Agenda

► Why MIFARE4Mobile?
► MIFARE in Mobile related technologies
  ▪ MIFARE technology
  ▪ NFC technology
► MIFARE4Mobile technology
  ▪ High level system architecture
  ▪ MIFARE4Mobile 1.01 specification overview
  ▪ MIFARE4Mobile 2.1.1 specification overview
    ❖ MIFARE4Mobile 2.1.1 architecture
    ❖ MIFARE4Mobile 2.1.1 certification
► NXP Products
► Successful implementations
MIFARE and NFC technologies

► MIFARE is the most widely adopted contactless technology on the market today
  - Essential element in public transportation schemes, ticketing systems, loyalty programs, and access management around the world.

► Smartphones are widely used not only for calls but also for gaming, navigation, photos / video recording, …
  - Smartphones share expected to continue growing from 67% in 2014 to > 80% or even higher in the coming years

► NFC technology in smartphones is becoming a commodity
MIFARE in Mobile

- MIFARE in Mobile is MIFARE technology in a Mobile device
  - Users can hold multiple Virtual Cards (VCs) in the same device
MIFARE4Mobile

► MIFARE4Mobile is a technology used to manage MIFARE-based services in NFC mobile devices, from over-the-air installation to end-user interaction via the user interface of the mobile phone.

► MIFARE4Mobile ensures interoperability among different Secure Element form factors (embedded SE, UICC SIM and micro SD) and different vendors.

► MIFARE4Mobile provides the most flexible and scalable platform for transit agencies to make use of their existing infrastructure.

► GlobalPlatform will enable MIFARE4Mobile to co-exist with other applications such as mobile payments.
Global Travelling facilitated by NXP’s MIFARE™ technology

There are more than 150 Million contactless readers worldwide supporting MIFARE® products

5.0 Billion+ MIFARE ICs shipped for more than 40 different applications
Regional and Countrywide e-ticketing schemes

- 1.2 Billion people go to work and return home every day with contactless ticketing using our MIFARE™ technology
  - 736 cities using MIFARE for transport ticketing solutions and 77% market share in transit ticketing worldwide
- 200M+ people rely on NXP technology to enter their offices and hotels every day
More than 40 different MIFARE® application types
MIFARE products

MIFARE Classic
- ISO14443A 1-3 compliant: 106 kbit/s
- Simple fixed memory structure: 1K,4K EEPROM size
- Security: Crypto1 (authentication and encryption)

MIFARE DESFire
- Fully ISO 14443A 1-4 compliant: 848 kbit/s
- 2KB, 4KB and 8KB memory with fast programming
- DES/3DES/3KDES/AES crypto algorithm in hardware
- Memory organization: File system
  - up to 28 applications in a card and 32 files per application
  - up to 14 keys, free, never per application
  - 1 master key for card maintenance

MIFARE Plus
- AES based CC certified IC that provides superior levels of security, performance and privacy, and a migration path from MIFARE Classic
End user requests card to Service Provider.

Personalization done by SP. **SP owns the card and the application.**

**Physical and logical flow follow the same path.**

Relations between stakeholders are clearly established.

Current MIFARE Ecosystem

Contactless Card Issuance
NFC Technology

- 850 million NFC handsets shipped between 2012 and 2014
- > 5 billion NFC handsets will ship between 2013 and 2018
- 3 in 4 mobile phones to come with NFC by 2018
Introduction to NFC

Near Field Communication is a short-range wireless connectivity technology *standard*, designed for *intuitive* and *simple* communication between *two* electronic devices.
NFC enables a new mobile experience

**Card Emulation**

Emulates the behavior of a contactless card.

**Peer to Peer**

Exchanges data between NFC devices

**Read/Write**

Reads / Writes data from any tag or contactless card
NFC – opening new experiences

► “Before” NFC

► With NFC

Screen & Keyboard

Connectivity

Processing Power

Battery

The physical card
Service Provider needs to load the MIFARE application into the SE.

Application owned by SP (logical flow) and SE owned by the SE (physical flow).

