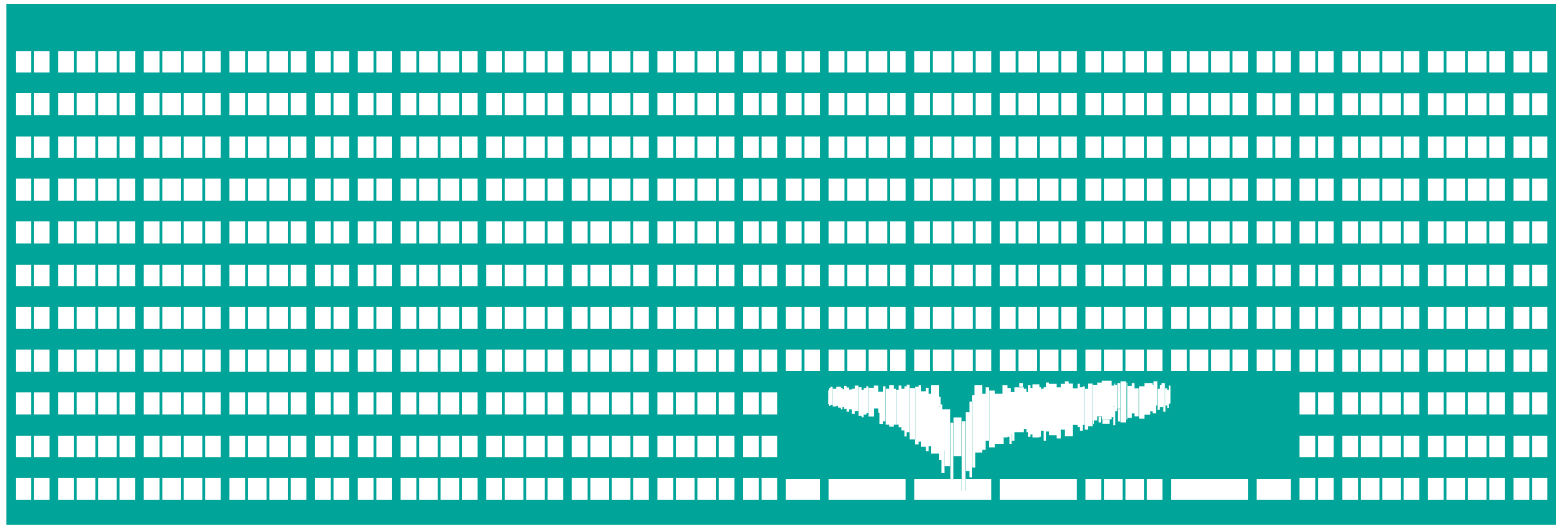
VŠB TECHNICKÁ UNIVERZITA OSTRAVA

VSB TECHNICAL UNIVERSITY OF OSTRAVA



www.vsb.cz

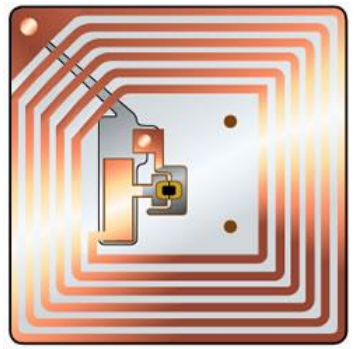
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Barcodes, RFID and NFC

Michal Krumnikl

Introduction

- **Radio-frequency identification**
  - Technology that uses radio waves to transfer data from an electronic tag, called RFID
  - Automatic Identification Procedure
- **Near field communication**
  - For simplified transactions, data exchange, and wireless connections between two devices in proximity to each other, usually by no more than a few centimeters.



RFID is Everywhere

Exxon SpeedPass

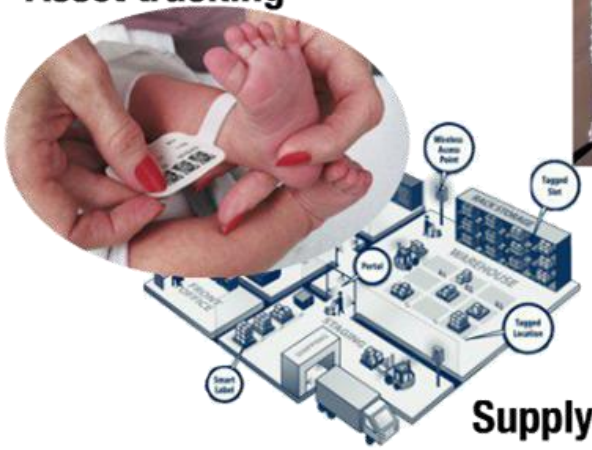
Mastercard PayPass

Financial Transactions

Identification

SmartPaper

Asset tracking



SF Muni Clipper pass

Supply chain

Access control

Casino Chips Theft Fail

man steals $1.5M in chips, cashes them in for $0 and jail

"RFID can void the stolen chips, like a registration that's no longer valid," Kendall said.

"When we manufacture RFID-embedded chips and send them to a casino, they're not worth anything until they register the codes. Until then, they're nothing but freight."

Waterpark ticket

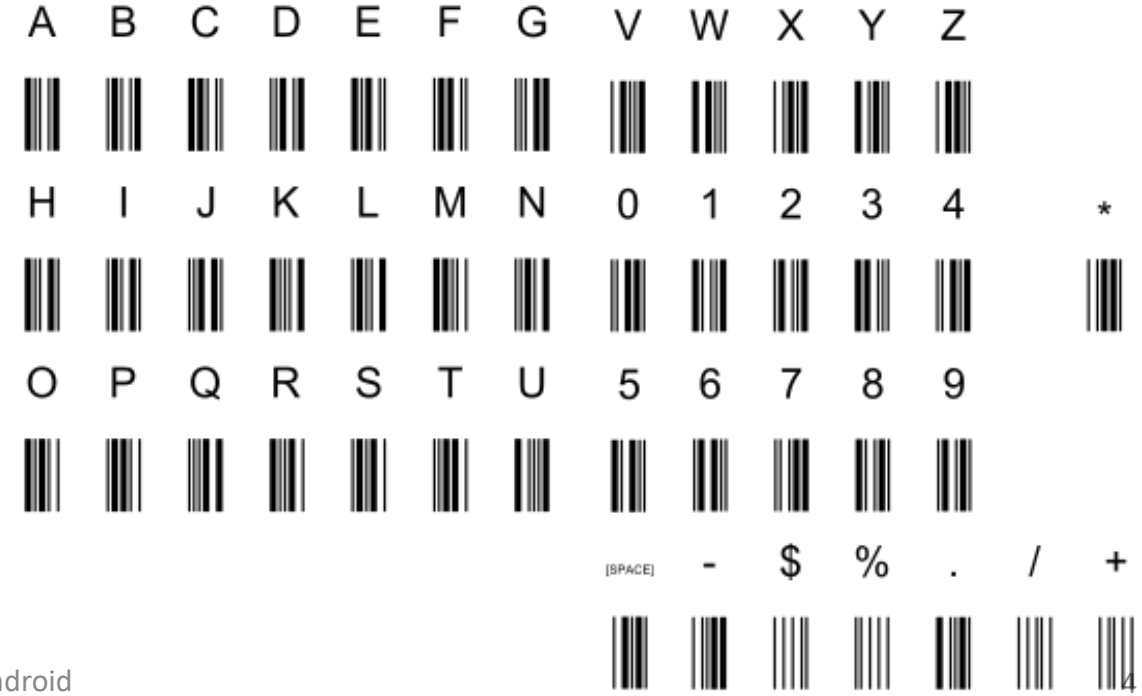
day-pass vs season pass

age-based restrictions

payment of food, beverages, merchandise

Barcodes and QR Codes

- **Designed to be machine readable**
  - They encode numbers and symbols using black and white bars.
- Example: **Code39**
  - Defines 43 Characters.
  - Typically used in non-retail areas.
  - One of the simplest barcode



Barcodes and QR Codes

- **QR Code**
- Most commonly used barcode as of recent especially with mobile phones.
- Has various numbers of functions: linking to websites, send SMS functions, etc.


