Near Field Communication: IoT with NFC

Dominik Gruntz
Fachhochschule Nordwestschweiz
Institut für Mobile und Verteilte Systeme
**NFC Experience at FHNW**

2005/06 First NFC demonstrator (with Siemens CX70 Emoty)
- NFC was included in a removable cover

2009/10 Mobile Payment project (Nokia 6131 NFC, S40 Phone)
- *touch’n’pay* Self Service Shop
- Supported by the Hasler foundation
- NFC Forum Global Competition: First price in the category "The Best NFC Service of the Year 2010"

2010/11 Android Nexus S (with NFC)
- Tag reading with 2.3.2
- Tag writing and P2P with 2.3.3 / 2.3.4
- Tag emulation with Android Wallet (2.3.5)
AGENDA

NFC Device Operating Modes
- What is NFC?

NFC Device Architecture
- What is the Secure Element?

NFC Applications (on Android)
- Which NFC applications are available in the Android store?
- Payment trials

Open Questions / Next Steps
What is NFC

NFC (Near Field Communication)
- Communication technology based on radio waves at 13.56 MHz frequency
- Short range (<= 10 cm theoretical, 1-4 cm typical)
- Low speed (106 / 216 / 414 kbps) => 13-50KBytes per sec
- Low friction setup (no discovery, no pairing)
  - Setup-time < 0.1 Sec
- Communication roles:
  - Master Device: NFC Initiator (starts communication, typically a device)
  - Slave Device: NFC Target (passive tag or device)

- Standardization: NFC Forum (founded 2004 by NXP, Sony, Nokia)
  - Definition of standards
  - Popularization of NFC
  - Today: More than 150 members
NFC Device Operating Modes

How to interact with it?

- Reader-Writer Mode
  - Inverted RFID Model: RFID: many tags and one reader
  - NFC: one tag and many readers

- Peer-To-Peer Mode

- Tag Emulation Mode
NFC Device Operating Modes

Reader-Writer Mode
- Mobile Device is able to read external tags/smartcards, Device becomes RFID reader/writer (and can launch applications)
  - Tag content: Text, URI (WebLink, Phone Number), SmartPoster
- Like QR-Codes, but faster
  - No need to launch an application
  - With Android, an intent is thrown if a tag is detected
- Tags
  - Different form factors for NFC tags: tags, stickers, cards, key fobs, clocks
  - Supported Technologies:
    - ISO 14443 A/B, Mifare Ultralight, Classic/Standard 1K/4K
    - NXP DESFire, Sony Felica, Innovision Topaz, Jewel tag
=> NFC Forum Specs define how NFC Messages are stored
NFC Device Operating Modes

Peer-To-Peer Mode

- Bidirectional P2P connection to exchange data between devices
  - Proximity triggered interactions
  - Android: Devices have to be placed back-to-back

- Applications
  - Exchange of vCards (e.g. XING)
  - Hand-over of Tickets & P2P Payment
  - Web-page sharing, Youtube-video-sharing
  - Application sharing
  - Exchange of device info in order to establish a faster connection automatically (e.g. Bluetooth)
NFC Device Operating Modes

Tag Emulation

- Device emulates a passive tag (typically a smart card)
  - Device can emulate (contain) multiple smartcards
  - Reader can’t distinguish between real smartcard & tag emulation
  - Android: Emulated tag can be read only if screen is on

- Examples
  - Access to the farm shop (Legic key)
  - Oyster-Card, London
  - Visa payWave Payment System
  - Google Wallet
AGENDA

NFC Device Operating Modes
  – What is NFC?

NFC Device Architecture
  – What is the Secure Element?

NFC Applications (on Android)
  – Which NFC applications are available in the Android store?
  – Payment trials

Open Questions / Next Steps
NFC Device Architecture

Structure of a NFC device

- Host-Controller
  - Application Execution Environment (AEE)
  - Controls UI, Communication and peripheral devices (Phone OS)
- NFC-Controller
  - Contactless Front-end (CLF)
  - Converter between HF signal and digital data
- Secure Element
  - Trusted Execution Environment (TEE)
  - Secure environment to execute and store security relevant applications and data

*Langer & Roland, Anwendungen und Technik von NFC, Springer, 2010*
Secure Element

Secure Storage in NFC device
- Tamper-proof storage for sensible data (money, tickets, keys)
- Cryptographic operations (encryption, signatures)
- Secure environment for the execution of program code (sandbox model)
  - May contain applications from different providers
  - Must provide individual installation, maintenance and revocation

Platforms
- SmartCard (Global Platform)
  - JavaCard system
  - APDU commands

Diagram:
- Host-Controller
- NFC Controller
- Secure Element
- External Reader

(C) Hochschule für Technik
Fachhochschule Nordwestschweiz
Secure Element

- **non-removable**
  - Embedded Hardware (Secure IC)
  - UICC over SWP (Secure SIM)
- **removable**
  - MicroSD-Card (Secure MC)
  - Bluetooth Stickers
  - Micro-USB Stickers
AGENDA

NFC Device Operating Modes
- What is NFC?

