Université Gustave Eiffel

INSTITUT D'ÉLECTRONIQUE ET D'INFORMATIQUE GASPARD-MONGE

MASTER 2 SSIO UPEM

Wireless access technologies

RFID/NFC case study

orange™

Samir Bellahsene
NFC-eSIM-IoT Technology Manager at Orange/TGI/CEP
samir.bellahsene@orange.com

September 2022

Contents

#1 Introduction

1.1 What is NFC ?

- NFC = Near Field Communications

  Near Field Communication (NFC) is a contact-less communication technology based on a radio frequency (RF) field using a base frequency of 13.56 MHz. NFC technology is perfectly designed to exchange data in a short range (< 10 cm) between two devices through a simple touch gesture.

1.2 What NFC does?

- Enables a smartphone / smartwatch as a wallet
- Provides access
- Smart Posters provide connection everywhere
- Sharing data
- Connecting two devices together
- recharges IoT devices

1.3 NFC by markets

- Retail and payment
- Mobility, Identity and transport
- Automotive
- Internet of Things (IOT)

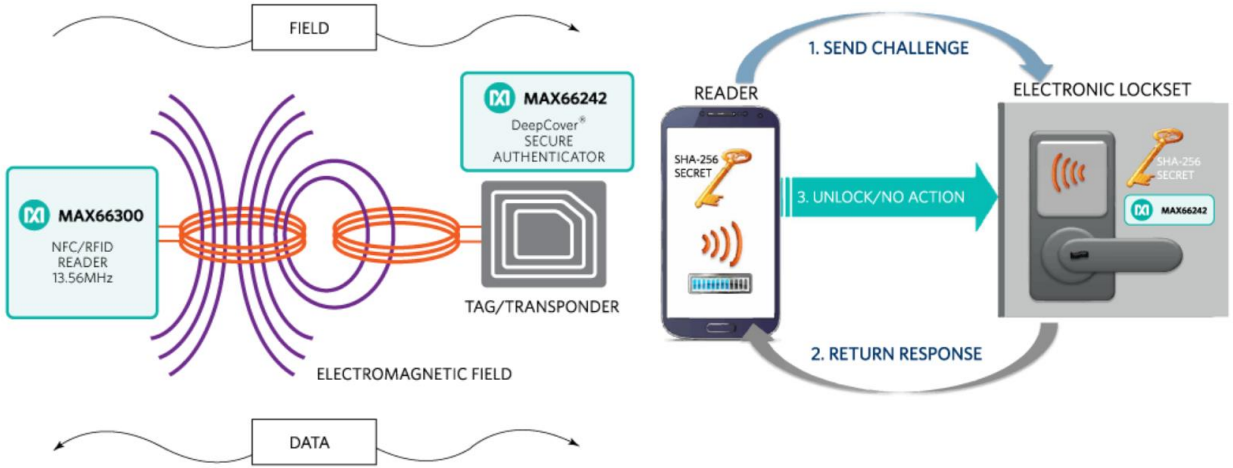
#2 NFC technology overview

2.1 NFC origins

- NFC concept started in the early of 2000s
- Sony and Philips (NXP Semiconductors today) were the mains contactless chip manufacturers
- Philips was dominating the markets with it's Mifare products family (Mifare based on the **ISO 14443-A** standard = type A)
- And Sony has its product family named Felica.
- Felica were not recognized by the International Organization for Standardization (ISO). Remains based on the Japanese Industrial Standrad (JIS) ➔ **JIS X6319-4.**
- 2002 : Philips and Sony with other industrials agreed to establish a technology specification and created a technical outline related to NFC.
- They established then : **ECMA 340** standard **(**ECMA= European Computer Manufacturers Association = European association for standardizing information) then, **ISO 18092 (**based mostly on the already existing standards : ie ISO 14443A & JIS X6319-4 and covers almost all the specifications present in ECMA 340 and introduced new communication modes).
- These standards were evolved to include ISO 14443B (type B) used mainly in the NFC public transport accesses

2.2 From RFID to NFC (1/2)

- NFC is an extension of RFID contactless technology
- RFID: Radio-Frequency Identification
- RFID encompasses communication technologies that use electromagnetic (radio) waves, part of electromagnetic spectrum, to communicate between RFID tags (transponders) and readers (interogators). RFIDs are mainly used to identify individual items, places, animals, people, control accessess…
- NFC standards specifications were inherited from those of RFID and the principles of near field communication are already defined or present in RFID systems

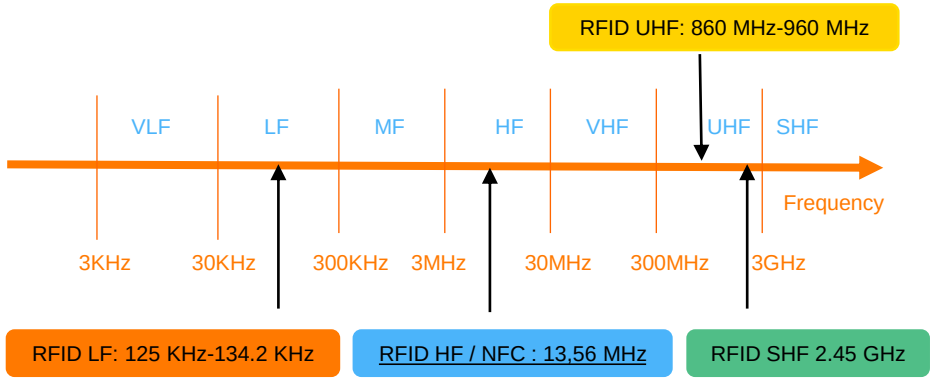


Source. Maxim integrated

2.2 From RFID to NFC (2/2)

- There are many frequency bands available for RFID systems
- Different standards are then defined to specify the working rules for each RFID system in each frequency band
- Different types of RFIDs : working distance (wave range), working frequency band, modulation and information coding
- Example : ISO 14443 and JIS X6319-4 (NFC communication standards = proximity) and ISO 15693 (RFID vicinity) are defined around the frequency band 15,56 Mhz.
- NFC is governed by the same communication standards than a High Frequency (HF) RFID