The Original


Completely Erased

Table 12 — Error correction levels

Error Correction Level	Recovery Capacity % (approx.)
L	7
M	15
Q	25
H	30

RFID vs Barcodes

- **Can have a lot more data than barcodes**
- **Can write data, no camera lag, no ugly QR codes**
- **Cheaper, low-overhead, easier to Bluetooth**
- **Cheap, definite, closely spaced location**

- NOT localization
- NOT proximity detection
- NOT fast data transfer
- NOT secure (for non-smartcard)

Most commonly used for?	Inventory control	Advertising website URL	Automated inventory management
Needs to be visible (line of sight for the scanner)	Yes	Yes	No
Range for reading by the scanner	Several inches to a few foot	Several inches to a foot	Up to 30 feet ("Passive" tags), up to 100s of feet ("Active" tags)
Range Read/Write capability	Read	Read	Read and write (data can be changed on tag)
Reliability/ ruggedness	Wrinkled tags won't work	Up to 30% recovery of data from wrinkled codes	Very reliable
Marginal cost (cost per tag USD)	$0.01	$0.05	$0.05 - $1.00
Interesting uses include	Barcodes as input into video games, event registration	Virtual store with codes by pictures of sale items, links on building permits	Interactive experiences at sporting events and festivals, pet tracking/identification tags

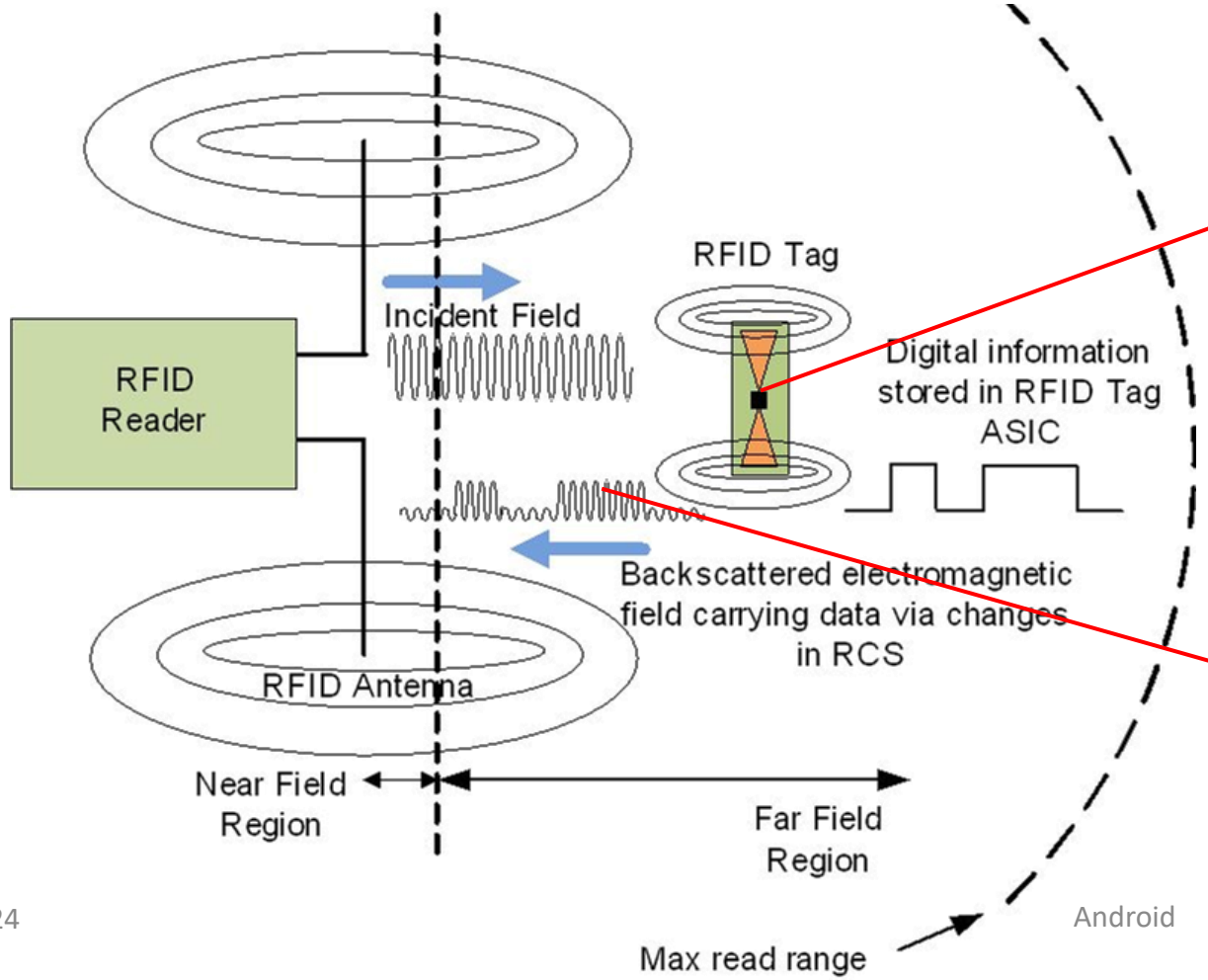
Source: https://www.rfsmart.com/blog/what-to-know-about-barcodes

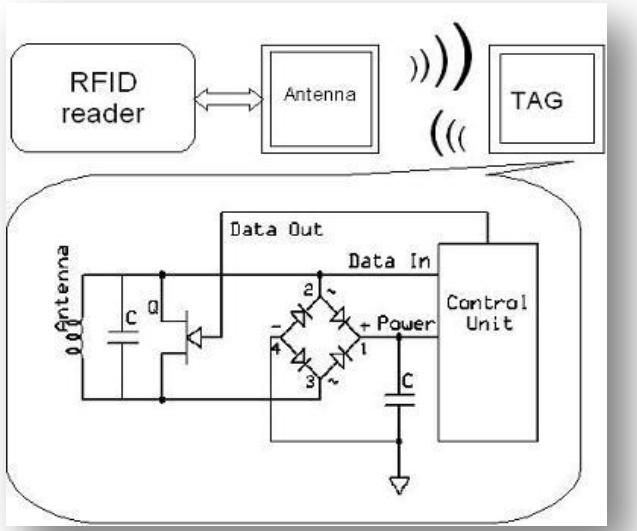
RFID/NFC vs Bluetooth

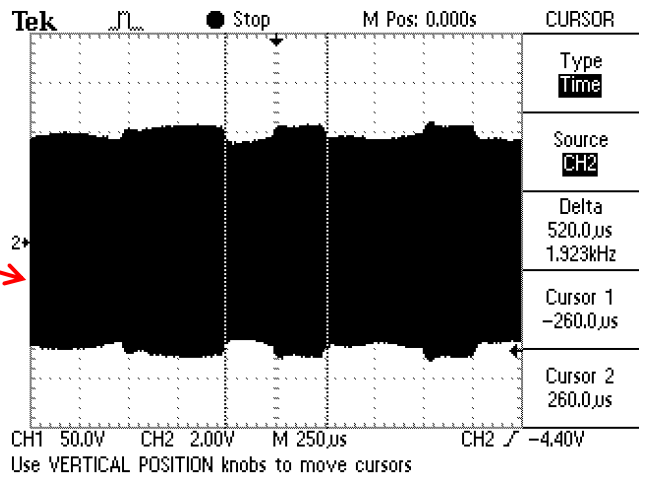
- **Bluetooth**
  - Great for persistent connections and broadcasts
  - Perfect for secure connection to wearables (once paired)
  - Public broadcasts (beacons)
- **NFC**
  - Great for short-lived connections and bootstrapping
  - Quick and secure link because of proximity
  - Small quantities of data
  - Use of NFC tags for pairing devices, configuring Wi-Fi

