PROCESS FOR DESIGNING AN NFC READER APPLICATION

TODD NUZUM AND MOHAMAD RAJGARA

CAS

AMF-IND-T2759 | JUNE 2017
AGENDA

• So, you want to build a reader
• User Chip types
• Architecture and Component Selection
• Design Issues
• Testing and Certification
• Summary
• Q&A
User Chip Type
NFC Reader / Card communication

1 – Power
The RF field oscillates at 13.56 MHz.
The card is powered through electromagnetic coupling

2 Sending commands
The Reader modulates the RF field to send commands

3 Answering to the reader
By modifying its consumption, the chip modifies the RF field, which is detected by the reader.

This mechanism is called: **Load Modulation**
The pillars of RFID & smartcard architectures:

- **Transponders (passive IC’s)**
  - ISO/IEC15693 Tags & labels
  - MIFARE families
  - ISO/IEC14443A NTAG labels & Smartcards, single & dual interface
  - NFC connected Tags (NTAG F and I²C)
  - UHF connected Devices (PCB tagging, UCODE I²C)

- **Readers (active IC’s)**
  - LF Readers
    - HTRC110, PCF7991AT
  - HF readers
    - NFC controllers
    - Frontends

- **Connected contactless (I²C)**
  - NFC Friendly

- **Contact reader IC’s**
  - Smartcard ISO/IEC7816 Readers
    - TDA 8xxx family

- **Secure Elements**
  - ISO/IEC7816
  - Secure key storage
    - SAM family, P5DFxxx
  - I2C/7816/14443 eSE key & application storage
    - Authentication families

- **TRAINING PRODUCT FOCUS**
  - MIFARE family
  - NTAG family
  - Hitag family
  - Icode family
  - Ucode family
Architecture and Component Selection
Components in an NFC access control system
Generic reader architecture

Reader
- Keypad (Optional)
- MCU FW
- Contact Reader IC (Optional)
- SAM (Optional)

Controller
- Backend System (Optional)
- Transceiver
- Other technologies (BLE, biometric…)(Optional)
- Contactless Reader IC
- Antenna matching network
- Generic embedded µController
- Ex: CLRC663

Transceiver
- Contactless object
- RFID card, NFC smart card, NFC phone or any other NFC object

Backend System (Optional)
- Ex: TDA family
- Ex: SAM AV2
Typical Active Contactless Architecture: NFC Frontend

- Active device has no «intelligence»:
  - Reader interface collects register settings and dispatch commands according to MCU state machine;
- ISO Protocol has to be implemented in MCU flash

**Embedded reader module**

- **Backend System**
- **μC**
- **Reader IC**
- **NFC object**

- **MCU FW**
- **Generic embedded µController**: Ex: CLRC663, PN5180
- **Analog matching network**
- **13MHz loop Antenna**

- RFID card, NFC Tag, NFC phone, or any other NFC object
Typical Active Contactless Architecture: NFC Controller

- Active device includes «intelligence» in built-in MCU:
  - FW1 includes ISO protocol;
- Host MCU requirements (FW2) are much softer:
  - «call functions» to most used interactions (usermanuals)
  - NCI functions (PN7120/PN7150)
NFC focus products for each application need

High end

- High-perf full NFC with DPC
  PN5180

- One chip system, freely programmable NFC controller with DPC
  PN7462/PN736x

All round

- High-perf multi-protocol reader
  CLRC663

- Plug&Play NFC for Linux, Android, Win
  PN7150

Entry level

- High-perf proximity&vicinity readers
  MFRC630
  (ISO14443A – MIFARE/NTAG reader)

- SLRC610
  (ICODE ISO15693 and ISO18000-3M3)

- NTAG I²C plus

Connected tag solutions
NFC tags with non-volatile memory and host connection

NFC Frontend solutions
NFC reader with NFC Reader SW Library

NFC controller solutions
NFC reader with integrated
32-bit Cortex MCU and either integrated firmware or freely programmable memory

* Single chip: Cortex M0 MCU + last generation NFC reader + iso7816 Contact reader
The Product Selection Path

Passive solution
- I will interact only with NFC phones

Active solution
- What OS requirements do you have?