Frequency Range	Frequency band	Range
LF	120–150 kHz	10 cm-50 cm
HF	13,56 MHz	10 cm–1 m
UHF	433 MHz	1–100 m
UHF	865-868 MHz (Europe) 902-928 MHz (North of America)	1–12 m
SHF	2450-5 800 MHz	1–2 m

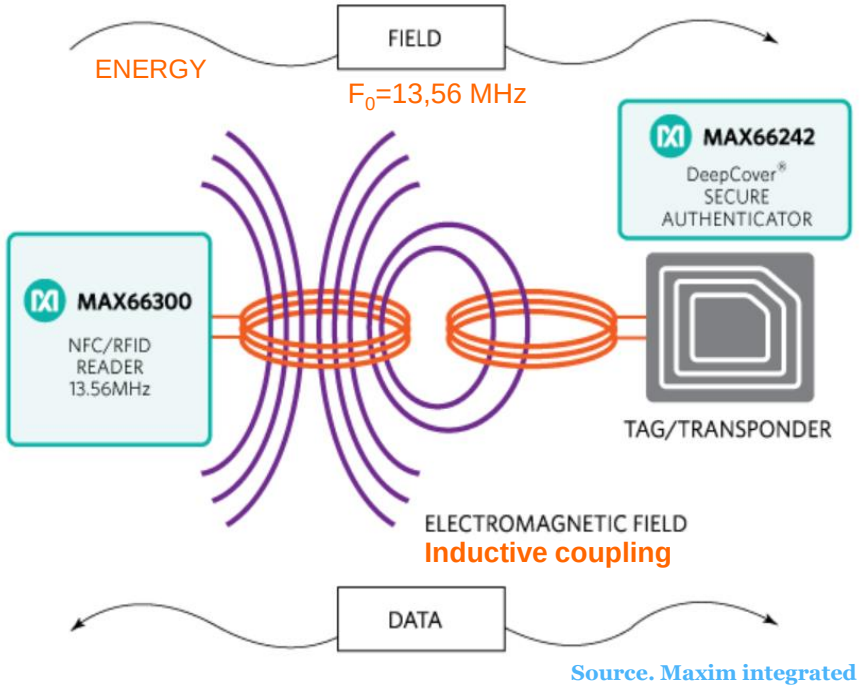


Source. Techniques de l'Ingénieur. La technologie NFC -Principes de fonctionnement et applications

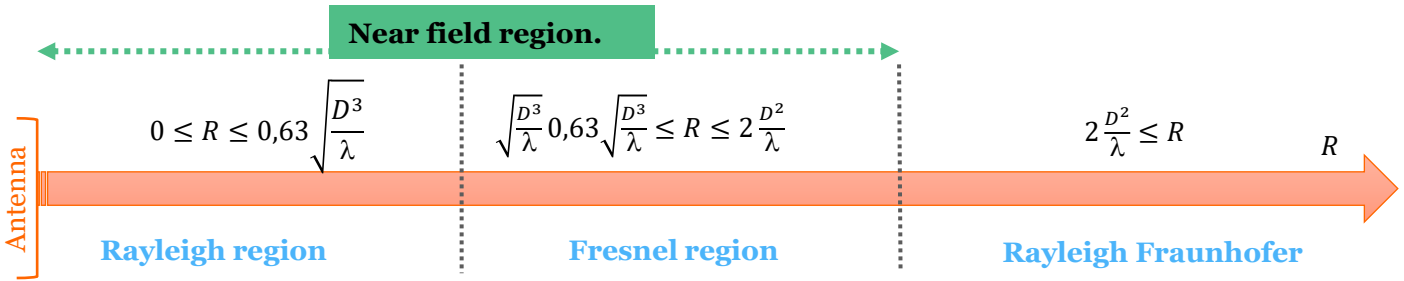
2.3 How a near field communication works? (1/4)

- LF and HF RFIDs like NFC are systems working in a near field range.
- NFC is an extension of RFID HF
- 3 regions of the propagation area : Near field area, intermediary, and far field.
  - Near field ➔ Inductive coupling
  - Intermediary field (remote coupling) ➔ Inductive or capacitive coupling
  - Far filed ➔ backscattered (capacitive) coupling
- Near field $\Rightarrow R < 2\frac{D^2}{\lambda}$. If f_0 = 13,56 MHz $\Rightarrow$ Near field is about tens of centimeters.

Where R= distance between reader & transcoder antennas; D= antenna diameter; λ= wavelength