	NFC	Bluetooth	Bluetooth Low Energy
RFID compatible	ISO 18000-3	active	active
Standardisation body	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	Point-to-point	WPAN	WPAN
Cryptography	not with RFID	available	available
Range	< 0.2 m	~10 m (class 2)	~100 m
Frequency	13.56 MHz	2.4–2.5 GHz	2.4–2.5 GHz
Bit rate	424 kbit/s	2.1 Mbit/s	~1.0 Mbit/s
Set-up time	< 0.1 s	< 6 s	< 0.006 s
Power consumption	< 15mA (read)	varies with class	< 15 mA (transmit or receive)

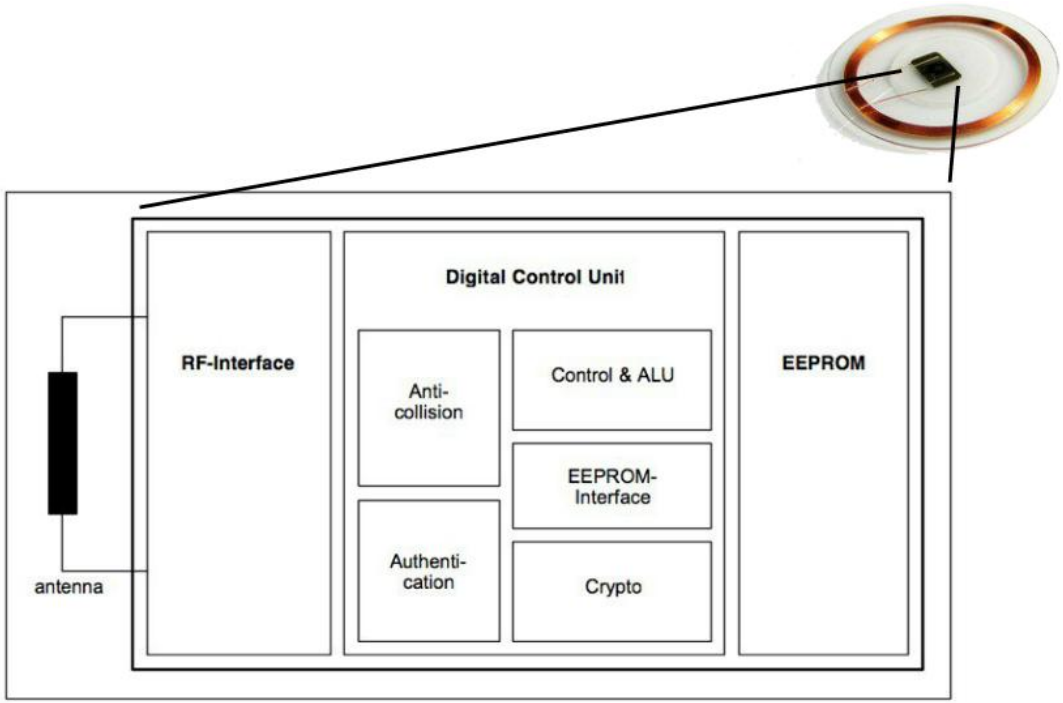
How RFID works ?

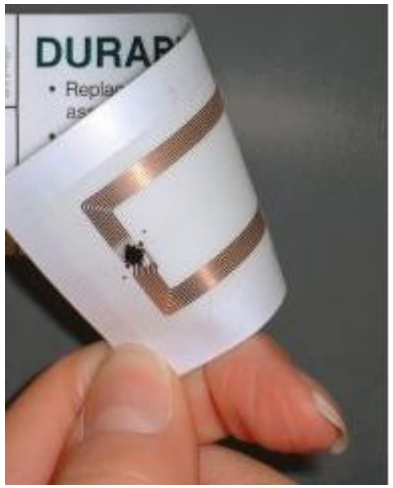


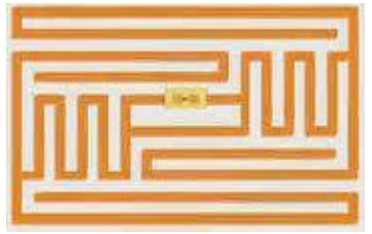


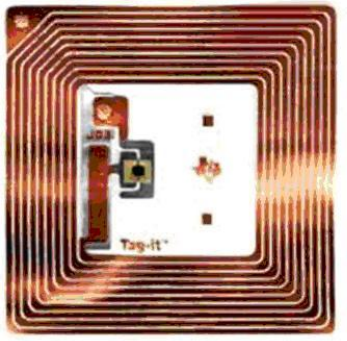


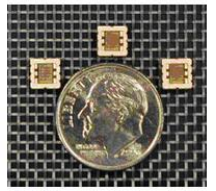
Passive RFID Tag Internals

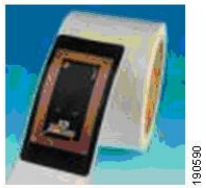












RFID

- **RFID tag**
  - Usually just a serial number, unique ID
  - UID 32-bit or 56-bit

- **Low-frequency** (LF: 125–134.2 kHz and 140–148.5 kHz)
- **High-frequency** (HF: 13.56 MHz)
- **Ultra-high-frequency** (UHF: 868–928 MHz)

NFC

- NFC is a set of **short-range** wireless technologies.
- Operates at **13.56 MHz** on ISO/IEC 18000-3 air interface and at rates ranging from **106 kbit/s to 424 kbit/s**.
- There are four types of tags defined by the NFC forum. There's a fifth that's compatible, but not strictly part of the NFC specification.
- Multi-part, mime-typed, textual data
- Devices can have 3 modes
  - **Tag reader/writer**
  - **Tag emulation**
  - **Peer-to-peer data transfer**

NFC TAG TYPE	STANDARD	NOTES
Type 1	ISO 14443A	Not commonly used (Topaz)
Type 2	ISO 14443A	Very popular (Ultralight, NTAGX, ST25TN)
Type 3	ISO 14443A	Not commonly used (Sony FeliCa)
Type 4	ISO 14443A, ISO 14443B	Not commonly used (DESFire)
Type 5	ISO 15693	Commonly used (SLI, SLIX, ST25TV)

Types of NFC Tags

- **Type 1**
  - Based on ISO-14443A specification.
  - Can be read-only, or read/write capable.
  - **96 bytes to 2 kilobytes of memory.**
  - Communication speed 106Kb.
  - No data collision protection.
  - Examples: Innovision Topaz, Broadcom BCM20203.