NTAG I²C plus

Linux Android Windows

Own application code

RTOS NullOS

I will talk to any NFC-enabled system

High performance full NFC with DPC

High performance multi-protocol reader

I will interact with contactless cards

High performance ISO/IEC18092 reader

High performance ISO/IEC18092 and ISO/IEC18000-3M reader

PN71xx NFC controller with integrated FW

PN7150

PN746x_736x NFC controller with customizable FW

PN5180 NFC frontend

CLRC663 NFC frontend

MFRC630 NFC frontend

SLRC610 NFC frontend
NFC Reader Design Process
Antenna tuning

Step 1: Measure Antenna parameter using Network Analyzer

\[ L = \frac{300.9}{2\pi \times 13.56\text{MHz}} = 3.53 \mu\text{H} \]
\[ R_{\text{Coil}} = 13.4 \Omega \]
\[ C_{\text{pa}} = ? \]
NFC Antenna: blocks for "matching"

- NFC - demoboard -> done by NXP

Example

L0 = 470nH; C0 = 220pF for current demoboard

Open!
To be done in the next steps.

antenna coil from customer -> done
Antenna tuning

Step 2: Calculating the matching caps

- Measured: L = 3500 nH, C_{pa} = 1 pF, R_{Coil} = 13 Ohm
- To be defined: Q, Target impedance 25 Ohm, f_{EMC} = 14.600 MHz.
- Calculated: Q_{a} = 23
- Result: R_{s} = -0.02 Ohm = R_{s}
- Chosen: L_{0} = 470 nH, C_{0} = 252.8 pF
- Result: C_{1} = 16.6 pF, C_{2} = 59.6 pF

Antenna coil
- measure L, R_{Coil} and C_{pa} @ 13.56 MHz
- Practical approach:
  - We measure L and R_{Coil} (and estimate C_{pa}).

Example

http://www.nxp.com/documents/other/AN11246_239810.zip
Antenna tuning

Step 3: Simulation - adapting C to optimize performance and taking into account commercial values
Antenna tuning

Step 4: First measurement with miniVNA using optimized values
Antenna tuning

Step 4: Adjustment hints

Tuning of C1

It seems C1 has to be reduced, therefore let’s remove 1pF from both branches
Antenna tuning

Step 6: 2nd measurement with miniVNA using optimized values

\[ C_{1_{\text{opt}}} = 13\, \text{pF} \]

\[ C_{1_{\text{opt}}} = 13\, \text{pF} \]
Antenna design and Register settings are strictly related

1. Many small antenna geometries although save pcb space, risk to end up in bad performing readers due to bad signal to noise conditions.

2. For ISO/IEC14443-A, there are registers like MIN-LEVEL defining the minimum level (threshold value) for the subcarrier detector unit, which should be higher than the noise level in the system…

3. and COLL-LEVEL which defines how strong a signal must be interpreted as a collision for Manchester subcarrier communication types.

4. 2 and 3 together with RXGAIN, which defines receiver signal voltage gain factor, should optimize RF behavior to support MIFARE technologies.
Design Issues
NFC Related Design Issues

1. **Radiation of unwanted harmonics**
   - causes violation of the CE & FCC limits.
   - disturbs other parts of the circuit (e.g. other RF circuits).

2. **Noise**
   - on Tx causes unwanted sidebands and violates CE & FCC limits.
   - on Tx causes unwanted sidebands and disturbs the NFC.
   - on Rx reduces the “sensitivity” and disturbs the NFC.
   - disturbs other parts of the circuit (e.g. other RF circuits).

3. **Magnetic coupling**
   - wastes a part of the energy.
   - causes trouble in other parts of the circuit.
   - couples noise into the NFC circuit.
Radiation of unwanted harmonics

* Single chip: Cortex M0 MCU + last generation NFC reader + iso7816 Contact reader
Typical NFC antenna circuit: Harmonics

**TX-Output**
- A second order low pass filter is sufficient.
- L must cover the power (current) requirement.
- C must be NPO.
- Layout area must be small and close to the NFC IC.
- **Layout area must be really small and very close to the NFC IC.**

**Harmonics:**
- Tx = push – pull output
- toggles between Vcc and GND
- generates a lot of harmonics

- **Filtering required!**

“Hot Spots“
Example Bad Layout

* Single chip: Cortex M0 MCU + last generation NFC reader + ISO7816 Contact reader
Example Bad Layout

* Single chip: Cortex M0 MCU + last generation NFC reader + iso7816 Contact reader
Example Good Layout
Example Good Layout
2) Noise

- Single chip: Cortex M0 MCU + last generation NFC reader + iso7816 Contact reader

- Other I/O: Display, keypad, Bluetooth, etc.

