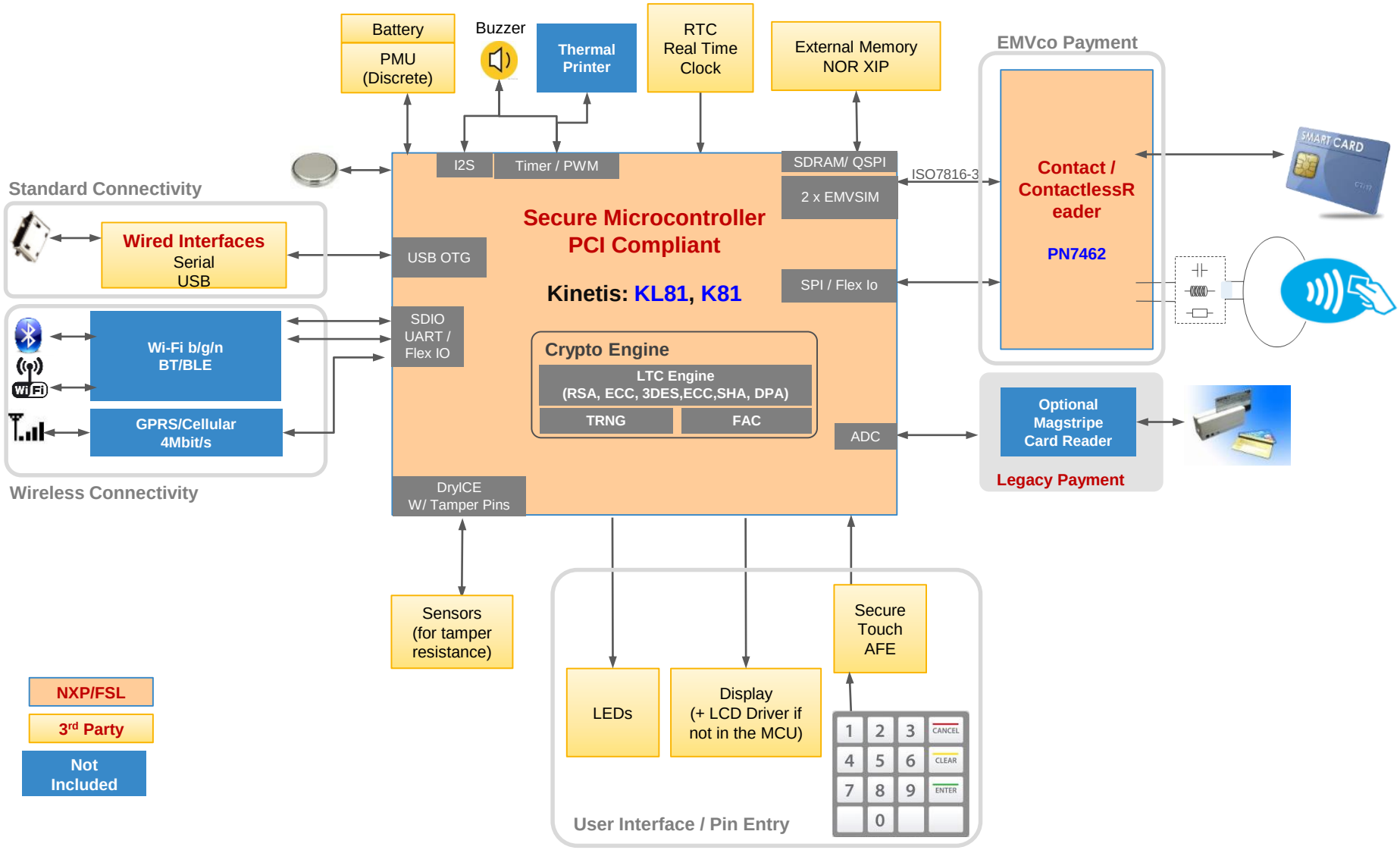
Secure MCU | Secure MPU | Reader | Software

Mobile Point of Sale (mPOS) Reader Solution Overview

- mPOS Reader Reference Design for applications requiring Payment Card Industry certifications
- NXP PN7462 Contactless/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:**
  - mPOS Terminals, Contact & Contactless, which connect to standard smart phones and tablets
- **Availability:** Launch Nov ‘16