NFC Device Architecture
- What is the Secure Element?

NFC Applications (on Android)
- Which NFC applications are available in the Android store?
- Payment trials

Open Questions / Next Steps
Applications

NFC Tag Info
- Displays card information
- Displays the sectors of a tag (hex / ascii)
- Displays NDEF content
Applications

NXP Tag Writer

- Supports Reading & Viewing content of a tag
- Supports Creating / Erasing / Protecting content
Applications

**WiFiTap**
Allows to store & load the WiFi configuration on a tag (i.e. Name & WPA/WEP password)

**NFC TaskLauncher**
Use NFC tags to automate tasks (e.g. set volumes, set alarms, etc)

**EnableTable**
Restaurant couponing & loyalty system
Tag is embedded in the check billfold

**NFC Security**
Locks Android application; application can only be started if a NFC tag with the key is read in

**TabPats**
Real-Time information for Stanford Marguerite bus departures, simply place the phone against the TapPATS badge at the bus stop
Google Wallet

Mobile Payment System

- Checkout at MasterCard PayPass-enabled terminals
  - Used by over 140'000 merchants
- Partners
  - Sprint: Telco Provider
  - Citi: Credit Card Issuer
  - FirstData: Accounting / Backend
- Application
  - Runs on new Android version (2.3.5)
  - Application on device requires that user authorizes transactions with a PIN
  - Uses SE on the device (Nexus S 4G only) [Sprint uses CDMA]
- Supported Credit Cards: Citi MasterCard & Google Prepaid Card
- No transaction fee
Mobile Wallet (Swisscom)

Pilot Project 1
- Galaxy S II (with custom ROM)
- SE on SIM card (SWP)
- Payment
  - Mastercard PayPass
- Loyalty program
  - Kaffee Spettacolo
- Q1 / 2012

Pilot Project 2
- Big Retailer

Pilot Project 3
- Visa payWave & MasterCard PayPass
Sunrise Trial

Pilot Project

- Special SIM Card
  - Oberthur Technologies Deutschland GmbH
- Mastercard PayPass
  - k kiosk
  - Avec
  - McDonalds
- Start: March 12
- Approx 20 Test Customers
# Applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>R/W Mode</th>
<th>P2P Mode</th>
<th>Emul Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment / Loyalty</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Ticketing</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Real-world Gaming</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Home automation</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location-based tagging</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Train time table, eLibrary in Klagenfurt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Couponing / Vouchers</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Map a real object to a URL</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC-initiated BT pairing</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Ski theft protection</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AGENDA

NFC Device Operating Modes
- What is NFC?

NFC Device Architecture
- What is the Secure Element?

NFC Applications (on Android)
- Which NFC applications are available in the Android store?
- Payment trials

Open Questions / Next Steps
Open Questions

Secure Element (Android)
- Who controls the keys of the secure element?
- Will Google lease space on its SE for free?

Secure Element (general)
- How are the SE (JavaCard) applets distributed?
  - For a SIM-based SE the MNO controls which apps are available
- How to revoke applications from a SE?
  - In case that device is stolen
  - In case that device changes ownership
- How to choose emulated card if SE contains several cards?
- How to choose the SE if device contains several SEs?
- Will there be a development key to access the SE?
Open Questions

Chicken Egg Problem

- With Google pushing NFC will it become widespread?
  - With the help of Motorola Google may push new NFC devices onto the market

- More and more Android are NFC enabled
  - 1,000,000 new NFC devices per week [Hamilton & Coenen, Google I/O 2012]

- Will iPhone 5 contain NFC?
  - Will be answered at Sept 12
NFC Next Steps

Projects & Trials

- Buy Nexus S and upgrade to Android 4.0 (ICS)
- Buy NFC Reader & Tags (=> Starter Kits)
- Install NFC Tag Info / NXP Tag Writer Apps
- Read Documentation
- Look at Sample Code (StickyNotes)
  - [https://nfc.android.com/StickyNotes.zip](https://nfc.android.com/StickyNotes.zip)
  - [https://code.google.com/p/nfcmemory/](https://code.google.com/p/nfcmemory/)
- Read NFC Book
  - Anwendungen und Technik von NFC
    Josef Langer & Michael Roland
    Springer, ISBN: 978-3-642-05496-9
Near Field Communication: Close Up

Dominik Gruntz, dominik.gruntz@fhnw.ch
Fachhochschule Nordwestschweiz
Institut für Mobile und Verteilte Systeme