* CARD or NFC device

Diagram:
- Vcc: Power supply
- Rx: Rx-Circuit
- Tx: EMC-Filter
- Impedance Matching
- Antenna coil
2) Typical NFC antenna circuit: Noise

Output power?

\[ P_{\text{tot}} = 5\, \text{V} \times 200\, \text{mA} = 1000\, \text{mW} \]
2) Typical NFC antenna circuit: Noise

- **NFC Specifics**
  - Tx Output generates 300 …1000mW.
  - Rx needs to be able to decode a few mV level of subcarrier.

- **Generic**
  - All other is standard EMC related design for analog and digital circuits!
3) Magnetic coupling

- Power supply
- Antenna coil
- Rx-Circuit
- EMC-Filter
- Impedance Matching

Other I/O: Display, keypad, Bluetooth, etc.
3) Magnetic coupling

- **Magnetic field**
  - The NFC Reader antenna is made to generate a magnetic field.
  - The coupling between
    - Reader and Card should be high.
    - Reader and rest of the circuit should be low.

- **Do’s and Don’ts**
  - Try to avoid
    - Magnetic loops in general (other than the antenna itself).
    - Strong magnetic coupling between antenna and anything else.
  - Try to make
    - Proper GND layer (area rather than single traces).
    - Use orthogonal crossing of antenna traces and others (if required).
Testing and Certification
FCC
https://www.fcc.gov/
Other RF testing

- Antenna
- Power
- Data Rate
- Modulation
- Frequency range

Country and Compatibility

- Specific Country requirements

<table>
<thead>
<tr>
<th>Technology List</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIFI(2.4G)</td>
</tr>
<tr>
<td>WIFI (5G)</td>
</tr>
<tr>
<td>BT</td>
</tr>
<tr>
<td>WWAN(2/3G)</td>
</tr>
<tr>
<td>LTE(4G)</td>
</tr>
<tr>
<td>Zigbee</td>
</tr>
<tr>
<td>Z-wave</td>
</tr>
<tr>
<td>SRD</td>
</tr>
<tr>
<td>NFC</td>
</tr>
<tr>
<td>NTSC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BT Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT 1.0 (GFSK)</td>
</tr>
<tr>
<td>BT 2.0</td>
</tr>
<tr>
<td>BT 2.1 EDR with AFH</td>
</tr>
<tr>
<td>BT 3.0 without HS</td>
</tr>
<tr>
<td>BT 3.0 with HS mode</td>
</tr>
<tr>
<td>BT 4.0 with LE</td>
</tr>
<tr>
<td>BT 4.0 w/o LE with BT1.0</td>
</tr>
<tr>
<td>BT 4.0 w/o LE with BT2.1</td>
</tr>
</tbody>
</table>
Credit Card based payments


- The PCI SSC currently consist 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 common set of security standards that are common to the whole payment infrastructure
  - Ensure a “standard” to protect payment account, transaction and authentication data
### PCI Certification

**PCI Data Security Standard**

- The PCI Data Security Standard applies to entities that store, process or transmit cardholder data or authentication data.

<table>
<thead>
<tr>
<th>Build and Maintain a Secure Network and Systems</th>
<th>PCI Certification</th>
<th>NXP support</th>
<th>End customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
<td>PCI PTS 4.0</td>
<td>Link to PCI test laboratories or external consultant</td>
<td>Certification</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>Security certification for terminals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Protect all systems against malware and regularly update anti-virus software or programs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Restrict access to cardholder data by business need to know</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Identify and authenticate access to system components</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Regularly test security systems and processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Maintain a policy that addresses information security for all personnel</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Account Data**
- Cardholder Data includes:
  - Primary Account Number (PAN)
  - Cardholder Name
  - Expiration Date
  - Service Code

**Sensitive Authentication Data includes:**
- Full track data (magnetic-stripe data or equivalent on a chip)
- CVV2/CVC2/CVV2/CID
- PINs/PIN blocks

**Certification**
- PCI labs: [https://www.pcisecuritystandards.org/approved_companies_providers/pci_recognized_laboratories.php](https://www.pcisecuritystandards.org/approved_companies_providers/pci_recognized_laboratories.php)
Credit Card based payments

**EMV Specifications (www.emvco.com)**

- 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 Contactless books provide extension for contactless transactions
- EMVCo is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders

---

**EMVCo Contact IC Stack**

- VSDC
- M/Chip 4
- Others

- EMVCo 1, 2, 3, 4 books
- ISO 7816 – 1/2/3/4/5 specifications

**EMVCo Contactless IC Stack**

- PayWave
- PayPass
- Others

- EMVCo Contactless A, B, C, D books
- ISO 14443
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 EMV L1 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 EMV L1 (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.