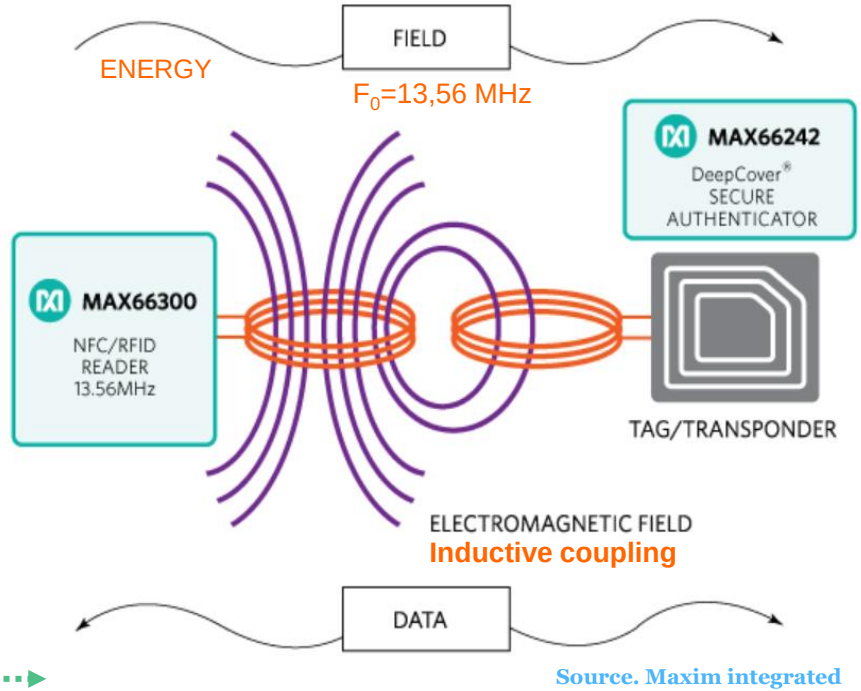
Source. Maxim integrated



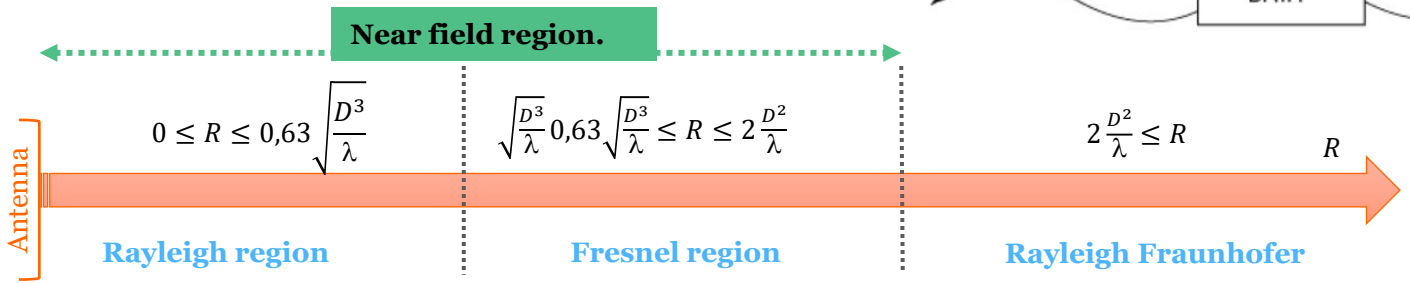
Source. Techniques de l'Ingénieur. La technologie NFC -Principes de fonctionnement et applications

2.3 How a near field communication works? (2/4)

- Near field $\Rightarrow R < 2\frac{D^2}{\lambda}$. If f_o = 13,56 MHz $\Rightarrow$ Near field is about tens of centimeters.
- More difficult for attackers to record the communication between an NFC reader and an NFC Tag compared to other wireless technologies which have a working distance of several meters
- The user of the NFC reader determines by the touch gesture with which entity the NFC communication should take place $\Rightarrow$ more difficult for the attacker to get connected $\Rightarrow$ High security level of the NFC communication compared to other wireless technologies.
- Other mechanisms are added to the NFC technologies to provide high level of security that we will see later.



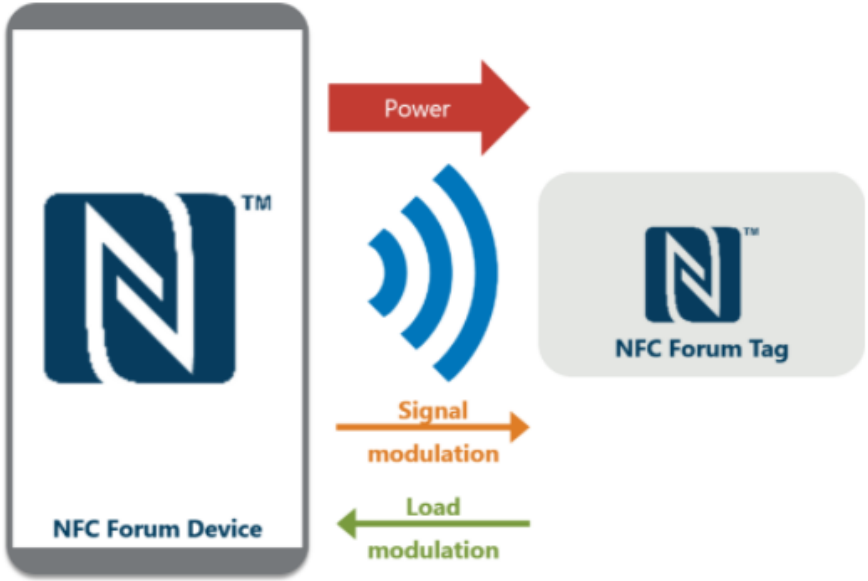
Source. Maxim integrated



Source. Techniques de l'Ingénieur. La technologie NFC -Principes de fonctionnement et applications

2.3 How a near field communication works? (3/4)

- The NFC reader communicate with an NFC tag over the generated RF field.
- The NFC tags don't need batteries or other power supplies for operation as the necessary power for communication is provided by the RF field. This technology is also ideal for small IoT devices acting as an NFC tag as no additional power is needed for the NFC communication.
- For Wireless Charging the primary goal of NFC Technology is to transfer power, thus extending communication. In this case NFC communication is used to regulate the power transfer. When Wireless Charging mode is active the field strength of the RF field can be increased allowing a power transfer of up to 1 W.
- The NFC device is sending information to an NFC Tag by modulating the RF field signal (signal modulation).
- The NFC device is receiving information from an NFC tag by sensing the modulation of the load generated by the NFC tag (load modulation).



2.3 How a Near Field Communication works? (4/4)

Information coding and modulations used in ISO 14443 A/B and JIS X 6319-4

	ISO 14 443 Type A	ISO 14 443 Type B	JIS X 6319-4
Modulation PCD → PICC	ASK (Amplitude Shift Keying) 100 %	ASK 10 %	ASK8-30 %
Modulation PICC → PCD	106 kbps : Load Modulation with subcarrier (OOK=On Off Keying) (fc/16 = 847.5 kHz). 212, 424 kbps : subcarrier BPSK	Load Modulation with subcarrier (BPSK) (fc/16 = 847.5 kHz)	Load Modulation with subcarrier (OOK)
Coding PCD → PICC	Miller modified	NRZ	Manchester
Coding PICC → PCD	Miller modified NRZ-L (212, 424 and 848 kbits/s)	NRZ-L	Manchester
Bit rate Kbytes/sec	106, 212, 424 et 848	106, 212, 424 and 848	212 and 424

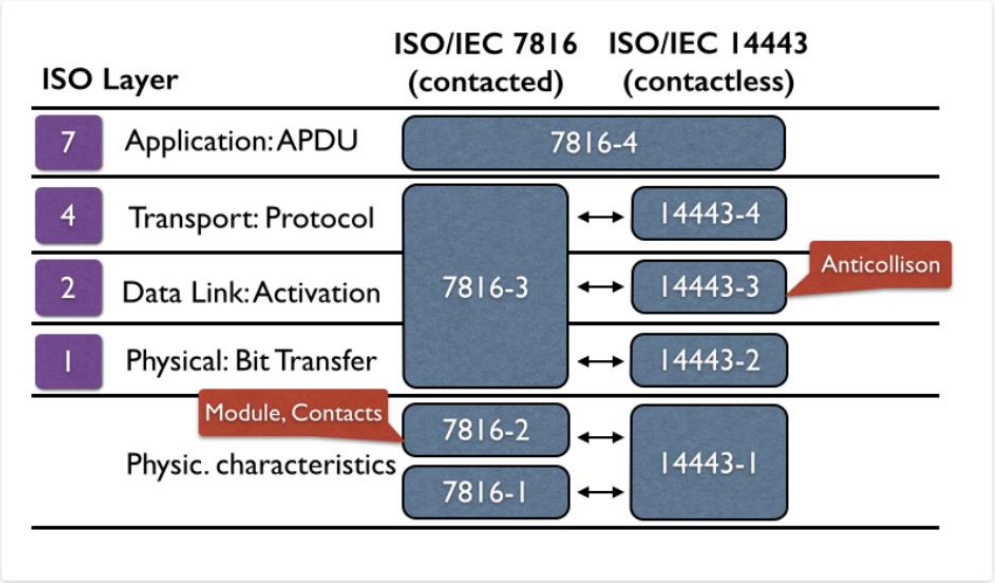
- PCD (Proximity Coupling Device) refers to the NFC/RFID reader named also interrogator
- PICC (Proximity Integrated Circuit Card) refers to the NFC/RFID tag also called transponder

Source. Techniques de l'Ingénieur. La technologie NFC -Principes de fonctionnement et applications

#3 NFC related standards and protocols

3.1 NFC related standards & protocol stacks (1/2)

- As NFC has inherited from RFID standards ⇒ NFC is defined by different organization standards (ISO, ECMA, ETSI, JIS, etc).
- NFC's anterior known RFID communication and testing conformity standards :
  - Communication: ISO 14443 (A & B), JIS X6319-4 and ISO 15693
  - Testing conformity: ISO 10373-7 (associated to Com. ISO 15693), ISO 10373-6 (associated to Com. ISO 14443)
- ISO 14443 common used standard for contactless cards, 10 mW, working distance ~10 cm; bit rate: ~some kbits
  - 14443-1 contactless integrated circuit cards: physical characteristics
  - 14443-2 contactless integrated circuit cards: radio frequency power and signal interface
  - 14443-3 contactless integrated circuit cards: initialization and anti-collision
  - 14443-4 contactless integrated circuit cards: transmission protocol
- Difference between NFC type A and B starts from layer ISO 14443-2
- ISO/IEC 7816 is a contacted standard that we will detail later (example : communication between NFC SIM Card (UICC) and a device modem).



Source. Protocolbench. Smart Cards in context of ISO/OSI Layer Model

3.1 NFC related standards & protocol stacks (2/2)

- Lower layers interfaces : NFC-IP1 and NFC-IP2 (NFC-Interface & Protocols) defined respectively by ECMA 340 (or ISO 18092) and ECMA 352 (ISO 21481).

- NFC-IP1- ECMA 340
  - Communication modes for NFCIP-1 using inductive coupled devices operating at 13,56 MHz.
  - Active and Passive communication modes for a communication between NFC devices.
  - modulation schemes, coding, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization.
  - transport protocol including protocol activation and data exchange methods.

- NFC-IP2 –ECMA 352 :
  - Communication mode selection mechanisms for devices implementing ECMA-340, ISO/IEC 14443 or ISO/IEC 15693 and operating in 13,56 MHz frequency.
  - NFC Mode, Proximity Coupling Device mode (PCD), Vicinity Coupling Device mode (VCD) and Proximity Integrated Circuit Card mode (PICC)

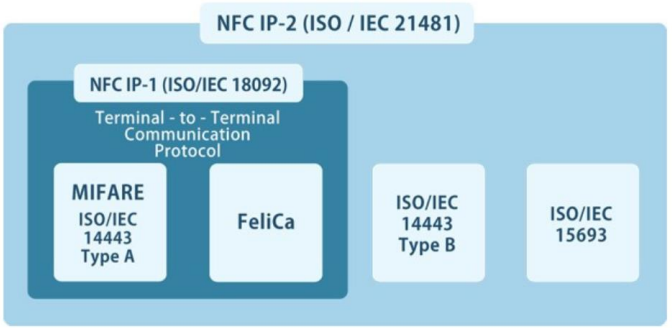
NFCIP-2 device: ISO/IEC 21841 entity

NFC MODE: mode in which an NFCIP-2 device operates as specified in ECMA-340

PICC MODE: mode in which an NFCIP-2 device operates as a Type A or Type B Proximity Integrated Circuit Card or Object as specified in ISO/IEC 14443-2, ISO/IEC 14443-3 and ISO/IEC 14443-4

PCD MODE: mode in which an NFCIP-2 device operates as a Proximity Coupling Device as specified in ISO/IEC 14443-2, ISO/IEC 14443-3 and ISO/IEC 14443-4

VCD MODE: mode in which an NFCIP-2 device operates as a Vicinity Coupling Device as specified in ISO/IEC 15693-2 and ISO/IEC 15693-3



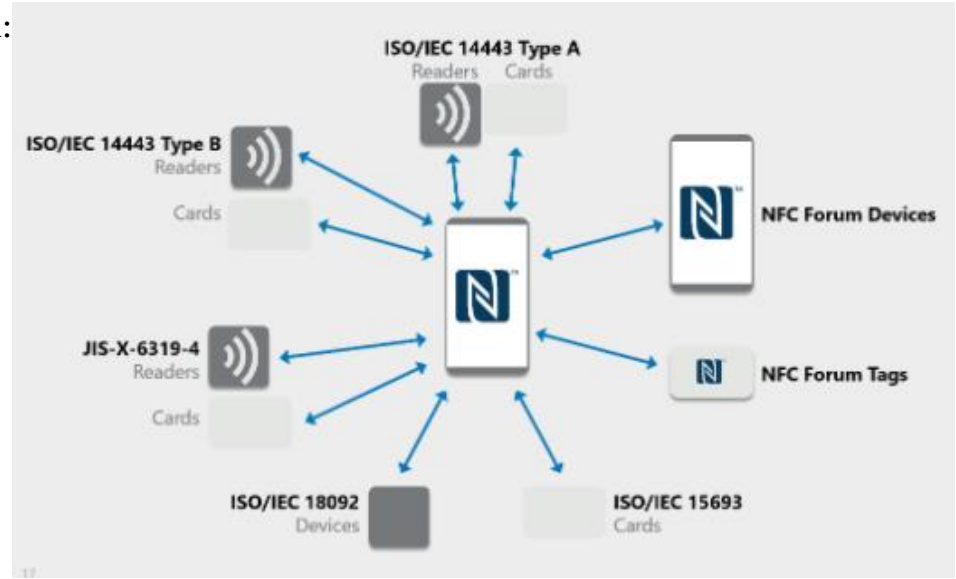
Source. eInfochips, an Arrow company

3.2 NFC Forum for better technology harmonization and standardization (1/2)

- NFC forum is a private organization established between different industrials which takes the role of technology harmonization and organization.
- Certifies NFC devices/tags for better interoperability between the different existing standards
- Provide a framework for application development and technology implementation and security of transactions. It is similar to EPCglobal/GS1 for UHF RFID.
- NFC Forum develops standards in the following areas: protocol Technical Specification; Data Exchange Format Technical Specification; NFC Forum Tag Type Technical Specifications – 5 tag types (as of Jun 2016); Record Type Definition Technical Specifications; Reference Application Technical Specifications

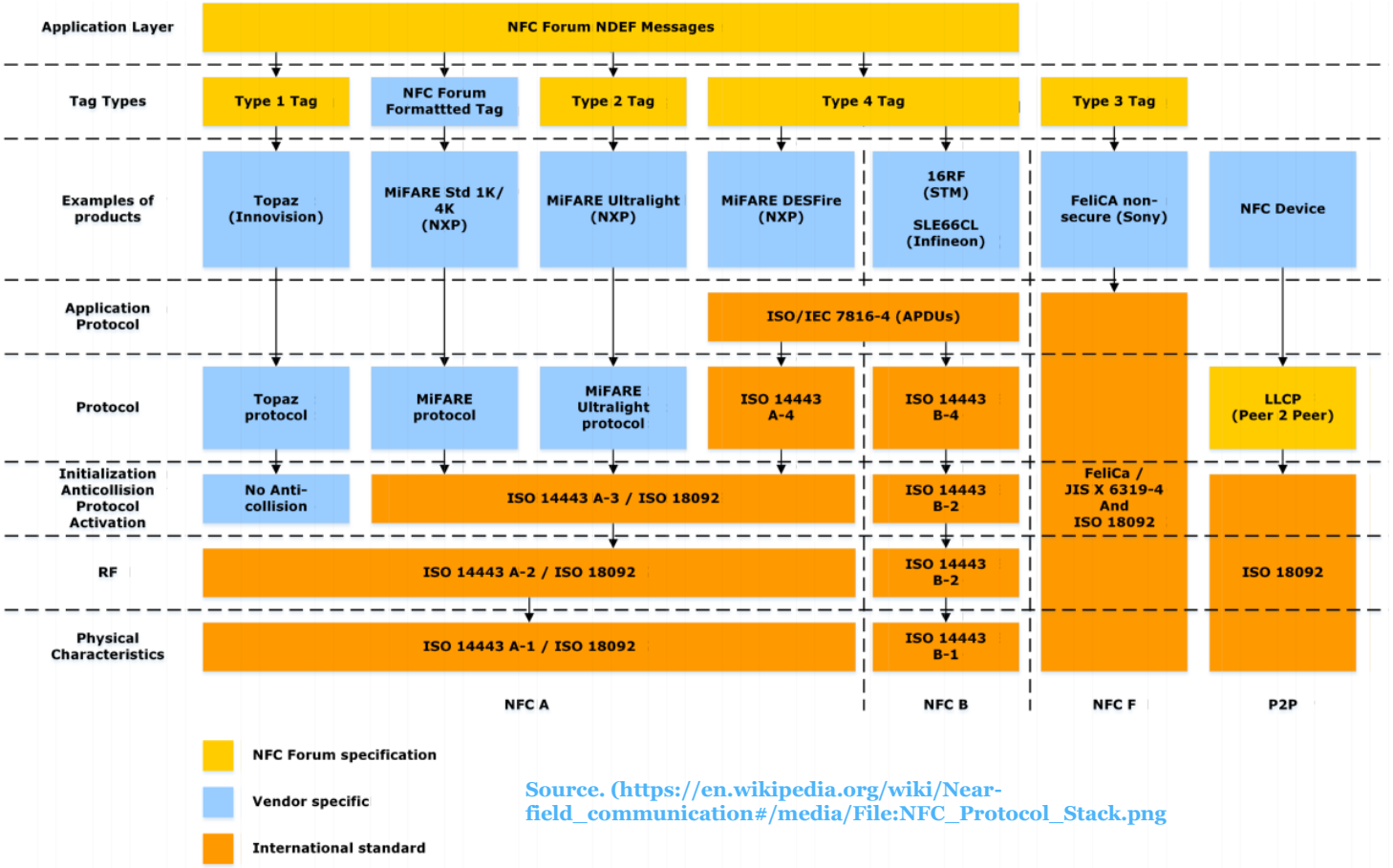
3.2 NFC Forum for better technology harmonization and standardization (2/2)

- Several different existing contact-less communication protocols in the market
- With different coding methods for signal and load modulation
- NFC Forum **(define maybe the organization in a slide at the beginning?)** created a set of specifications allowing NFC Forum Devices to use these different communication protocols
- A certified NFC Forum device is able to communicate with:
  - Readers and cards compliant to the ISO/IEC 14443 Type A standard
  - Readers and cards compliant to the ISO/IEC 14443 Type B standard
  - Cards compliant to the ISO/IEC 15693 standard
  - Devices compliant to the ISO/IEC 18092 standard
  - Readers and cards compliant to the JIS-X 6319-4 standard
  - NFC Forum Tags
  - Other NFC Forum Devices



- **Depending on the communication protocol used and the capability of the remote device, a communication speed of up to 424 Kbit/s is supported by NFC Forum Devices.**

3.3 Interroberability between differents technologies and standards (1/3)



Source. (https://en.wikipedia.org/wiki/Near-field_communication#/media/File:NFC_Protocol_Stack.png

3.3 Interroberability between differents technologies and standards (2/3)

- NFC reader shall be able to read transponders from different standards (ISO 14443 (A or B) or JIS X6319-4 even if the coding, modulation or data frames are different
- NFC Forum was established to guarantee this interoperability and provide a better harmonization for the NFC technology
- Definition of NFC forum Device and NFC forum Tag
- Five types of tags : defined by following the used technology, by product families and manufacturers, the size and type of memory (EEPROM, microprocessor, etc
- Type 1 & type 2 are based on ISO 14443A. Type 3 on JIS X6319-4 (NFC F : Felica). Type 4 on ISO 14443 (NFC A & B) and Type 5 on ISO/IEC 15693 (NFC-V).
- With these types, NFC Forum aims to guarantee the interoperability between different manufacturers

3.3 Interroberability between differents technologies and standards (3/3)

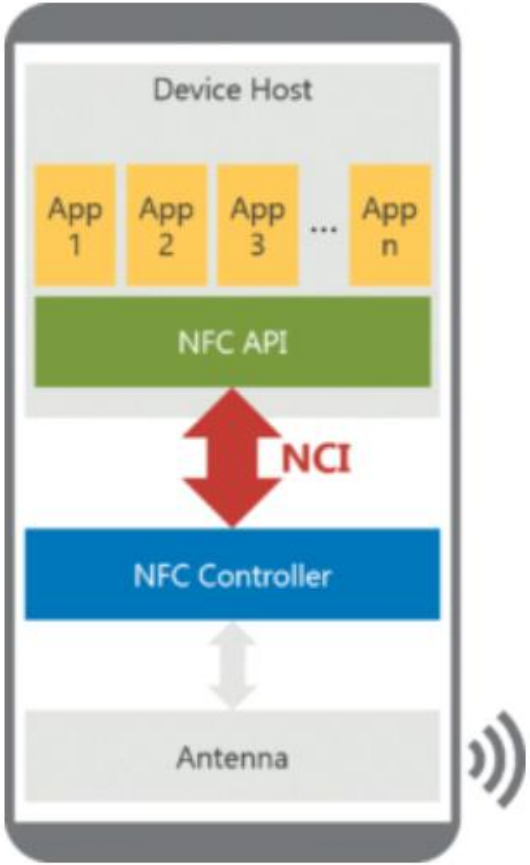
Tag Type	Use Case	Chip Examples	User Memory (bytes)*	UID Length (bytes)	Cost
Forum Type 1 ISO 14443 A	Specialized	Innovision Topaz	90 - 454	4	$
Forum Type 2 ISO 14443 A	Most common, low cost, single application like smart poster, personal label etc.	NXP MIFARE UL, MIFARE UL-C, NTAG 203, 210, 212 etc.	46 – 142	7	$
Forum Type 3 JIX S6319 4	Specialized, Asian markets	Sony FeliCa (Lite)	224 – 3984	8	$$$
Forum Type 4 ISO 14443 A ISO 14443 B	High memory applications, high security (in non NFC mode)	NXP MIFARE DESFire EV1 -2K, 4K, 8K, Inside Secure VaultIC 151/161, HID Trusted Tag™	1536 - 7678	7	$$$
Forum Type 5 (NFC-V / ISO 15693)	If longer read range is required, industrial rugged tags – added as forum tag type June 17, 2015.	NXP ICODE SLIx family, EM4233, Fujitsu FRAM MB89R118C, MB89R112, HID Vigo™	32 – 8192 (112 for ICODE SLIx)	8	$ - $$$
MIFARE Classic	Very common, high memory Not compatible to all devices!	NXP Mifare Classic 1K, 4K	716 - 3356	4 or 7	$$

Source. https://rfid4u.com/nfc-standards-nfc-forum/

#4 NFC operation modes

4.1 Schematics of NFC Forum Devices

- NFC Controller connected with an antenna transmits and receives all NFC communication frames of the NFC Forum Device.
- NFC applications which are initiating and managing the NFC transactions are either:
  - apps located in the Device Host using the NFC API of the operating system inside the NFC Forum Device or are
  - located inside an optional available secure element directly connected to the NFC Controller.
- To support the implementation of interoperable NFC Forum Devices, the NFC Forum has defined the NFC Controller Interface (NCI) between an NFC Controller and the Device Host of the NFC Forum Device.

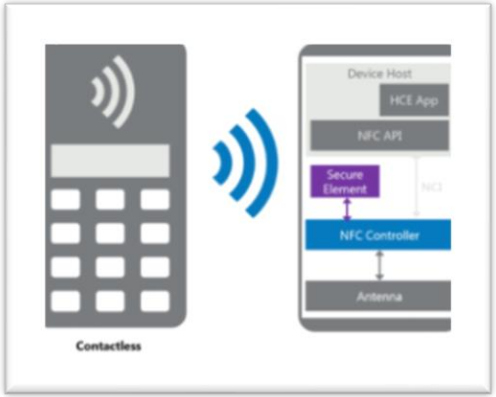


4.2 Operation modes of a NFC devices

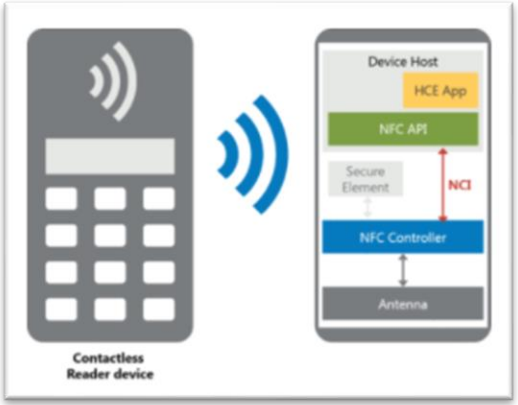
Reader/Writer mode

Peer-to-Peer mode

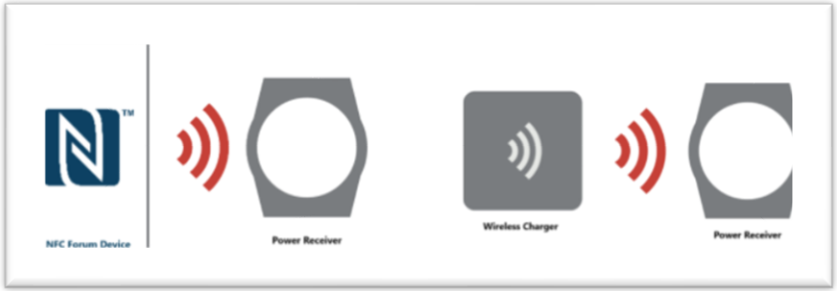
Card Emulation mode



Host Card Emulation mode



Secure Element based Card Emulation mode



Wireless Charging Mode

4.2.1 Reader / Writer mode

- NFC The NFC Forum Device operates like a contact-less reader device which is able to communicate with contact-less tags or cards. A typical use case is to read smart posters, opening a specific internet web site for example
- The Reader/Writer Module covers the behavior of an NFC Forum Device implementing Poll Mode behavior in combination with the Reader/Writer functionality.
- Poll Mode : a mode of an NFC Forum Device when it generates a carrier and polls for other devices .
- Ability to read and/or write to a Type 1 Tag, Type 2 Tag, Type 3 Tag, Type 4A/B Tag and Type 5 Tag.

4.2.2 Peer-to-Peer mode

- Two NFC Forum Devices are touched together to exchange data. This mode is used to easily exchange the contact data of the device users for example.

4.2.3 Card Emulation mode

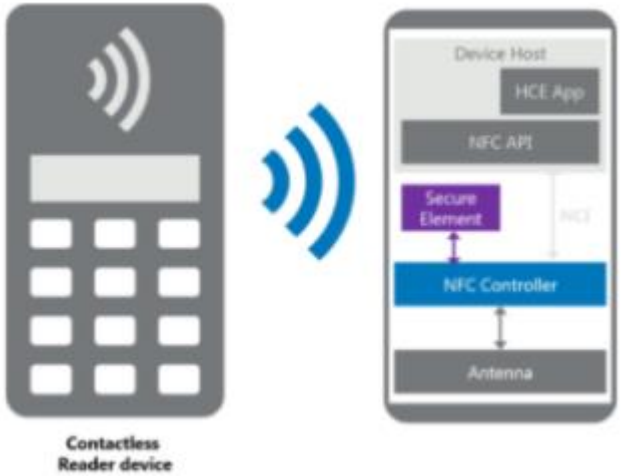
- The NFC Forum Device operates like a contact-less card that is able to communicate with a contact-less reader device. Typical use cases are the emulation of contact-less banking cards to perform money transactions or to emulate contact-less tickets for public transport.

4.2.4 Host Card Emulation mode

- With this implementation, an HCE app located in the Device Host is taking care of emulating the contact-less card. In this configuration, the NFC Controller is forwarding all received contact-less commands to the Device Host. The HCE app can then communicate with the contactless reader device by using the NFC API.

4.2.5 Secure Element based Card Emulation mode

- With this mode, the emulation of the contact-less card is managed by a secure element inside the NFC Forum Device. This Secure Element can be either a security chip embedded in the NFC Forum Device or an NFC enabled SIM card inserted in the NFC Forum Device. For both solutions, the commands received from the contactless reader will be forwarded to the secure element for processing. This implementation allows the same high-security level for transactions as those provided by contact-less smart card solutions.