Physical and logical flow follow different paths !!

New players modifying the established business model of contactless.
MIFARE in mobile
What is MIFARE4Mobile?

MIFARE4Mobile is a technology that provides mobile network operators, trusted services managers and service providers with a single, interoperable programming interface to remotely provision and manage MIFARE-based services in Secure Elements of mobile NFC devices "over the air" (OTA).

MIFARE4Mobile Industry Group founded in 2010

The MIFARE4Mobile interface specifications are grouped into 3 categories:

- **Wallet / User Interface APIs** for displaying MIFARE content on the handset screen
- **Over The Air / Trusted Service Manager APIs** for OTA installation, operation and revocation of MIFARE products
- **Secure Element Platform APIs** to provide common access to the hardware resources of the MIFARE portfolio
Find all the MIFARE4Mobile information in http://mifare4mobile.org website !!!

- Whitepapers, presentations, specifications, ...

Specifications are licensed free of charge to anyone who wishes to implement MIFARE4Mobile applet on a SE and agreeing to the terms & conditions (Robustness, security, self certification, Non-assert of IPR,...)
MIFARE4Mobile High Level Architecture Overview

Back Office System

Sales

Validation

Transport Operator

End User

Wireless Carriers
Overview MIFARE in Mobile

- Moving from dedicated MIFARE ICs to Secure Elements that hold multiple applications
- SE contains MIFARE Implementation offering MIFARE functionality:
  - **Host Interface** to remotely manage the MIFARE applications and allow information extraction
MIFARE4Mobile 1.01

Concepts

- **MIFARE Implementation**
  - Single MIFARE Classic Virtual card

- **Service Manager (SM)**
  - Offers Remote Management API and Wallet API
  - Holds keys for remote secure messaging

- **Service Object (SO)**
  - Contains MIFARE application + Metadata

- **SO stored in SM**
  - Loaded into MIFARE implementation upon activation
  - Multiple SO per SM
  - Multiple SO in MIFARE Implementation if no collision of resources
MIFARE4Mobile 2.1.1

Concepts

► **MIFARE Implementation**
  - Multiple Virtual cards supporting MIFARE Classic and MIFARE DESFire

► **Virtual Card**
  - Own UID and activation parameters
  - RF interface and Host interface
  - Can hold multiple applications (no resource collision)

► **Virtual card Manager (VM)**
  - Offers Remote Virtual card management API
  - 1 to 1 with Virtual Card
  - Holds keys for remote secure messaging

► **MIFARE Application**
  - Always kept in MIFARE Implementation
  - Associated with one virtual card

► **Service Manager (SM)**
  - Offers Remote Application Management API and Wallet API
  - 1 to 1 with Application
  - Holds keys for remote secure messaging
**MIFARE4Mobile 2.1.1**

**Architecture**

- GlobalPlatform for the secure management of multi-applications in the Secure Element
  - Integration with GP Amendment C

- User Verifier for the optional verification of the user’s identity

- Parser for the optional processing of retrieved data
Service Provider defines VC settings during its creation

- Type of MIFARE VC
  - MIFARE Classic (1K or 4K memory size)
  - MIFARE DESFire (2K, 4K or 8K memory size)
- MIFARE VC settings
  - ATQA, SAK
- UID Allocation
  - 7 Byte Master UID
  - 4 Byte Random FnUID
  - 4 Byte FnUID inherited from the 7 Byte Master UID
- MIFARE Keys
- MIFARE Access Data Conditions (MDAC)
- Usage of a Parser for the data retrieval
- Usage of a User Verifier for the data retrieval
MIFARE4Mobile 2.1.1

Certification

- MIFARE4Mobile Test Center commercial launch
  - Platform Cert. (platform ready for M4M V2.1.1 impl.)
  - Secure Element Cert. (TSM & wallet IF)
MIFARE4Mobile 2.1.1

Status

- MIFARE structure deployed
- Smartphones with NFC more and more popular
- MIFARE4Mobile Industry Group and licensing ready
- MIFARE4Mobile Specifications ready
- Certification Test Centre ready
- MIFARE4Mobile is ready to go!!!
GSMA and MIFARE4Mobile IG collaboration