<table>
<thead>
<tr>
<th>Certification</th>
<th>NXP support</th>
<th>End customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMVCo L1 contact analog</td>
<td>Application notes; demo board; Report from test house</td>
<td>Need to test at certified lab on final device</td>
</tr>
<tr>
<td>EMVCo L1 contactless analog</td>
<td>Antenna design guide, loop back example; internal test report; demo board;</td>
<td>Need to test at certified lab on final device</td>
</tr>
<tr>
<td></td>
<td>antenna design trainings</td>
<td></td>
</tr>
<tr>
<td>EMVCo L1 contact digital</td>
<td>Application note; source code; ICS example; internal test report;</td>
<td>Need to test at certified lab on final device</td>
</tr>
<tr>
<td>EMVCo L1 contactless digital</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Certification</th>
<th>NXP support</th>
<th>End customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMVCo L2 contact</td>
<td>Link to partners for stack Pre-integration support *</td>
<td>Debug with EMVL2 partners ICS to be defined by customer and stack supplier. Certification on final device</td>
</tr>
<tr>
<td>EMVCo L2 contactless</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Only if NXP EMVCo L1 stack is used
Other certifications

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

<table>
<thead>
<tr>
<th>Certification</th>
<th>NXP support</th>
<th>End customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mastercard TQM</td>
<td>Link to lab or external consultant</td>
<td>Certification</td>
</tr>
<tr>
<td>Mastercard TQM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Needed to support MasterCard cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UKCC, SEPA, …</td>
<td></td>
<td>Certification</td>
</tr>
<tr>
<td>Country specific security certification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Certification (CE,FCC,…)</td>
<td>Guidelines for contactless</td>
<td>Certification</td>
</tr>
<tr>
<td>RoHS</td>
<td>Provision of RoHS compliance report of NXP components</td>
<td>Request document from manufacturing entity</td>
</tr>
<tr>
<td>RoHS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restriction of Hazardous Substances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card acceptance scheme</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MasterCard PayPass, Visa PayWave, DiscoverZip</td>
<td></td>
<td>To be checked with EMVL2 supplier</td>
</tr>
</tbody>
</table>
Summary
How to develop applications around NFC frontend solutions

NFC Reader Library
Software support for NFC frontend solutions:
Available for: **PN512, CLRC663, SLRC610, MFRC630, PN5180** for embedded systems (RTOS/NullOS) and Linux

Development kits and demo boards
PNEV512B      PNEV512R
CLEV663B      CLEV663
OM25180FDK   OM5597

Source code examples
SW examples based on NFC Reader Library demonstrating frontend capabilities

Development environment
LPCXpresso IDE for LPC MCUs

Documentation
Application notes
User Manuals
Getting started guides

NFC Cockpit
A PC tool that eases design process, antenna tuning and register configuration
*(only for PN5180)*
NFC Resources

- NFC community
- NFC use cases
- NFC Trainings
- NFC IDH Partners
- NFC Product selection guide

If you have an NFC question please contact: nfc.readers@nxp.com
Use our technical community for your questions

Become a registered member and get expert advice from the developer community
https://community.nxp.com/community/nfc

How to get there
- NFC and Reader Ics → NFC Technology hub → NFC support → NFC community
- URL: https://community.nxp.com/community/nfc

Ask your question
Look for answers
Watch on-demand any recorded session

Tap into our free on-demand training library.

Hundreds of hours of webinars and presentations on NXP products, applications, software, and tools.

Find recorded sessions, among others, for:

- NFC essentials
- NFC use cases
- NFC standards
- NFC reader antenna design (6 sessions)
- NFC reader portfolio
- NFC in smart home, gaming, payments,
  * …

How to get there

- NFC and Reader ICs → NFC Technology hub → NFC support → NFC webinars
- URL: http://www.nxp.com/support/online-academy/nfc-webinars:NFC-WEBINARS
Q&A