Types of NFC Tags

- **Type 2**
  - Similar to type 1 tags, type 2 tags are based on NXP/Philips Mifare Ultrali) specification.
  - Can be read-only, or read/write capable.
  - 96 bytes to 2 kilobytes of memory.
  - Communication speed 106Kb.
  - **Anti-collision support.**
  - Example: **NXP Mifare Ultralight.**

- See list of applications at https://en.wikipedia.org/wiki/MIFARE
- Security algorithms have been broken
  - Karsten Nohl et Henryk Plötz
  - https://www.usenix.org/legacy/event/sec08/tech/full_papers/nohl/nohl.pdf
  - MFOC : https://code.google.com/p/mfoc/

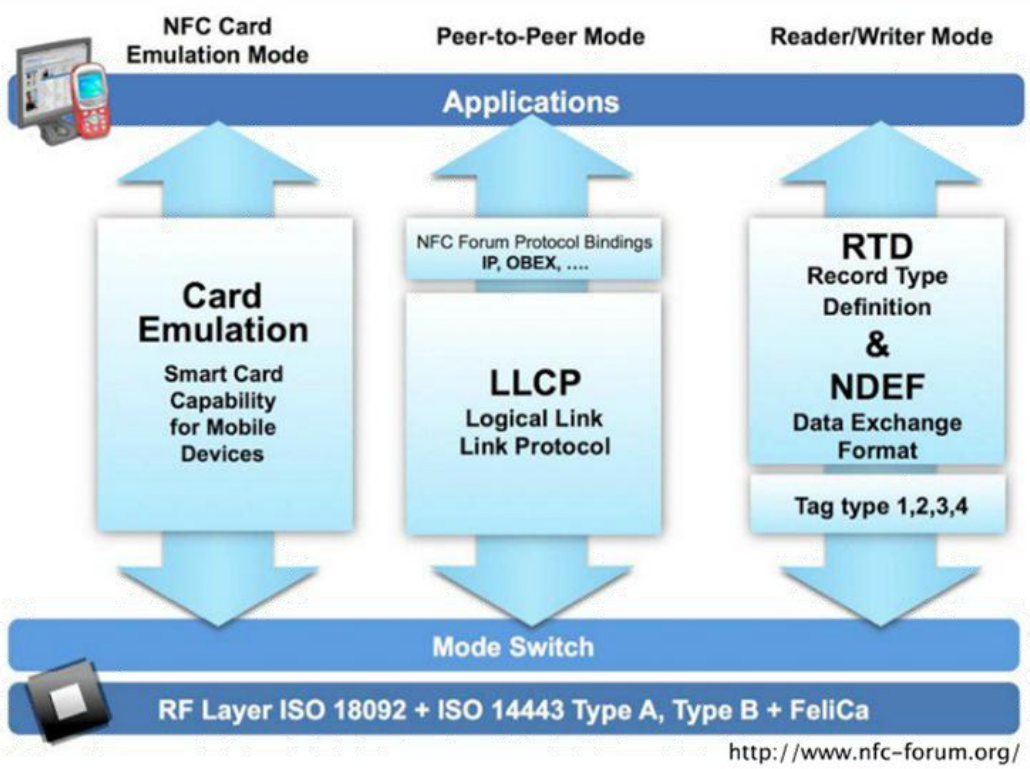
Types of NFC Tags

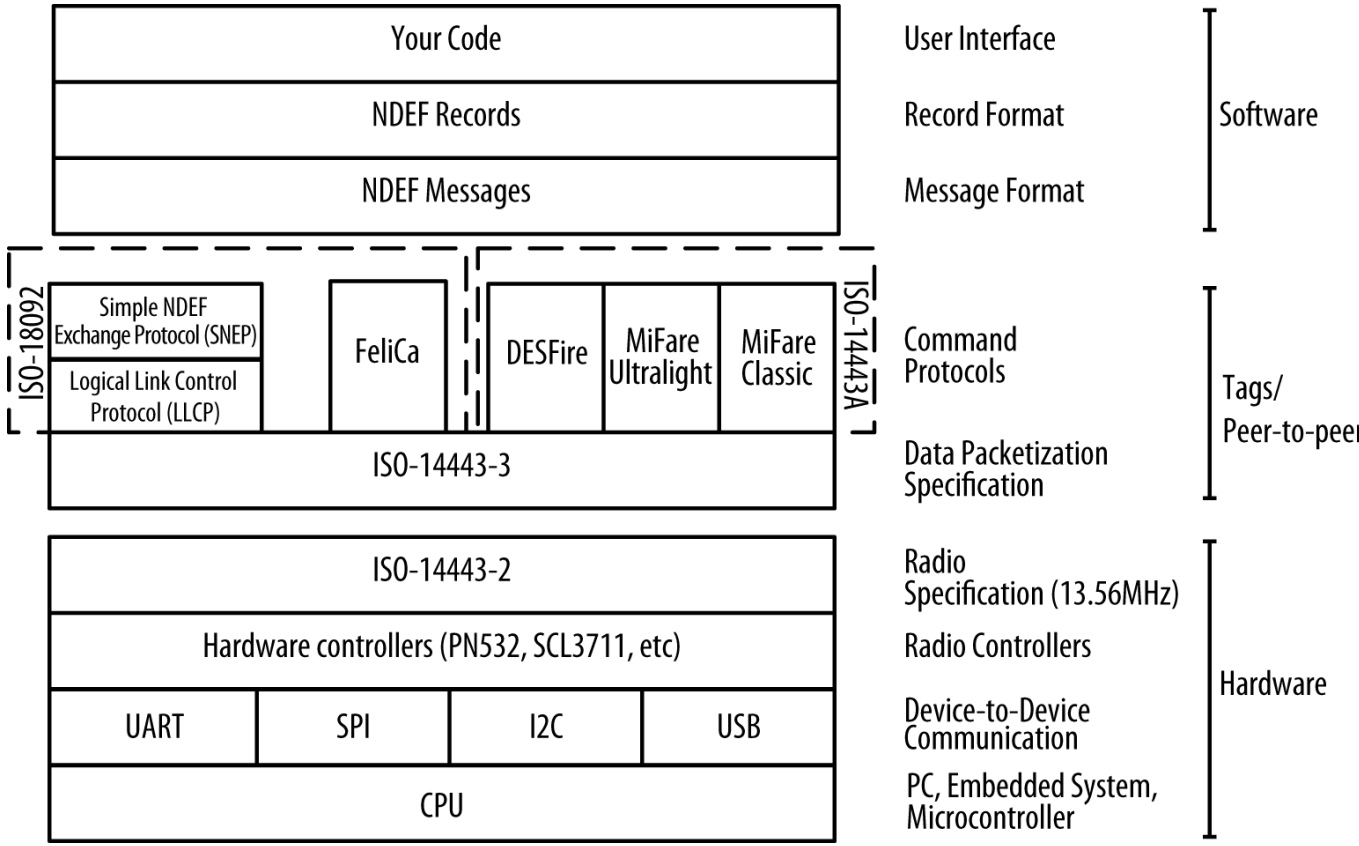
- **Type 3**
  - These are based on the Sony FeliCa tags (ISO-18092 and JIS-X-6319-4), **without the encryption and authentication** support that FeliCa affords.
  - Configured by factory to be read-only, or read/write capable.
  - Variable memory, **up to 1MB per exchange**.
  - Two communication speeds, 212 or 424Kbps.
  - Anti-collision support.
  - Example: Sony FeliCa.

Types of NFC Tags

- **Type 4**
  - Similar to type 1 tags, type 4 tags are based on NXP DESFire tag (ISO-14443A) specification.
  - Configured by factory to be read-only, or read/write capable.
  - 2, 4, or 8KB of memory.
  - Variable memory, up to 32KB per exchange.
  - Three communication speeds: 106, 212, or 424Kbps.
  - Anti-collision support.
  - Example: NXP DESFire, SmartMX-JCOP.

NFC Architecture

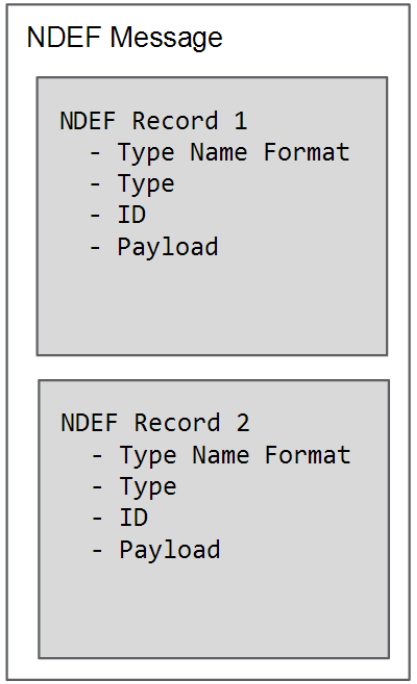




Source: Beginning NFC – Near field communication with Arduino, Android & PhoneGap, Tom Igoe, Don Coleman and Brian Jepson, O'Reilly, January 2014

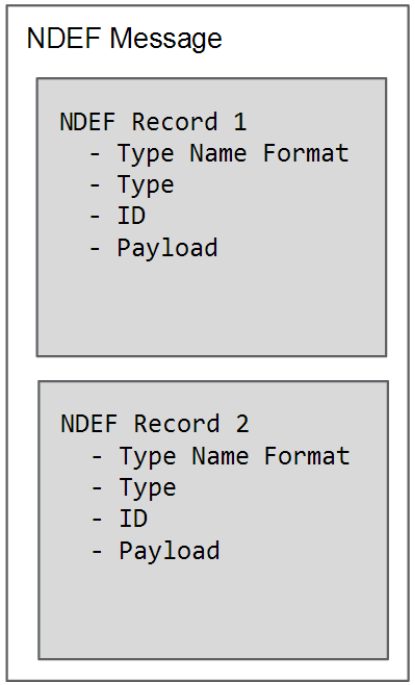
NDEF Message

- Reading NDEF (**NFC Data Exchange Format**) data from an NFC tag
  - By design, NDEF data is dispatched to only one activity
  - The type of the first NDEF record is used for dispatch
  - The data container format for NFC



NDEF Record

- **NDEF Message has at least 1 record**
  - Each record is a single piece of data

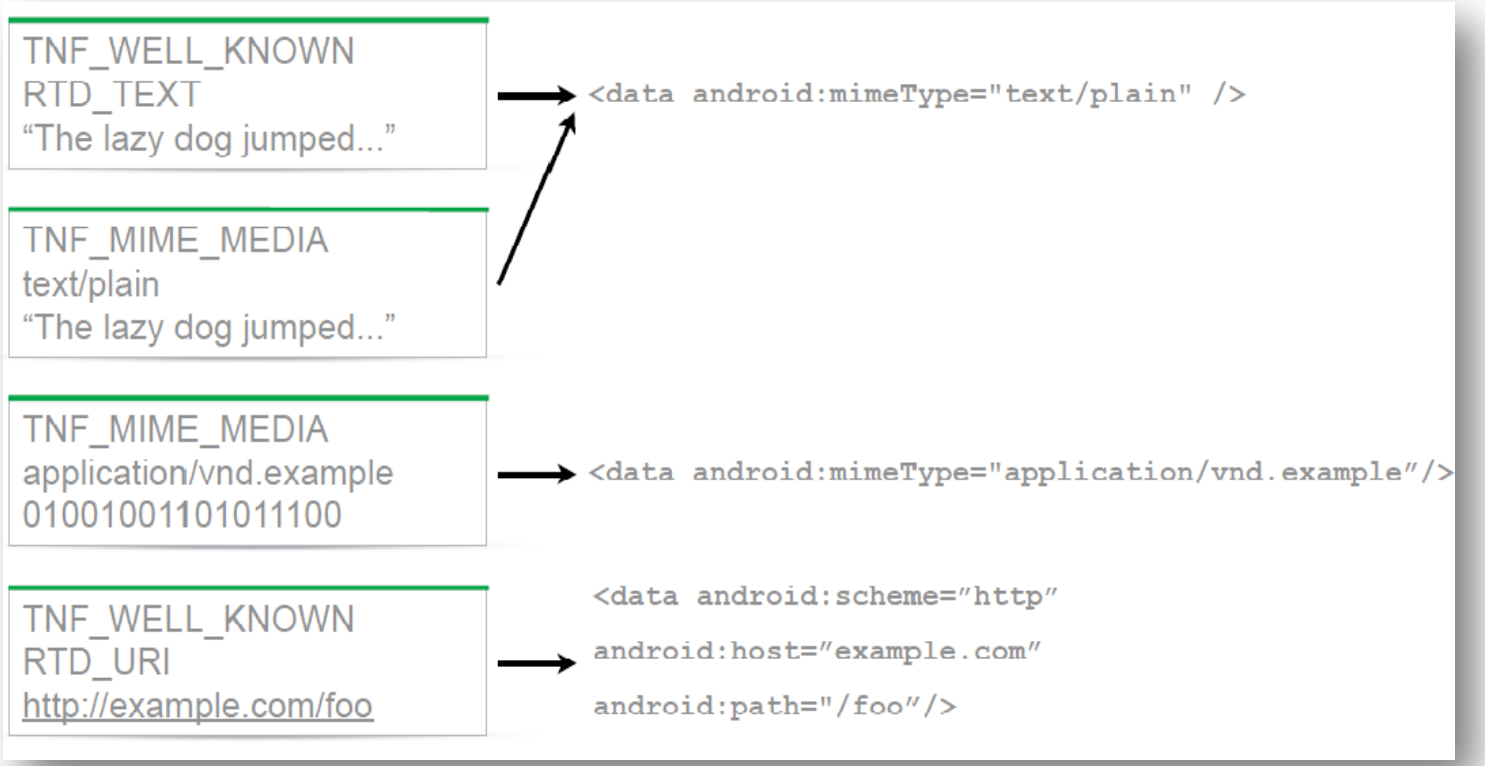



```
NdefRecord rec1 = new NdefRecord(
        short tnf, // Use NdefRecord.TNF_...
        byte[] type,
        byte[] id,
        byte[] payload);

NdefMessage msg = new NdefMessage(rec1, rec2);
```

NDEF Types

- Different Dispatch Types



NFC Data Exchange Format

- TNF set to NdefRecord.TNF_WELL_KNOWN
  - Type field contains well-known Record Type Definition
  - Use NdefRecord.RTD_URI for Uri record
  - Use NdefRecord.RTD_TEXT for Text record
- TNF set to NdefRecord.TNF_MIME_MEDIA
  - Type field contains mime-type, eg “image/jpeg”
  - Use “application.vnd/...” for app-specific mimes

Type name format	Type name	Description
MIME	text/x-vCard	Business card
MIME	text/x-vCalendar	Calendar note
NFC Forum RTD	urn:nfc:wkt:Sp	Smartposter
NFC Forum RTD	urn:nfc:wkt:U	URI record
NFC Forum Ext Type	urn:nfc:ext:nokia.com:bt	Bluetooth record (for printing/image frame)

http://wiki.forum.nokia.com/

NFC Capabilities on Android

- Support Android 2.3.3 (API 10) as the NFC APIs drastically changed from 2.3.2
- **New Intent Filter** and **TechFilter APIs** for registering interest in types of cards, types of NDEF messages, types of NFC events.4
- Android Ice Cream Sandwich 4.0 introduced a new peer-to-peer interaction model
  - 0-click contact sharing
  - 0-click web page sharing
  - 0-click youtube video sharing

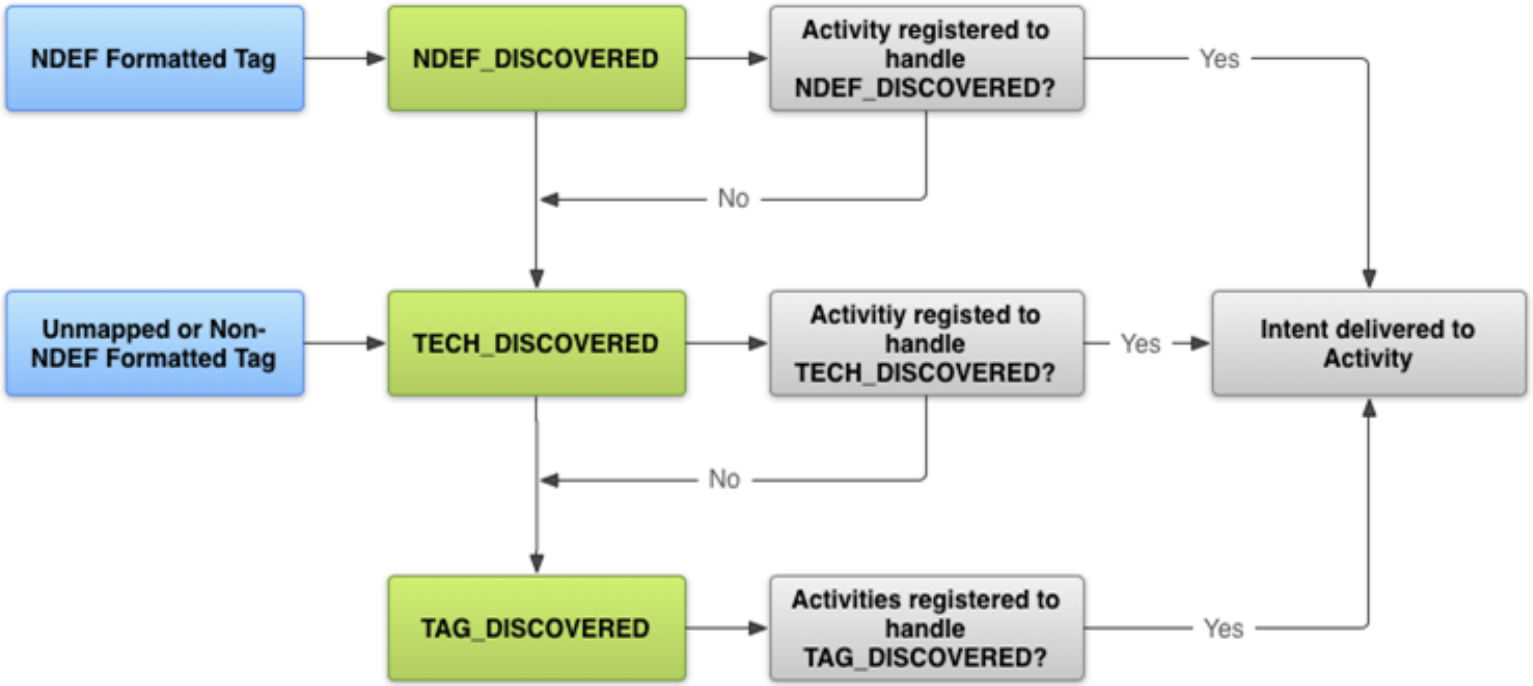
NFC Capabilities on Android

- Supported features
  - **Tag reader, writer**
  - **Tag emulation (of certain NFC NDEF tags)**
  - **P2P communication (Android specific)**
  - **Tag emulation of Smart Cards**
- Unsupported features
  - P2P communication with Nokia NFC phones
- Currently support on most phones

NFC Implementation

- Configure AndroidManifest.xml
  - Minimum SDK version
    - **<uses-sdk android:minSdkVersion="10" />**
  - Hardware permissions
    - **<uses-permissions android:name="android.permission.NFC" />**
    - **<uses-feature android:name="android.hardware.nfc" android:required="true" />**
  - Intent Filters
- Two possibilities how to use in application
  - **Intent Dispatch** – run your Activity on tag presence
  - **Foreground Dispatch** – intercept tag intents

NFC Implementation



NFC Intents

- Filter **ACTION_NDEF_DISCOVERED**

```
<intent-filter>
    <action android:name="android.nfc.action.NDEF_DISCOVERED"/>
    <category android:name="android.intent.category.DEFAULT"/>
    <data android:mimeType="text/plain" />
</intent-filter>
```

- If your activity filters for the **ACTION_TECH_DISCOVERED** intent, you must create an XML resource file that specifies the technologies that your activity supports within a **tech-list set.**

```
<resources xmlns:xliff="urn:oasis:names:tc:xliff:document:1.2">
    <tech-list>
        <tech>android.nfc.tech.IsoDep</tech>
        <tech>android.nfc.tech.MifareClassic</tech>
    </tech-list>
</resources>
```

Obtaining Information from Intents

- If an activity starts because of an NFC intent, you can obtain information about the scanned NFC tag from the intent. Intents can contain the following extras depending on the tag that was scanned:
  - **EXTRA_TAG (required):** A Tag object representing the scanned tag.
  - **EXTRA_NDEF_MESSAGES (optional):** An array of NDEF messages parsed from the tag. This extra is mandatory on intents.

```
public void onResume() {
      super.onResume();
          if (NfcAdapter.ACTION_NDEF_DISCOVERED.equals(getIntent().getAction())) {
           Parcelable[] rawMsgs =
        intent.getParcelableArrayExtra(NfcAdapter.EXTRA_NDEF_MESSAGES);

          //process the msgs array
      }
```

Reading NDEF Data

- AndroidManifest.XML

```
<intent-filter>
     <action android:name="android.nfc.action.NDEF_DISCOVERED" />
     <category android:name="android.intent.category.DEFAULT" />
     <data android:mimeType="text/plain" />
</intent-filter>
```

- *onResume* method in main Activity

```
@Override
   protected void onResume() {
            …
            if (NfcAdapter.ACTION_NDEF_DISCOVERED.equals(getIntent().getAction())) {
            NdefMessage[] messages = getNdefMessages(getIntent());
            byte[] payload = messages[0].getRecords()[0].getPayload();
            …
   }
```

Writing NDEF Data

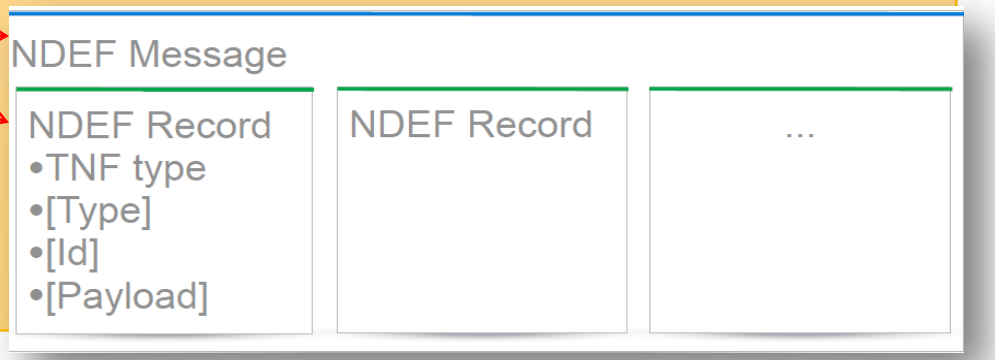
```
String text = "TAMZ2";

//Create NDEF record
NdefRecord textRecord = new NdefRecord(NdefRecord.TNF_MIME_MEDIA,"text/plain".getBytes(),
   text.getBytes());

//Put text into NDEF message
NdefMessage textMessage = new NdefMessage(new NdefRecord[]{textRecord});

//get TAG
Tag tag = getIntent().getExtra(NfcAdapter.EXTRA_TAG);
Ndef ndef = Ndef.get(tag);

ndef.writeNdefMessage(textMessage);
```



Writing P2P Data

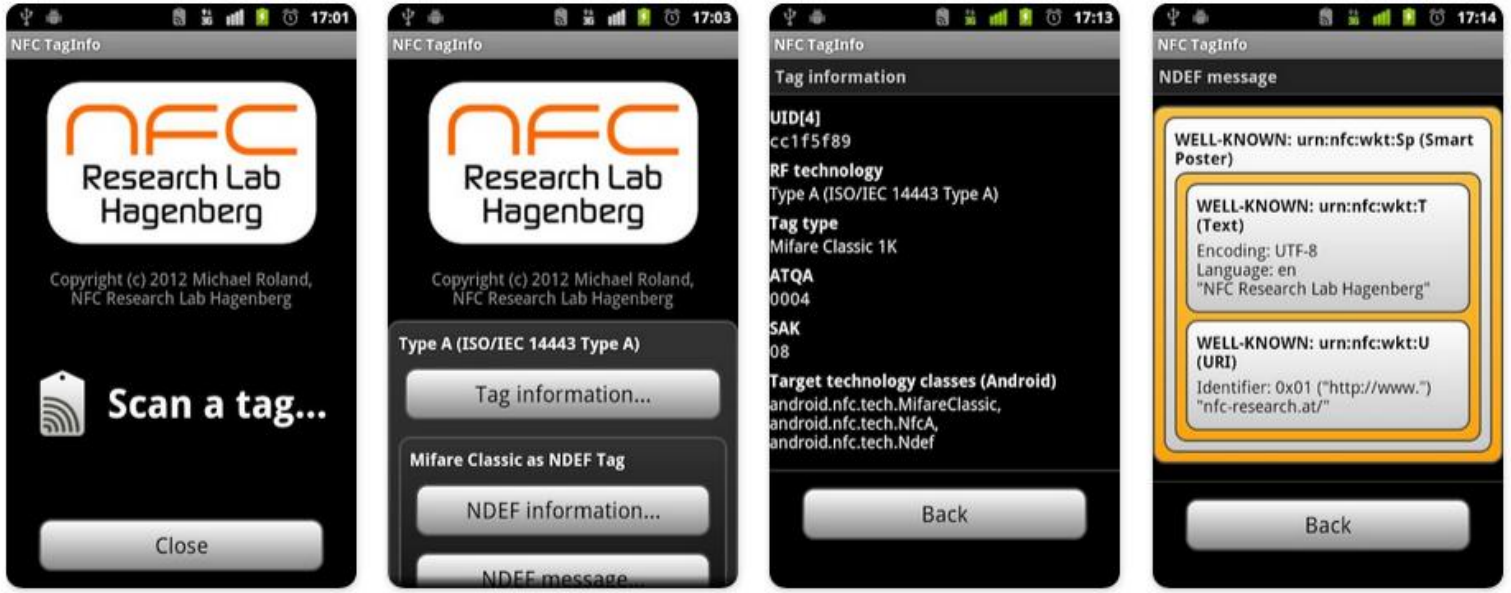
- Foreground Activities can register an NDEF payload for P2P push
  - adapter.enableForegroundNdefPush(this, ndefMessage);
- > Android 4.0 code
  - Register interest in P2P in advance, push the payload live

```
public interface NdefPushCallback {
   public NdefMessage createMessage();
}
adapter.registerForegroundNdefPush(this, callback);
```

- https://jessechen.net/posts/2011/how-to-nfc-on-the-android-platform

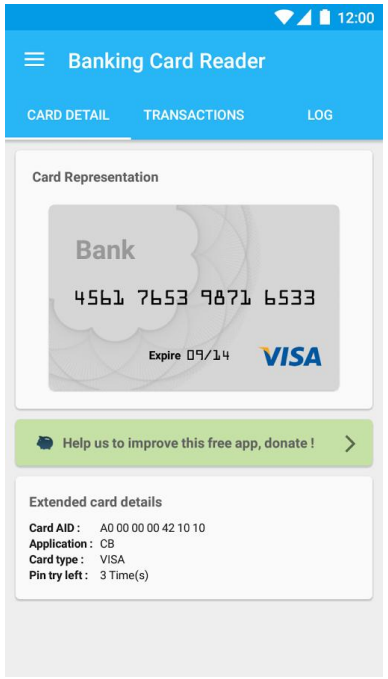
Useful NFC Applications

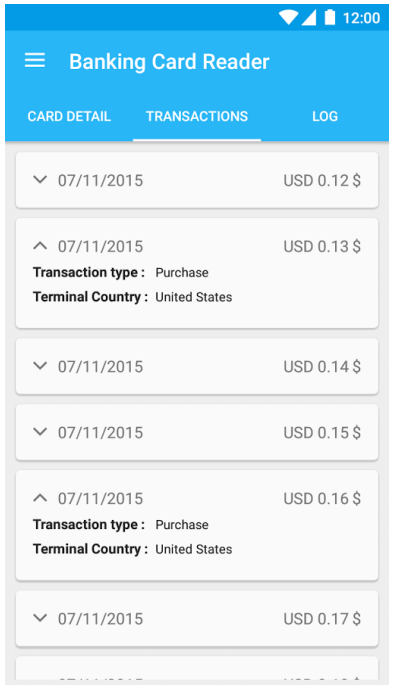
- **NFC TagInfo**
- https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo

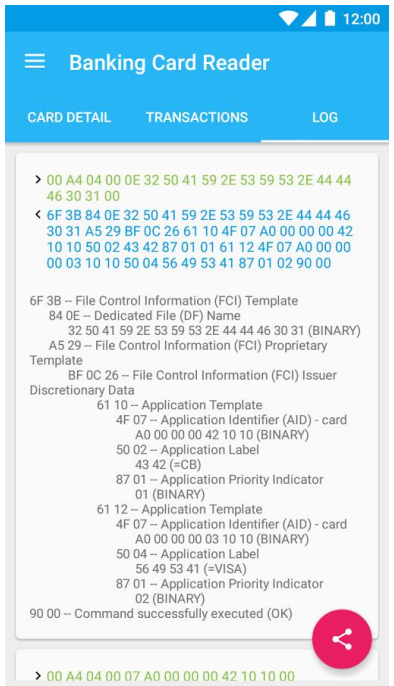


Useful NFC Applications

- **Credit Card Reader NFC**
- https://github.com/devnied/EMV-NFC-Paycard-Enrollment







Biometric Passports

- Combined **paper** and electronic passport that contains **biometric information**
- **RFID Contactless smart card** technology, including a microprocessor chip
- The passport's critical information is both printed on the data page of the passport and stored in the chip.
- **Public Key Infrastructure** (PKI) is used to authenticate the data stored
- The currently standardized biometrics used for this type of identification system are **facial recognition**, **fingerprint recognition**, and **iris recognition**.
- Only the digital image (usually in **JPEG** or **JPEG2000** format) is actually stored in the chip.

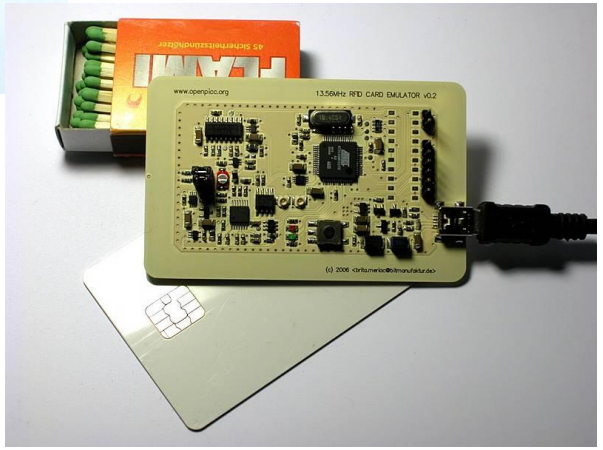
Biometric Passports

- **Data protection**
  - Non-traceable chip characteristics
  - **Basic Access Control (BAC)**
  - Passive Authentication (PA)
  - Active Authentication (AA)
  - Extended Access Control (EAC)
  - Supplemental Access Control (SAC)
  - Shielding the chip

- Erik Poll, E-passports, Digital Security Group Radboud University Nijmegen - https://www.cs.ru.nl/E.Poll/ufrj/C_ePassport.pdf
- epassport-reader - https://github.com/Glamdring/epassport-reader
- https://en.wikipedia.org/wiki/Biometric_passport

Hackers NFC/RFID Devices

- Proxmark III
- OpenPICC
- T4F OPEN RFID Tag
- PicNic
- Flipper Zero



Relay Attacks

- "Mole" reader gets close to target mobile device
- Attacker's mobile gets near POS terminal
- APDUs are passed via TCP/IP

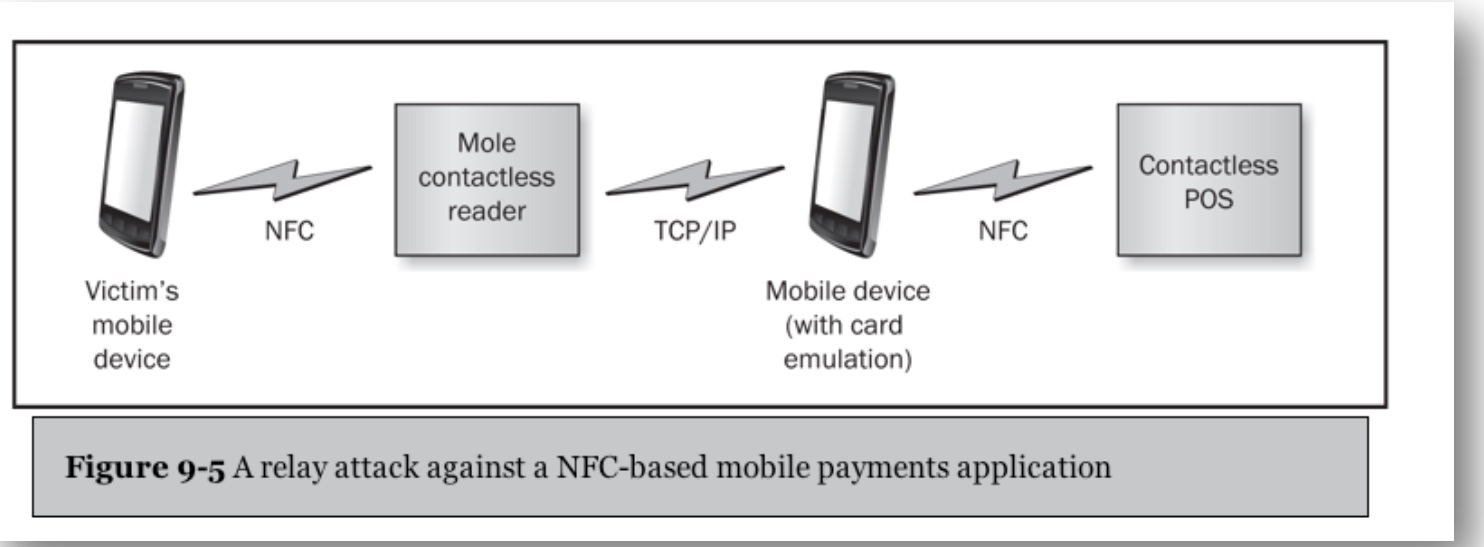


Figure 9-5 A relay attack against a NFC-based mobile payments application

Relay Attacks

- Relay Through a Malicious App
- Requires root privileges to bypass SE API signature authentication

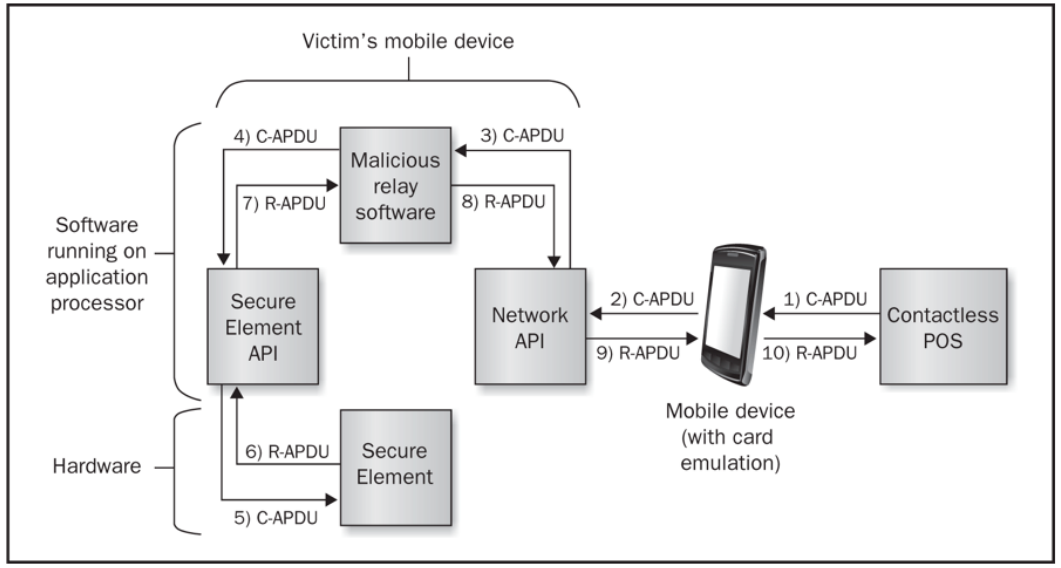


Figure 9-6 A next-generation relay attack against a NFC-based mobile payments application that exposes payment applets over the contact interface

References

- http://developer.android.com/reference/android/nfc/package-summary.html
- http://developer.android.com/reference/android/nfc/NdefMessage.html
- http://developer.android.com/reference/android/nfc/NdefRecord.html
- http://www.jessechen.net/blog/how-to-nfc-on-the-android-platform/
- Chris Gribe, Barcode/QR Code Technology

Thank you for your attention

Mgr. Ing. Michal Krumnikl, Ph.D.

+420 597 325 867

michal.krumnikl@vsb.cz

www.vsb.cz