- GSMA MIFARE4Mobile Implementation Guidelines
  - To be published April 2015
- Collaboration to develop guidelines for mobile operators to implement interoperable ticketing and access services.
- These guidelines move the industry towards a uniform approach to deliver ticketing and access services at scale on NFC-enabled devices by:
  - Formulating recommendations and preferred options in MIFARE4Mobile specs.
  - Defining a migration path from existing MIFARE solutions to MIFARE4Mobile.
- GSMA to provide a webinar on 30th April
  - [https://www.brighttalk.com/webcast/7615/153603](https://www.brighttalk.com/webcast/7615/153603)
NXP SOLUTIONS
MIFARE4Mobile solutions

- NXP announces that the first MIFARE4Mobile eSE certificates become available
  - MIFARE Classic Support
    - 1K & 4K
    - Anti-collision & select with single size FnUID derived from 7 byte masterUID
  - MIFARE DESFire Support
    - 2K, 4K & 8K
  - MIFARE4Mobile Implementation
    - M4M Framework Specification Version: v2.1.1
  - Card Operating System Options
    - Contactless Self Activation supported? Yes
    - CRS Application present? Yes
  - Secure Element configuration
    - SmartMX2 with JCOP 3.1 R1.2.1
MIFARE4Mobile training

- One-day MIFARE in Mobile training
- Both theoretical and practical sessions
  - Workshop using PN65T demoboard
- Training given by our CAS MIFARE4Mobile experts
- Training focused on MIFARE4Mobile 2.1.1
  - MIFARE4Mobile 1.01 including NXP’s 1.8 extension training on demand.
MIFARE4MOBILE
LATEST NEWS
NFC mobile ticketing MIFARE® commercial roll outs
Reference Transport Services
Dubai

- Scalability of MIFARE product portfolio
  - Smart cards (MIFARE DESFire)
  - Bank cards (convergence)
  - UICC SIM (MIFARE DESFire)

- Successful proof of working licensing program
  - UICC SIM vendors supplying

- NFC enabled device
  - 4 NFC enabled devices involved at the start

- OTA management

Committee members:

- SmartCards install base: 4 Mpcs
- DU MNO subscriber base 4.5 Min (2011)
- ETISALAT MNO subscriber base 6.3 Min
Reference Transport Services

Bangkok

✓ Scalability of MIFARE product portfolio
  • Smart cards (MIFARE DESFire)
  • Bank cards
  • UICC SIM (MIFARE DESFire)

✓ Successful proof of working licensing program
  • OT - UICC SIM vendor supplying

✓ NFC enabled device
  • 2 NFC-enabled devices focused at the start

✓ OTA management

SmartCards install base: 1,6 Mpcs
MNO subscriber base 35,7 Mln
Reference Transport Services

Valencia

- Scalability of MIFARE product portfolio
  - Smart cards (MIFARE Classic)
  - UICC SIM (MIFARE Classic)
- NFC enabled device
- OTA management

- Services
  - Transit ticketing (Bus, Metro, Tram, Trains)
  - Access control to public service building (libraries city-wide)
  - Loading and reloading of anonymous transport contracts
CONCLUSION
MIFARE4Mobile

Wrap up

► MIFARE4Mobile is the combination of two leading edge technologies
  ▪ MIFARE technology by NXP
    ◆ Worldwide leader solution for Smart Mobility
    ◆ More than 40 different applications rely on MIFARE technology
  ▪ NFC technology
    ◆ Proximity card technology in your smartphone
► MIFARE4Mobile 2.1.1 is already in place
  ▪ Specifications available
    ◆ Definition of the MIFARE4Mobile 2.1.1 architecture
  ▪ Products and solutions available
  ▪ Certification available
► NXP’s products address both hardware and software solutions
► First MIFARE4Mobile-based solutions in the market
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.
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.themobileknowledge.com/content/knowledge-catalog-0