Fundamentals of Near Field Communication (NFC)

Tvrtko Barbarić
NXP Semiconductors
Global player with local reach
- 2013 revenue >$4.8 Billion
- >25,000 employees

Identification Business Unit
- Secure Passports, Banking, Mobile Transactions/NFC,
- Transport, Infrastructure/Reader IC’s, RFID (LF, HF, NFC, UHF)
Overview of NFC related standards

Products may implement various combinations of standard
NFC modes of operation

NFC peer-to-peer

NFC reader/writer

NFC card emulation
NFC reader/writer mode

• An active, field generating device (reader/writer or r/w) communicates with either
  • Passive device (tag or card) or
  • Active device emulating a tag or card (‘card emulation’)

• Typically:
NFC Tags

- NFC Forum Tag is a contactless tag compatible to one of four* NFC Forum Tag platforms capable to store NDEF formatted data
- NFC Forum introduced standardized technology architecture, initial specifications and tag formats for NFC-compliant devices in June 2006

- These specifications include:
  - NFC Forum Data Exchange Format (NDEF), defines a message encapsulation format to exchange information
  - Record Type Definition (RTDs) The RTD specification provides a way to efficiently define record formats for new applications and gives users the opportunity to create their own applications based on NFC Forum specifications of TEXT, URI, Smart Poster, and Generic Control.

*Type 5 specification under review of NFCForum
NFC Data Exchange Format (NDEF) and Record Type Definition (RTD)

Records are processed sequentially

- ‘vcard’
- ‘iscwest’ or ‘mytype’
## NFC Tags – Overview of available types

<table>
<thead>
<tr>
<th>NFC Forum Tag Type</th>
<th>Standard Compliance</th>
<th>Comm. Speed</th>
<th>Configure Capability</th>
<th>Memory availability</th>
<th>Available Tag ICs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type 1</strong></td>
<td>ISO14443 A</td>
<td>106 kbit/s</td>
<td>Tags are read and re-write capable, users can configure the tag to become read-only</td>
<td>512 bytes</td>
<td>Topaz512</td>
</tr>
<tr>
<td><strong>Type 2</strong></td>
<td>ISO14443 A</td>
<td>106 kbit/s</td>
<td>Tags are read and re-write capable, users can configure the tag to become read-only</td>
<td>512 bits to 2k Bytes</td>
<td>MIFARE Ultralight family NTAG family</td>
</tr>
<tr>
<td><strong>Type 3</strong></td>
<td>JIS X6319-4 (Japanese Industrial Standard)</td>
<td>212 or 424 kbit/s</td>
<td>Tags are pre-configured at manufacturer to be either read and re-writable, or read-only</td>
<td>4k bytes</td>
<td>Sony FeliCa</td>
</tr>
<tr>
<td><strong>Type 4</strong></td>
<td>ISO14443-4 ISO7816-4</td>
<td>Up to 424 kbit/s</td>
<td>Tags are pre-configured at manufacturer to be either read and re-writable, or read-only</td>
<td>Up to 32k bytes</td>
<td>NXP MIFARE DESFire™ EV1, SmartMX/JCOP</td>
</tr>
</tbody>
</table>
NFC peer to peer (P2P) mode

- Two smart devices communicating with each other
  - 2 different modes with (active & passive)
  - 2 different roles supported (initiator & target)

- Typically:
P2P modes

• Active

Transitions to:

• Passive

Data flow
Card emulation modes

Secure Element based

- HW based secure element can be either embedded (eSE) in device or in the SIM

HCE

- HCE was introduced in 2013 by Google on Android 4.4 (KitKat)
- Supports ISO/IEC 14443-4 and APDUs as defined in the ISO/IEC 7816-4
- Mandates support based on ISO/IEC 14443-3 Type A, the support for ISO/IEC 14443 Type B is optional

HCE implementation in the phone

- Host CPU
- eSE
- SIM
- NFC Controller

- Secure HW
- Unsecure HW

- Runs the application based HCE service
- Communicates with the backend if required
- Stores the applications securely
- Runs the lower layer emulations securely (e.g. MIFARE Classic)
- Performs the protocol based routing first
- After that, based on the registered AID routes the communication to the corresponding host
HCE security considerations

• HCE offers per design the same level of security as the Android platform
• The payment applications rely heavily on the backend systems to mitigate risks of the unsecured implementation
• Smaller installations with security relevance often do not have the required infrastructure
Summary

• NFC offers variety of different communication modes between two devices
• In order to communicate with an NFC device, system can adopt only the most appropriate mode of communication and ignore others
• NDEF offers a flexible, standardized platform to share data or trigger actions at target device
• Proprietary implementations can be encapsulated inside the standard conform data format
• HCE offers alternative platform for card emulation on NFC Android devices, but carries potential security risks in security relevant applications
Contact:
Tvrtko Barbaric
Business Development Director, BU Identification
tvrtko.barbaric@nxp.com
+1 408 674 9488