Speed Design and Certification of EMV Payment Acceptance

Ingenutec Module Based on NXP Point-of-Sale Reader Solution

The way we pay for goods and services is undergoing dramatic changes. The trend towards self-serve economy and unattended payment kiosks is driving the need for manufacturers to integrate cashless payment into their products. One of the leading providers of payment terminals, Ingenico, has seen 200% year-on-year growth[1] in unattended payment solutions. At the same time, consumers are expecting merchants to always accept card or mobile payments, regardless of how large or small the merchant or transaction amount. This has also given rise to simpler, more cost-effective solutions in the traditional fixed point-of-sale (POS) terminal. At the same time, more and more consumers are equipped with EMV chip cards and mobile phones with payment capabilities that further drive the pay anywhere, pay anytime experience of secure cashless payments.

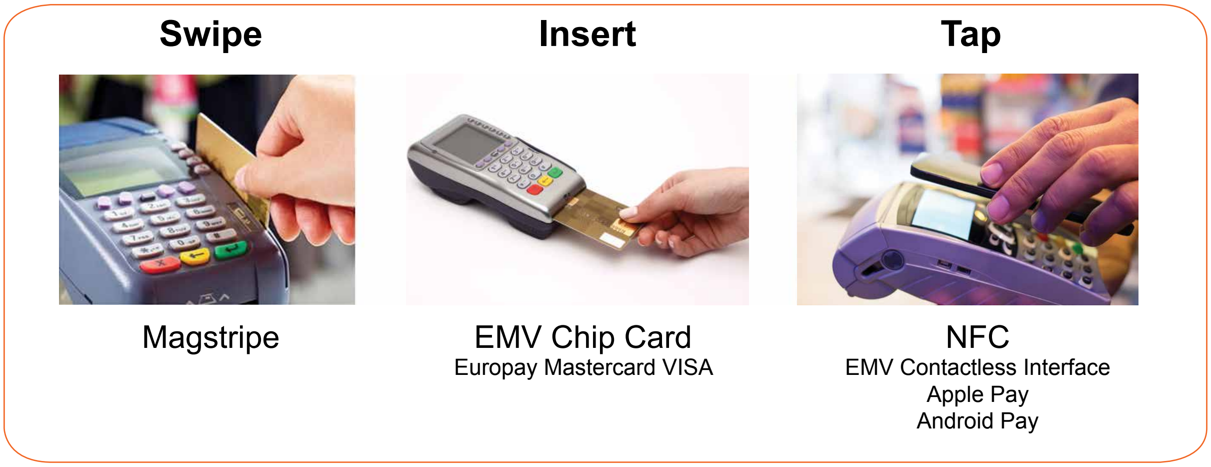
Point-of-sale terminals have typically been the domain of large, specialized manufacturers who develop and certify these products to global payment standards to ensure security and interoperability. Now however, many manufacturers of products, like kiosks, that offer a self-service experience want to include such hardware and software to support, secure cashless payment. At the same time, new companies designing mobile point of sale (mPOS) and Smart point of sale (SmartPOS) devices must also meet the same stringent security and certification requirements as those of traditional stationary attended POS terminals.

[1] https://www.ingenico.com/press-and-publications/press-releases/all/2017/01/ingenico-group-achieves-rapid-growth-through-expansion-of-unattended-partner-program.html

INGENUTEC
NFC: we just make it work | ingenutec.com

This white paper offers a background and reference of the applicable standards as well as design recommendations for manufacturers seeking to integrate POS capabilities into their products. NXP is a leader in secure payment technology across payment terminals, mobile payment and payment cards as well as the co-inventor of Near Field Communication (NFC) Additionally, this paper will introduce NXP's integrated hardware and software certified solution (SLN-POS-RDR) implemented, by Ingenutec, an NXP Independent Design House. Ingenutec specializes in NFC and EMV technologies and offers IP and design services in the form of a POS Module (POSMOD). The POSMOD is an EMV Payment System on Module leveraging NXP IP. This module permits ODM manufacturers to accelerate the integration of cashless payment acceptance into their devices with a minimal amount of custom hardware and software design, while reducing technical risk and facilitating compliance with mandatory certifications required by the payment ecosystem.

Payment Acceptance Methods and Technologies



Swipe

Insert

Tap

Magstripe

EMV Chip Card
Europay Mastercard VISA

NFC
EMV Contactless Interface
Apple Pay
Android Pay

EMVCo Standards for Security and Interoperability Underpin Move to Cashless

Payments for goods and services is steadily increasing to digital payment methods over cash, at a CAGR of nearly 10% globally[2]. Card use and mobile payments continue to increase across the globe as does mobile payments as the infrastructure to support contactless and in-app payments continues to develop. At the same time, data breaches like that of Equifax or Target in recent years have made merchants more aware of the need to ensure transaction and personal data security. The global movement toward secure pay anywhere, pay anytime cashless payment is supported by merchants, manufacturers, credit card issuers and consumers alike.

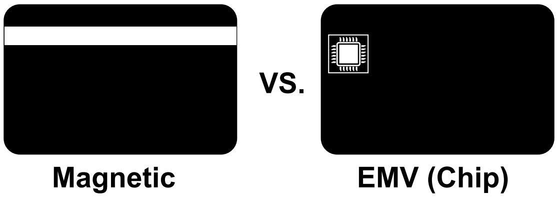
EMVCo was formed in the early 1990s by the major credit card issuers to help ensure global interoperability and establish regularly reviewed security certifications. EMVCo is named for original founders: Europay, Mastercard and VISA but now also includes American Express, Discover, JCB and UnionPay. As an independent body, EMVCo drives technical specifications as well as testing and certification criteria of hardware and software for secure microcontroller cards, mobile payment devices and point-of-sale terminals. All EMVCo specifications and the required approval process for cards and readers can be found at www.emvco.com.

One of the last countries to convert to EMV transactions was the United States. As of October 2016, the US shifted liability for fraudulent transactions made with non-EMV cards from the issuer to the merchant. At the same time mobile manufactures Apple, Google and Samsung introduced their contactless payment methods. Merchants began upgrading payment terminals to accept EMV cards for chip and PIN transactions as well as often incorporating NFC to accept contactless EMV mobile payments.

[2] CapGemini World Payments Report 2016

In parallel, cashless and contactless payments were taking over historically coin-based payments as well. Laundromats, parking meters, toll booths, car washes, vending machines, electric vehicle charging stations, and transit stations are just a handful of the unattended point-of-sale products which are now accepting contactless payments. Similarly, retail and service industries providing mobile and roaming in-store unattended checkout or the use of mPOS and SmartPOS devices in the hands roaming sales assistants is improving the shopping experience.

EMV Liability Shift Forcing out Magstripe



Magstripe: Trivial to counterfeit
Chip Card: Very strong encryption

Liability Shift Dates by Card Brand

	Mastercard[1]	Visa[2]
POS	October 2015	October 2015
ATM	October 2016	October 2017
AFD	October 2017	October 2020

Issuers: Mandates Chip (EMV transactions or merchant pays for fraud

Results:

EMV virtually eliminates fraudulant card present transactions

Payment Acceptance Integration: Build vs. Buy

For manufacturers seeking to add payment convenience to their products, a typical route to market is to purchase and integrate a third-party POS terminal into the product. Often, this is a substantially higher cost when compared to the actual bill-of-materials (BOM) for the terminal alone. Additionally, the continued support and maintenance of the terminal software and drivers by the terminal supplier are a concern. Manufacturers therefore generally prefer to build the complete product and control the software Intellectual Property (IP).

However, the development of secure, payment terminals is complex. A payment terminal product must undergo testing in a specialized lab and pass a battery of tests to ensure the product meets the applicable security, performance and interoperability requirements as established by the certifying authorities. Until the tests are passed, the device will is not approved for use in the EMV based financial system. Failure to adequately address the requirements imposed by the tests and standards at the beginning of the project will generally result in substantial difficulty passing the tests at the end of the project or a redesign to achieve compliance. This prevents many ODMs from moving forward with their own designs.

Not only do terminals need to pass the functional and security requirements of EMVCo, but also need to be compliant with the Payment Card Industry (PCI) security standards. Protecting customers' credit card information, as well as that of the financial institutions which issue and process the payments, is the mission of the PCI Security Standards Council founded in 2006 by AMEX, Discover, JCB International, Mastercard and VISA. Since certification is at the core of successful payment acceptance product development, it is paramount that the certification process and applicable standards are understood at the product's inception.