Mobile Point of Sale (mPOS) Reader Solution Architecture



Future Linux Point of Sale (POS) Reader Solution

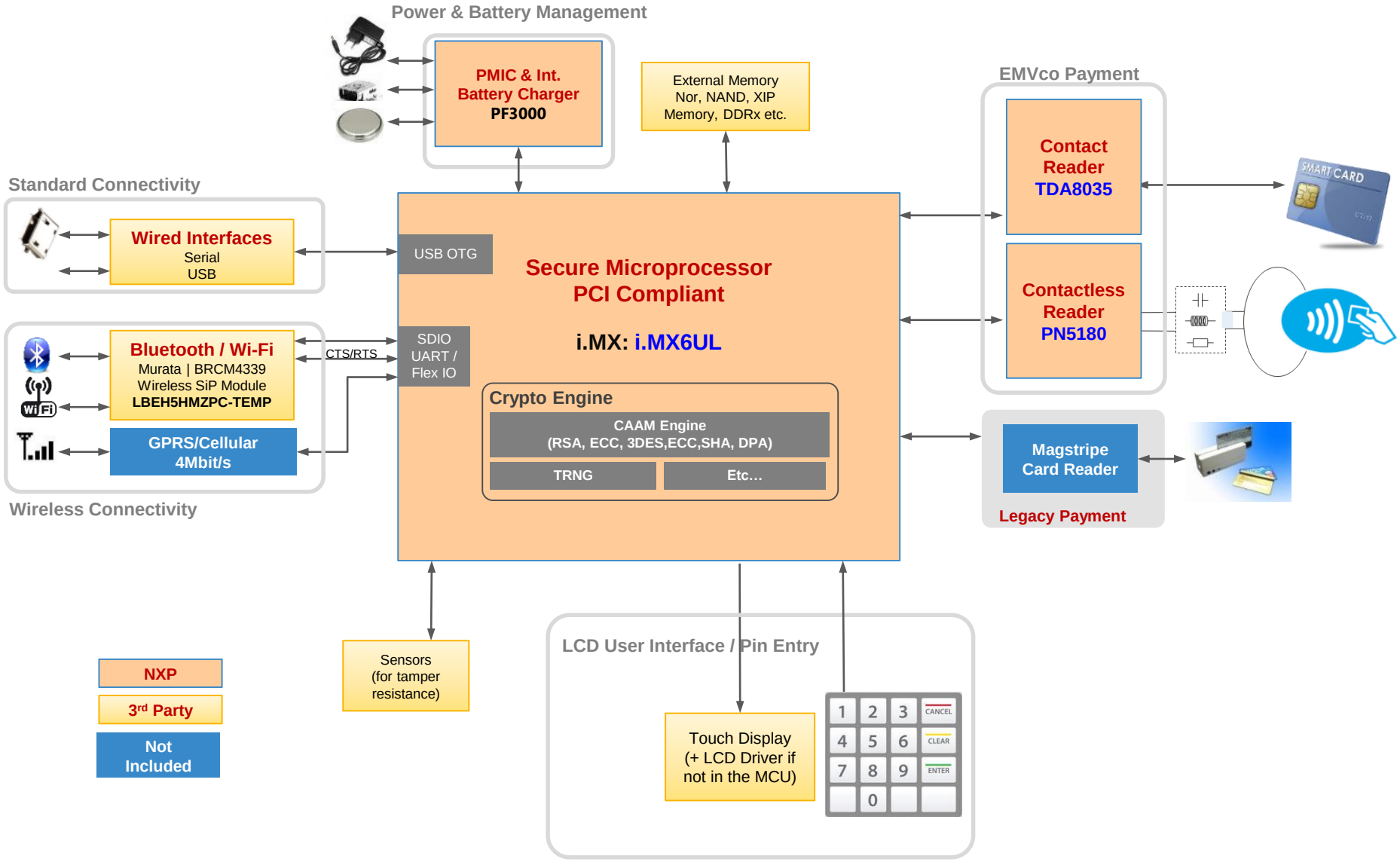
New i.MX6UL TWR w/WiFi BT/BLE

TWR-POS-PN5180

TWR-LCD-RGB

4.3” touch
480x272 RGB

Linux Point of Sale (POS) Reader Solution Architecture



THANKS FOR ATTENDING!

NFC TECHNOLOGY HUB

Your source for everything NFC

www.nxp.com/nfc

- Latest NFC technology news
- Latest product news
- Technical NFC Community
- Downoads
- And more to discover...

SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT