# Payments: POS, mPOS & Mobile payments

Gorka Hernando (Speaker) / Eric Leroux (Host)

### Webinar Instructions

- Audio settings:
  - You are in "listen only" mode due to possible background noise
  - Set Mic & Speakers option (headset + external mic advised)
- For questions:
  - Write them in section "Questions" of your GoToWebinar panel
  - The Host will receive and compile them for the Q&A time
- Materials will be made available to you
  - (please check email after the session with the address)
- The session will be recorded for on-demand viewing
  - · (please check email after the session with the address)
- Please answer the evaluation questions after session

#### Scheduled Sessions for 24/07/2015

10:00 am - 11:00 am CET 5:00 pm - 6:00 pm CET







## Payments: POS, mPOS & Mobile payments Public

MobileKnowledge July 2015

## Agenda

- Introduction to payments
  - Payment transactions, EMVCo, PCI
- Introduction to POS, mPOS market
  - POS, mPOS definition
  - Market view, trend
- ▶ The standards for POS/mPOS & Certification
  - EMVCo L1/L2, PCI, Others ...
- ► High level architecture view (main POS/mPOS components).
- NXP product offering for POS, mPOS
  - Contact & Contactless
  - NXP SW stack (EMVL1) & Partners stack (EMVL2)
- NXP POS design kits & mPOS demonstrator
- NFC Based payments
  - Secure Element, HCE, Tokenization, Apple Pay, Android Pay





# **Introduction to Payments**

# Introduction to payments

From bartering to mPayments

- A payment is the transfer of an item of value from one party to another in exchange for the provision of goods, services or both, or to fulfill a legal obligation
- Payments are frequently preceded by an invoice and result in a receipt





### **Evolution of "plastic" money**



- Payment data is stored in the magnetic band of the card
- Easy to clone, static data, short life

#### Magnetic Stripe



- Payment data is stored in high-secure tamper-resistant ICs
- Impossible to clone, data can be updated on-demand, long life

#### Chip Card



- Payment data is stored in high-secure tamper-resistant ICs
- Impossible to clone, data can be updated on-demand
- Wireless purchases are completed in a faster and more intuitive way
- ▶ Longer life since no physical connection is needed



- Payment data is stored in high-secure tamper-resistant ICs or in the cloud
- Multiple credit cards can be stored in one NFC Device
- The payment solution is more convenient than ever









#### **Payment transaction**





**Payment transaction** 





## Credit Card based payments EMV Specifications



- EMVCo is currently governed by Visa, MasterCard, Amex, Discover, JCB & CUP
- ► EMVCo books define debit, credit and prepaid payment systems for IC based transactions
  - It facilitates worldwide interoperability and acceptance of secure payment transactions
- ► EMVCo releases specs for contact & contactless IC, common payment application, card personalization and tokenization
- ▶ EMVCo is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders



EMVCo Contact IC Stack

EMVCo Contactless IC Stack

► For more information: <u>A Guide to EMV Chip Technology v2.0</u>





- EMV makes the payment transaction more secure
  - Card authentication: protecting against counterfeit cards
  - Cardholder verification: protecting against lost and stolen cards
  - Transaction authorization: using issuer-defined rules to authorize transactions either offline or online based on security risk analysis
- EMV Fraud Reduction numbers
  - Europe (EMV Continent)
    - ✤ 96% transactions being EMV
    - \* 36% overall drop in fraud over 5 years
    - \* UK fraud drops 69% over five years
    - Fraud basic point drops 25% in France
  - US (only non-EMV G20 Country)
    - \* \$6.1 billion fraud losses in 2012
    - Potential \$44.8 billion fraud losses over the next 5 years
    - \* EMV migrating costs estimated at \$8.6 billion







Source: EMVCo



### Payment Card Industry Security Standard Council



- ▶ The PCI SSC consists of the five major payment brands: Visa, MasterCard, American Express, Discover & JCB
- ► The main objective of PCI SSC is to foster broad adaption of cardholder security standards
- ► The PCI policies, standards and procedures were developed to:
  - Encompass several separate data security efforts
  - Create a set of security standards that are common to the whole payment infrastructure
  - Ensure a "standard" to protect payment account, transaction and authentication data

## PAYMENT CARD INDUSTRY SECURITY STANDARDS

#### **Protection of Cardholder Payment Data**





# **Introduction to POS / mPOS market**

## Traditional POS Definition

- The traditional POS definition primarily covers traditional desktop solutions and standalone mobile solutions designed to improve POS mobility without the requirement of connecting with another mobile device.
- Traditional POS does not harvest Internet accessibility from other mobile devices. It is traditionally hardwired into a network or has its own integrated Bluetooth and/or Wi-Fi capability or standalone cellular connectivity.
- 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.











- POS devices that require a connection with another mobile device, be it a handset, tablet, or PDA.
- Connections are typically made wirelessly via Bluetooth or physically through a device's audio jack or charger connection.
- ✓ Typically it is the mPOS device where the card is swiped, and the chip is read or a contactless card is tapped on to read the card information.
- There are instances in which the contactless chip is read by an NFC-enabled handset, but most in-part mPOS devices provide a standalone solution for card reading using the connectivity of a handset/tablet to authenticate online.
- The devices themselves come in different shapes and forms, designed to accept the differing types of payments, whether it be chip and PIN, chip and signature, or the swiping of the magnetic strip.
- 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









# **POS / mPOS solutions**

### Key use cases - Applications





## POS

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

## 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







# POS / mPOS solutions

### Market status and forecast

- ▶ By 2018, 90% of the POS / mPOS solutions shipped will support contactless transactions.
- ▶ By 2018, 42% of the POS solutions shipped will be mPOS solutions.







#### POS & mPOS Terminal shipments wwide (Munits)

Source: ABI Research 2014



## **Contactless solutions**

### Growth through collaboration





# **POS / mPOS Certification**

# POS / mPOS solutions

### **Specifications and Certifications**

- Requirements to be EMV Certified
  - Contact & Contactless Level 1, Level 2
- Requirements to be PCI Certified
  - PCI DSS, PCI PTS, ... depending on the device
- ▶ Regulatory certifications (RoHS, FCC, CE, ...)
- ► ISO/IEC 14443 licenses
  - Terminals shall comply to ISO 14443-A & 14443-B patent licensing scheme
  - NXP component cover both patents in ASP
- Certification is completed by independent labs
  - Certifications are performed according to card acceptance schemes
    - Mastercard PayPass, VISA PayWave, Amex ExpressPay, DiscoverZip
  - Certifications need to be done on the commercial product







## **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





## EMV Certification EMV Level 1

- NXP provides EMVL1 stack for contact and contact-less products
- ▶ This stack is accessible under NDA for usage with NXP chipset and it is provided as source code.
  - It has been pre-validated for EMVL1 (4.3 for contact and 2.3.1 for contactless).
  - It is portable on various architectures thanks to the abstraction layers which are integrated in the delivery
- The stack is available with our POS demo kits.

Certification	NXP support	End customer
EMVCo L1 contact analog	Application notes; demoboard; Report from test house	Need to test at certified lab on final device
EMVCo L1 contactless analog	Antenna design guide, loop back example; internal test report; demoboard	Need to test at certified lab on final device
EMVCo L1 contact digital EMVCo L1 contactless digital	Application note; source code; ICS example; internal test report	Need to test at certified lab on final device



## EMV Certification EMV Level 2

- ▶ NXP demonstrates NXP chipset capabilities through reference designs and demonstrators developed with partners.
  - The reference designs and demonstrators are usually pre-validated for EMVCo L1 or L2 compliance and occasionally the partner's hardware can be PCI certified
- NXP initiative aims to reduce TTM at new customers in this POS/mPOS growing market and to develop the infrastructure for contact-less payment acceptance using cards or NFC-equipped mobile phones
- ▶ NXP has setup an EMVL2 partnership with several companies for integration and certification
  - For more information contact NXP marketing team (<u>michel.brun@nxp.com</u>).

Certification	NXP support	End customer
EMVCo L2 contact EMVCo L2 contactless	Link to partners for stack Pre-integration support *	Debug with EMVL2 partners ICS to be defined by customer and stack supplier. Certification on final device

\* Only if NXP EMVCo L1 stack is used



# PCI Certification

### PCI Security Standards Council

- ▶ POS / mPOS terminal requirements to be PCI Certified
  - PCI Data Security Standard (DSS)
  - PCI Pin Transaction Security (PTS) for Point of Interaction (PTS Pol)
- PCI Payment Application (PA)
- PCI Point to Point Encryption (P2PE)

Certification	NXP support	End customer
PCI PTS 4.0	Link to PCI test laboratories or external consultant	Certification

- Additional certifications on the final device may be required
  - Depending on the accepted card schemes

Depending on the region

Certification	NXP support	End customer
Country specific: UKCC, SEPA,		Certification
CEM Regulatory Certification	Guidelines for contactless	Certification
RoHS (Restriction of Hazardous Substances)	Provision of RoHS compliance report of NXP components	Request document from manufacturing entity
MasterCard PayPass, Visa PayWave, DiscoverZip		To be checked with EMVL2 supplier



# **NXP Portfolio for POS / mPOS**

## **POS & mPOS Architecture**





## NXP offers a complete CL/NFC portfolio for POS





## NXP offers a complete CT reader portfolio for POS & mPOS



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



## OM5597/RD2663 POS Design Kit

#### Description

- OM5597/RD2663 is a reference design of a cost effective EMV compliant Point of Sales Terminal based on NXP components. It provides an EMV Level 1 compliant software stack for contactless based on CLRC663 RF frontend as well as contact payment based on TDA8026.
- ▶ Easy integration of NXP components into a cost efficient POS reader.
- Fast development of a certifiable software stack, due to reuse of already EMV L1 certified source files.
- Reusable showcase of closed loop payment, contact and contactless payment card selection as well as NFC functionality.



Reader IC: POS Reference Design Based on CLRC663 & TDA8026 MCU: LPC1768 Orderable part number: OM5597/ RD2663 12NC: 9352 981 91699

URL: http://www.nxp.com/demoboard/OM5597.html

#### Features

- EMVC0 4.3 analogue and digital compliant for contact reader.
- EMVCo 2.3.1 RF and digital compliant for contact-less interface.
- ▶ NFC Peer to Peer communication showcase.
- The user interface composed out of an LCD screen and a keyboard demonstrates the following showcases:
  - Closed loop payment based on MIFARE DESFire EV1 together with MIFARE SAM AV2
  - First steps of contact and contactless EMV payment with JCOP Dual Interface card
  - First steps of payment with a mobile phone including P2P data exchange
- The OM5597/RD2663 board comes together with all design files including the hardware Gerber Files and the software source files.
- One smartcard slot and four SAM slots.

#### **Documentation**

File name	Title	Туре	Date
AN11271	Toolchain information for POS Development Kit OM5597/RD2663	Application note	2014-08-06
AN11270	Hardware description for POS Development Kit OM5597/RD2663	Application note	2014-08-11
AN11269	Software design guide for POS Development Kit OM5597/RD2663	Application note	2014-08-11
AN 11268	Quick startup guide for POS Development Kit OM5597/RD2663	Application note	2014-09-09
SW304011	SW stack and schematics for OM5597/RD2663	Software	2014-10-13
<u>UM10493</u>	POS Reference Design - Firmware description	User manual	2014-04-14





## **mPOS** Demonstrator

#### Description

- The mPOS reference design is a cost effective EMV compliant solution for a mobile Point of Sales Terminal based on NXP components. Supports contactless payments using PN5180 (PN517 in phase 1) and contact payments using TDA8035.
- ▶ Easy integration of NXP components into a cost efficient mobile POS reader.
- Fast development of a certifiable software stack, due to reuse of already EMV L1 certified source files and EMV L2 SW stack available through 3<sup>rd</sup> parties.
- Android demo application available for phone or tablets together with contactless card and enables full contact and contactless payment transactions.



#### Features

- EMVCo L1 pre-certified software stack for contact & contact-less
- EMVco L1 pre-certified RF implementation for contact-less interface
- EMVCo L2 stack available from 3rd party through direct licensing program
- Hardware schematics available for Hardware partner ViewaT
- Antenna design guide available
- PCI evaluation report available
- Android application demo available for phone or tablet





## Target customers for POS / mPOS Reference Design Kits

- ▶ New players in the Payment industry willing to implement a cost efficient payment terminal.
- ► Companies developing a reader with contact as well as contactless payment functionality.
- Reader manufacturers or system integrators including payment functionality into their AFC/Access readers
- Reader manufacturers looking into the NFC showcase in payment or even any other application.
- Service providers aiming at integrating loyalty and mobile payments





# **Mobile Payments**

## NFC-based payments The technology in a nutshell

- Payment data stored in our mobile device
- NFC-enabled mobile devices used as payment cards
  - Proximity communication and difficult to spy (2cm)
- Transactions are carried out in the same way
  - No impact on security
  - Compatible with current standardized infrastructure (POS)
- Advantages of a NFC phone compared to a card
  - Processing power & memory
  - Connectivity
  - User interface
  - Battery





## NFC-based payments Card Emulation configurations

- Secure Element
  - Proven high-secure and tamper-resistant microcontroller in the device
    - \* Same family of product as used mass market solutions: payment cards, e-Passports...
  - A specific IC to handle and store sensitive data
    - \* Non-Volatile Memory, Security CPU, Crypto co-processors
  - Protected through cryptographic keys againsts attacks and tampering
    - Only authorized entities can access the SE
  - Secure IC validated by third parties certification, i.e. Common Criteria
- Host Processor
  - Main processor of the device in which the OS and applications reside
  - Sensitive information is stored in the Host Processor or in the Cloud
    - \* More memory available via host versus secure element
  - Application/service providers and end users get (more) control
  - "more-simple-but-less-secure" card emulation
- ► The NFC Controller forwards each APDU according to its Routing Table







# NFC-based payments

### Tokenization

- Tokenization: replacement of sensitive data with a unique identifier that cannot be mathematically reversed.
- Must be monitored in real time, which always forces online authentication at POS
- PCI mandates PAN's not to be stored on non-PCI DSS compliant devices

PAN	Token	Comment
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

EMV Payment Tokenization Specification (March 2014)





## NFC-based payments eSE Tokenization – Apple Pay

- Virtualized credit cards are integrated into Passbook
- iTunes accounts are automatically transferred. Additional credit cards can be virtualized using the camera.
- When a new credit card is scanned, a unique Device Account Number – token – is stored in the Secure Element
  - The DAN does not change between transactions
  - The DAN is not stored in Apple's servers
  - The Token Service Provider entity knows the PAN DAN mapping
- The transaction cryptogram integrates a one-time dynamic security code unique to each particular transaction.
- A "Touch ID" registered finger must be pressing the home button for additional cardholder recognition





# NFC-based payments

HCE Tokenization – Android Pay

- Android Pay is a set of Android Framework API for in-store/in-app payments and Loyalty applications
- Android Pay is (also) Google's own implementation of in-store/in-app payment and single tap loyalty services
- ▶ Based on HCE, it does not mandate use of a SE.
- Android Pay uses tokenization services of the Payment networks as well as (Android) backend risk management engines to mitigate fraud.
- ▶ Payment tokens used in Android Pay need to be refreshed periodically.
- Android Pay to be available on Android devices with KitKat and higher versions
  - Likely to be introduced around Q3 2015 in the USA.
- ► No modification to existing EMVCo contactless payment infrastructure.
  - Wherever Apple Pay is accepted, Android Pay can be accepted.





# NFC-based payments

### Wearables

- ▶ NFC Wearables will be an essential part of NFC payments
  - Wristbands, Smart Watches, Glasses, Clothes, ...
- Smartphone application to manage the wearable, but not needed during the in-store payment
  - Payment application stored in the wearable itself
- Retail revenue of wearable devices will reach \$19 billion by 2018 compared with \$1.4 billion this year
- ▶ 75% of wearable owners consider themselves "early adopters"



#### Source: ABI Research 2015





# Conclusion

## Payments: POS, mPOS & Mobile Payments Summary

- While contact chip-based credit cards have already gained maturity, contactless and mobile payments are constantly growing
- ▶ POS and mPOS market is expected to grow during the coming years
  - Support for contactless payments is also growing
- Several certifications are mandatory on final devices
  - EMVCo Level 1 & 2, PCI, RoHS, SEPA, UKCC, ...
  - NXP supports customers throughout the certification procedure
- NXP Provides the widest portfolio for the integration of both contact and contactless payments
  - Reference designs available for the best POS terminal deployment
- Mobile payments, either based on the Secure Element or Host Card Emulation, will become more and more popular





## Payments: POS, mPOS & Mobile Payments

Gorka Hernando (Speaker) / Eric Leroux (Host)

# Time for Q & A





## MobileKnowledge Thank you for your attention

We are a global **competence team** of hardware and software technical experts in all areas related to **contactless technologies** and applications.

Our services include:

- Application and system Design Engineering support
- Project Management
- ► Technological Consulting
- Advanced Technical Training services

We address all the exploding **identification technologies** that include NFC, secure micro-controllers for smart cards and mobile applications, reader ICs, smart tags and labels, MIFARE family and authentication devices.





## Payments: POS, mPOS & Mobile Payments

Gorka Hernando (Speaker) / Eric Leroux (Host)

# Thank you for your kind attention!

- Please remember to fill out our evaluation survey (pop-up)
- ► Check your email for material download and on-demand video addresses
- Please check NXP and MobileKnowledge websites for upcoming webinars and training sessions

www.nxp.com/products/related/customer-training.html www.themobileknowledge.com/content/knowledge-catalog-0