[1] https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/liability-shift.jsp

[2] file:///C:/Users/nxp40634/Downloads/merchant-emv-chip-faqs.pdf

Contact EMV L1 and Contact EMV L2 Product Approval Process

EMV cards address the low security of magstripe cards and are available in both contact and contactless formats. Contact cards require insertion into the reader which communicates electrically with the card via the metal contact plate visible on the front of the card. The specifications governing the mechanical, electrical, and low level digital protocol specifications comprise what is referred to as the EMVL1 Contact Specification and are defined in Book 1 of the EMV ICC Specifications for Payment Systems. A contact card reader (also referred to as Card Acceptance Device) must be tested by an EMV-approved lab and certified to be compliant with EMV L1 standards according to EMVCo's published Terminal Type Approval (TTA) Process. After a product has successfully passed EMV L1, a Letter of Approval (LOA) is issued for that product.

The scope of Contact L1 specifies the reader's interaction from insertion, up to the point where the smart card's application is selected. The procedures necessary to complete a transaction are specified in EMV Book 3 Application Specification, which refers to additional specifications that prescribe behavior of other components of an EMV compliant reader including security, key management, and interface requirements. These specifications are commonly referred to as Contact EMV L2 specifications. The embedded reader software which implements Contact EMV L2 is referred to as a EMV L2 Contact Kernel. A separate Type Approval (TA) session must be successfully conducted at an EMV-approved lab to certify contact EMV L2 compliance, which results in a Contact L2 LOA.

Contactless EMV L1 and Contactless EMV L2 Product Approval Process

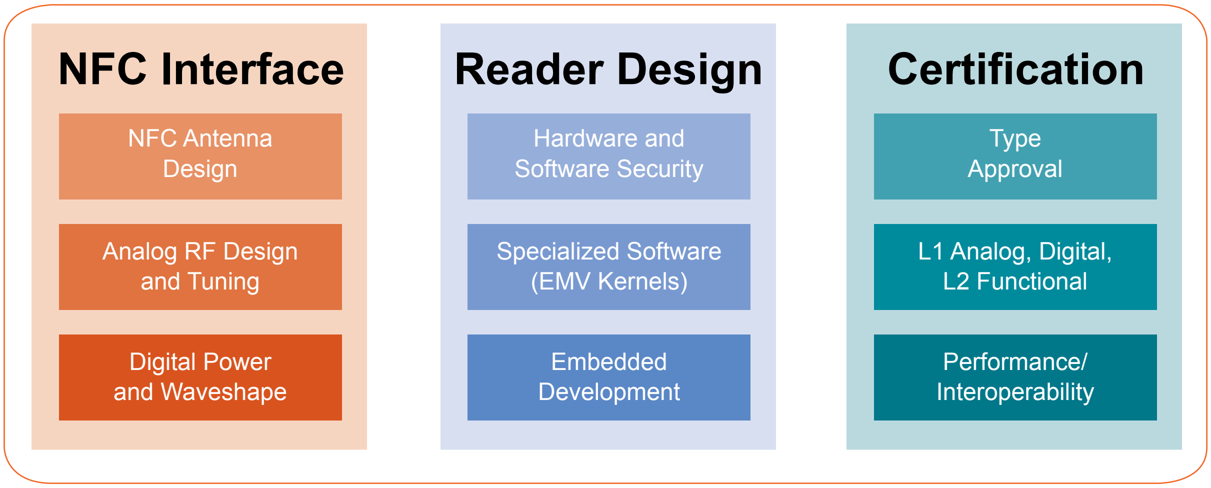
Contactless cards use ISO 14443 communication protocol designed to work at short distances, less than 4cm. Contactless EMV card specifications borrow heavily from the Contact specifications. A simplified model of a contactless EMV card is one in which the metal contacts are replaced with a contactless interface.

A contactless card tap-to-pay transaction provides a user experience which is typically faster and more convenient than a contact card. Also, the card is never out of the user's hand. This is the same principle used with mobile payment via Near Field Communiction (NFC). In this case, the phone emulates the particular card selected by the user in the phone's wallet app.

As was the case for EMV Contact devices, manufacturers must successfully pass separate tests validating compliance with Contactless EMVL1 and Contactless EMVL2 Specifications and receive the corresponding Letters of Approval (LOAs) before they can be deployed. However, achieving Contactless L1 and L2 compliance is substantially more difficult.

First, since communications between a contactless reader and card (or smart phone) is via ISO1443 instead of electrical contacts, the Contactless Level 1 specification is more complex. The addition of an NFC reader interface adds a layer of complexity to the design that significantly impacts the level of effort required for a product to pass Contactless EMV L1 TA when compared to the simple electrical interface of a contact card.

"Why is this so Hard?"



NFC Interface

NFC Antenna Design

Analog RF Design and Tuning

Digital Power and Waveshape

Reader Design

Hardware and Software Security

Specialized Software (EMV Kernels)

Embedded Development

Certification

Type Approval

L1 Analog, Digital, L2 Functional

Performance/ Interoperability

At the very beginning of the product's inception, the contactless reader's antenna design, location within the device, proximity to metal or other radio-frequency (RF) generating components (e.g. batteries and displays) must be considered. These considerations in a Smart POS design, which essentially combine a smart phone with an EMV reader in the smallest possible package, are especially challenging. It is not uncommon for first-time NFC designers to "complete" a product, only to discover after spending many expensive hours "tweaking" the design in the test lab, that the only option to achieve compliance is a costly re-spin of the hardware.

NFC performance is fundamentally an RF design challenge. Achieving acceptable NFC RF performance requires careful attention to the tedious tasks of impedance matching, tuning and optimization of the NFC front-end configuration. Even when following best practices, optimized RF designs virtually always require iterative testing and tuning to reach a "sweet spot" in performance across a variety of competing metrics. For NFC, these include RF power, signal integrity (overshoot, undershoot, modulation depth, etc) and positional performance. By way of example, contactless L1 testing measures power output, waveform and digital performance at a variety of distances and locations relative to the antenna's center. Increasing power to pass at the maximum distance of 4 cm can cause the test to fail at 0 cm for excessive power or waveform distortion. In addition, to assure a consistent user experience, these tests are performed using a variety of contactless cards and mobile devices. The make and model of the cards and mobiles are confidential to the test lab, making it impossible for a manufacturer to perform the same tests in their own lab. It is important not to underestimate the difficulty in passing EMV L1 for contactless.

Similarly, Contactless EMV L2 certification has its own challenges. For contact readers, there is only one kernel for EMV L2. The specifications for the contact kernel is mature and stable. In the contactless case though, each of the major credit card issuers maintains their own unique proprietary secure transaction applications which evolved from legacy implementations that pre-date EMVCo.

For a reader to accept Mastercard, VISA, Discover and AMEX it must implement four different Contactless EMV L2 Kernels; one for each issuer. The reader must also pass all the unique tests specified by the issuer. Consequently, unlike contact L2 approval, which only requires one TA, a separate contactless L2 TA is required for each card type that the reader will support. To submit a reader for contactless L2 TA, a manufacturer must have first passed contactless L1 TA and received an L1 LOA. The manufacturer must also provide a device test environment (DTE) which conforms to the issuer's specifications. The DTE configures the reader for each test case that will be executed during TA and is unique to the issuer.

To illustrate the complexity of the test process, Mastercard TA requires that a reader pass functional tests, performance tests, combination tests and integration tests. There are over 2,000 unique functional tests alone requiring dozens of different configurations which the DTE must support and the reader must pass. Performance tests measure the products ability to process transactions within times measured in milliseconds. These tests are performed using a variety of cards and mobile devices which cannot be disclosed to the manufacturer. Failing a test during TA essentially requires a restart of the TA session. For a company embarking on its first-time certification the learning curve is generally costly and inefficient.

PCI Security Compliance

In 2013, an attack and breach of their POS terminals caused retail giant, Target to inform 110 million credit/debit-card shoppers, who made purchases during the busiest shopping season of the year, that their personal and financial information had been compromised. The attack successfully exploited vulnerabilities in Target's intranet to infiltrate Target's servers and installed "RAM scraping" malware on the POS terminals. This malware collected and forwarded cardholder data to the attackers, using Target's own network. Other, less public security breaches of POS systems have involved gaining physical access to POS devices and installing snooping hardware to retrieve cardholder account numbers, PIN codes and other sensitive data.

PCI has published standards for protection of cardholder devices for Payment Application Software Developers (PCI PA DSS), merchants (PCI DSS) and manufacturers of POS Pin Entry Devices (PCI PTS).

According to PCI:

> “PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PTS standards include PIN Security Requirements, Point of Interaction (POI) Modular Security Requirements, and Hardware Security Module (HSM) Security Requirements. The device requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved.”

The security requirements defined in PCI PIN Transaction Security (PTS) Point of Interaction (POI) provide vendors with a list of all security requirements against which their product will be evaluated in order to obtain PCI approval. To obtain PCI approval, the manufacturer submits physical samples and extensive technical documentation to a PCI Assessor, who through both technical analysis and active efforts attempts to attack the device and defeat its security architecture. These attacks can exploit hardware, software or network vulnerabilities. The device is assessed in the areas of physical security, logical security, PIN security, integration with the POS terminal, network (open protocols), configuration management and secure reading and exchange of data.

Achieving PCI certification is another gate that any POS reader must pass through before the product can be deployed to process credit card transactions. As is the case with NFC, the PCI security requirements impose constraints on the hardware design, which if not considered up front could prevent a product from achieving compliance. The security architecture of the hardware and software must assure that requirements are met. To accomplish this, a secure processor with hardware tamper detection is required. Hardware encryption that is resistant to side channel analysis and secure storage of user data - preferably encrypted, program storage, are some of the hardware support features which aid in achieving compliance.

Ingenutec’s Solution

Ingenutec is an NXP Independent Design House specializing in NFC. The engineers at Ingenutec, whose tag line reads “NFC: we just make it work” have been engaged in providing engineering design services and consulting in NFC hardware and software for over 10 years. Ingenutec assists companies that are struggling to get their products EMV certified, and has solved some of the most difficult problems in this area, developing significant experience and strong working relationships with the approved EMV and PCI labs.

Ingenutec is unique in that it is capable of providing NFC consulting on all elements of the design with services ranging from “antenna to app”. Project experience includes:

- EMV L1 compliance on a stand-alone parking meter
- Design and certification of an EMV reader for EV charging stations
- NFC embedded reader for an underwater ROV manipulator
- Architecture development of an NFC stack for a major South Korean handset manufacturer’s custom NFC front end
- Resolving numerous EMV L1 certification issues caused by suboptimal RF designs
- Developing and certifying an EMV L1 stack, an EMV L2 Mastercard kernel and an EMVL2 VISA kernel

Working with a of number OEMs, Ingenutec fills a set of common needs among its clients. Many clients want to add contactless payment to their products quickly and with a high level of confidence in passing the required certification on a predictable schedule. Their clients’ long-term goals were to own the technology, manufacture it and develop the in-house resources required to maintain and enhance it. However, they could not afford the time required to climb the steep learning curve by starting from scratch.

Ingenutec Capabilities: Antenna to App

Antennas	Hardware	Embedded Software	Applications	Certification Services
Design	Architecture	Reader Firmware	Embedded	Pre-Certification
Matching	Circuit Design	Stack Integration	Mobile	EMV L1
Power	PCB Layout	L1/L2 Kernels	Desktop	EMV L2
Performance	Fabrication	RTOS / BareMetal	Test	PCI
Compliance	Validation	Compliance	Customization	FCC

Ingenutec solves this problem by packaging design and certification services with the requisite IP to enable OEMs to integrate EMV payment acceptance directly into their products. By eliminating dependence on a third-party reader, the OEM benefits from lower product costs and reduced risk of obsolescence. Engaging with the OEM at the start of the project, Ingenutec helps the OEM's design team avoid the common pitfalls that lead to compliance test failures and redesign. Ingenutec's experience helps save the client money by avoiding excessively high lab fees caused by unproductive testing and debugging cycles. Ingenutec's methodology assures that the riskiest elements of the design are addressed and validated early in the project when they have the least impact on cost and schedule.

Ingenutec works closely with the NXP IoT & Security Solutions team and therefore had early access to the NXP POS Reader Solution. NXP's POS Reader Solution is a complete POS design that includes hardware, software, certification and documentation. The production grade solution combines a Kinetis® K81 secure MCU, PN5180 contactless NFC reader as well as a TDA8035 contact reader and is preassembled in a Tower® System. From the beginning, NXP committed to achieving all required PCI and EMV certification with the solution. With this commitment from NXP, Ingenutec recognized early on that the NXP solution could serve as the basis for the common needs of its clients.

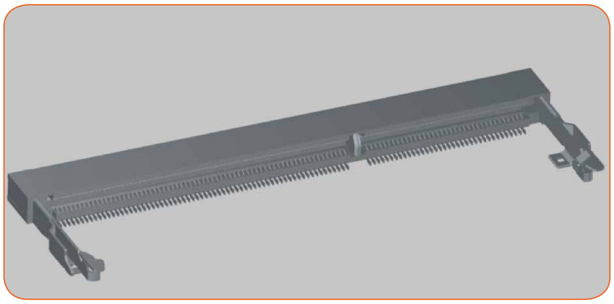
NXP POS Reader Solution

Ingenutec recognized that while the NXP solution serves as a basic reference design, the NXP form factor was not optimal for rapid integration into an existing product and required a fair amount of design to minimize the size and component count.

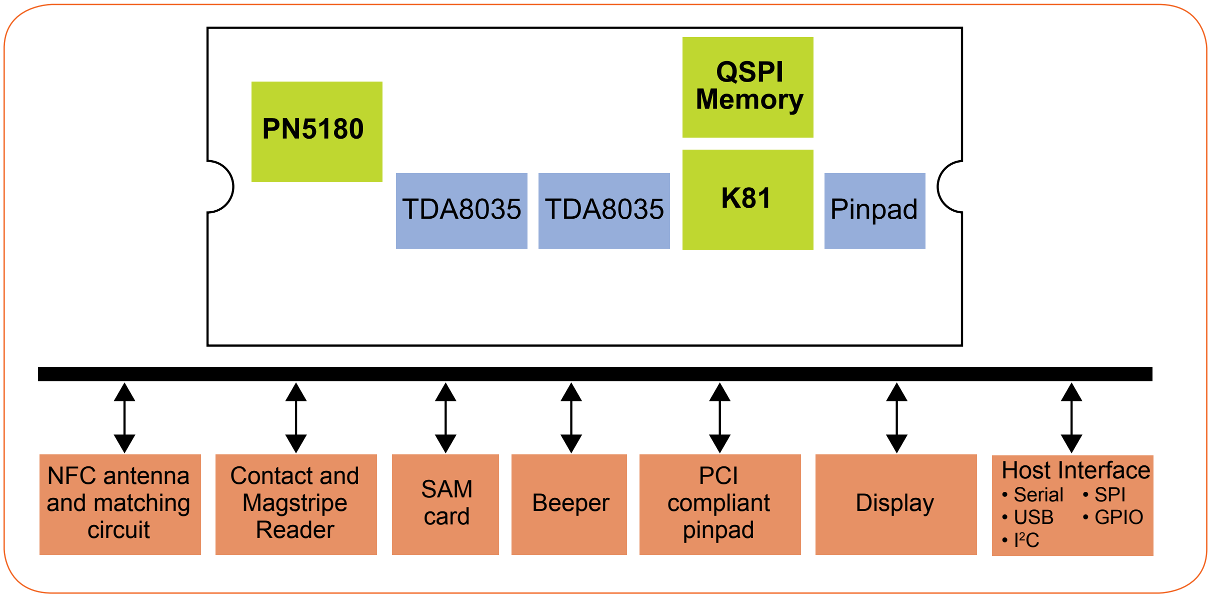
To address this need, Ingenutec partitioned NXP's POS Reader Solution into two sections. One section included the components that were required for all readers, including the K81 Secure Processor, QSPI program store, the PN5180 NFC front end, smart card controller and PIN pad controller. Then they created a module that uses a standard SODIMM memory connector and PCB footprint used in laptops. This choice yields a module with a small footprint, that is easy to integrate and uses a low-cost connector which is available in high volume.

Ingenutec POS Module (POSMOD)

$3 SODIMM POSMOD Connector



For any NFC payment terminal, the location and design of the antenna, buzzer, LEDs, smart card slot, etc. are dictated by the OEMs product form factor and use case. Consequently, these were excluded from the module's BOM to be customized as appropriate.

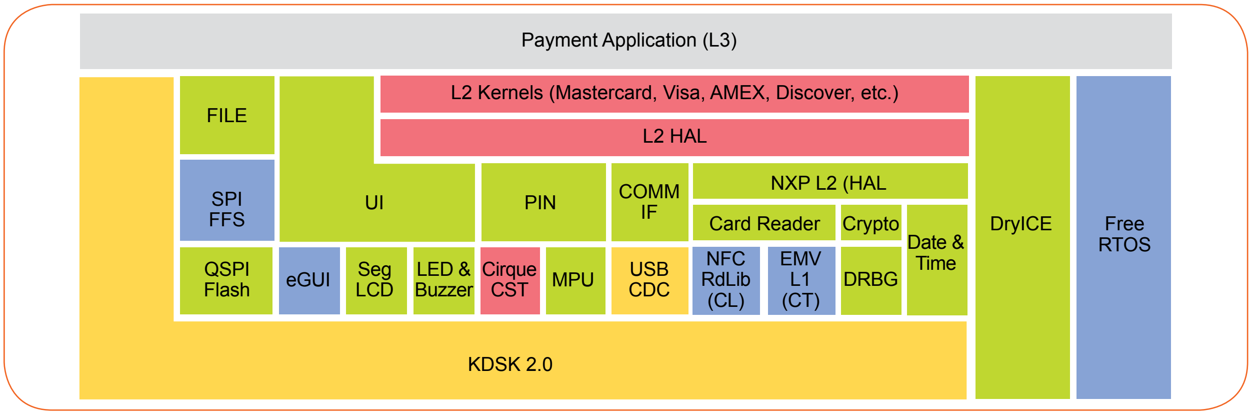


The POSMOD gives customers a jump start with hardware integration. It is a proven debugged hardware design that can be used as is, implemented at the schematic level on an OEM's controller board or modified as required. By integrating multiple PCBs and interconnects from the NXP platform into a single module and removing the product dependent components from the schematic, it facilitates the rapid development of prototypes that work the first time.

Perhaps even more important are the benefits accrued by the combination of Ingenutec's experience in certification of new designs with NXP's previously certified design. Leveraging a previously certified design means starting with a foundation that has already demonstrated compliance with the requirements. Real-world experience taking products through test labs and interacting with their staff helps Ingenutec avoid delays and obstacles experienced on prior projects.

As mentioned previously, PCI compliance requires documenting the security architecture in sufficient detail for the assessor to determine how vulnerable the product is to physical, network and software attacks. Developing this documentation is a significant undertaking. Similarly, bringing the PCI assessor up to speed on the security architecture takes time. Both of these activities have significant impact on the development budget and timeline. As an NXP Independent Design House, Ingenutec can leverage the preassessment documentation and prior knowledge of the assessor to reduce the OEM's certification costs.

While designing the POSMOD, Ingenutec maintained 100% software compatibility with the NXP Solution. Consequently, all Ingenutec designs can leverage the Reader Solution SDK and development tools. The SDK is a rich foundation of pre-certified software including an EMV L1 compliant contact and EMV L1 compliant contactless software stack.



The NXP SDK was designed to support the integration of third party L2 kernels via an L2 Hal. Ingenutec performed this integration and licenses to its ODMs pre-certified EMV L2 Contact and Contactless kernels for all the major credit card brands. They also provide a device test environment which the test labs are already familiar with; therefore, reducing the technicians' learning curve. As with PCI, EMV Certification is also facilitated by leveraging the NXP Payment Solution's pre-certified code and again results in certification with significantly less development effort.

Software development and customization services are provided by Ingenutec and implemented using NXP's Kinetis Design Studio (KDS). KDS is Eclipse based and provides full support for developing and debugging software on the NXP POS architecture.

In keeping with its goal of facilitating fast track NFC designs for its clients, Ingenutec licenses IP and provides training to its ODMs to help them maintain and support the product during its lifecycle.

Summary

Whether in attended and unattended environments, the need to accept contact or contactless EMV based payments is growing. Designing a POS product and achieving the required certifications is a complex process. Many ODMs see the ownership of the design as offering greater flexibility and cost-savings in product design.

Ingenutec responded to this need and packages design and certification services with the requisite hardware and software IP to enable OEMs to integrate EMV payment acceptance directly into their products. To jump start this process they developed a POS System on Module (POS-SoM) based on the pre-certified NXP POS Reader Solution. By eliminating dependence on a third-party reader, the OEM benefits from lower product cost and reduced risk of obsolescence.

The combination of NXP's proven hardware and software solution with Ingenutec's design services and certification experience help bring products to market faster. OEMs can benefit with the same design ownership as an in-house program, but save time developing NFC and EMV expertise in the the product development phase.

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXPHalbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Semiconductor
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014 or +81 3 5437 9125
support.japan@nxp.com

Asia/Pacific:
NXP Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

Ingenutec, LLC:
Ingenutec, LLC
10629 Hardin Valley Rd, #194
Knoxville, TN 37932
+1-865-405-5695
www.ingenutec.com