4.2.6 Wireless Charging mode

- This mode is used to transfer power. Communication is performed to manage the power transfer. The NFC Wireless Charging mode allows the contact-less transfer of up to 1 W power. This mode will charge small IoT devices with a limited power supply such as a Bluetooth headset, fitness tracker or smartwatch. NFC Forum Devices capable of the Wireless Charging mode have the ability to charge these kinds of IoT Devices.

Alternatively, these IoT Devices can be also charged by dedicated NFC Wireless Chargers

4.3 Listening for remote NFC devices

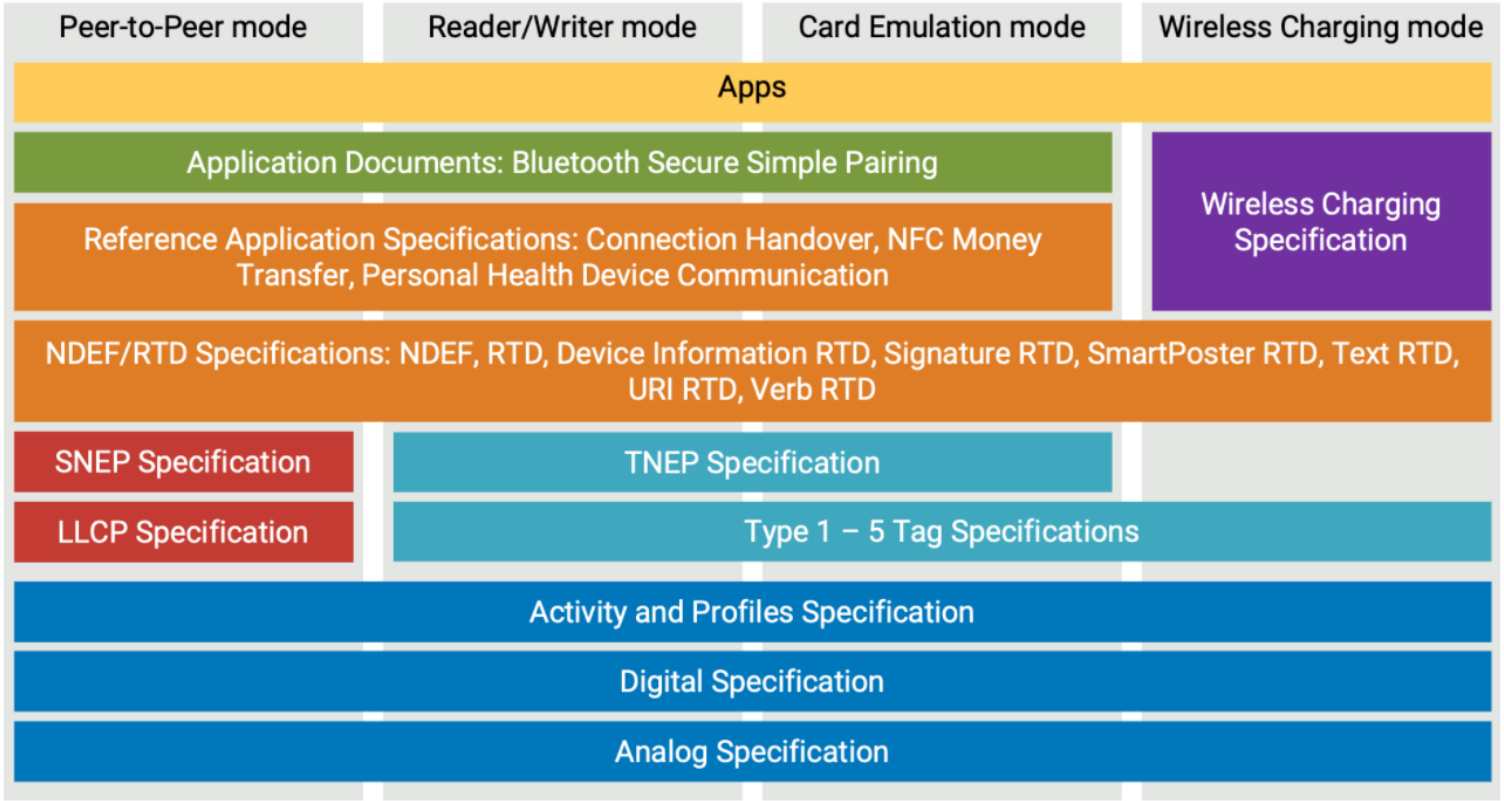
- These operating modes are available at the same time as the NFC Forum Device generates periodically for a short time frame an RF field to sense for a remote device (Poll Mode). The NFC Forum Device will initiate a Reader/Writer, Peer-to-Peer or Wireless Charging operation mode in the event a remote device is detected. The rest of the time the NFC Forum Device listens for communication requests from remote contact-less reader devices or NFC Forum Devices and answers to their communication requests.

- As the time period for generating a RF field is significantly shorter than the listen time period the reception of NFC communication requires only a relatively low power supply. The user will normally not identify a significant reduction in the battery run time on his/her mobile NFC Forum Device when enabling the NFC function all the time.

#5 NFC Forum specifications overview

5. NFC Forum specifications overview (1/7)

❑ Build Solutions and Ensure the Global Interoperability



5. NFC Forum specifications overview (2/7)

5.1 Peer-to-Peer Technical specifications

❑ Logical Link Control Protocol Technical Specification (LLCP):

- Defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications. The specification defines two service types, connectionless and connection-oriented, organized into three link service classes: connectionless service only; connection-oriented service only; and both connectionless and connection-oriented service. The connectionless service offers minimal setup with no reliability or flow-control guarantees (deferring these issues to applications and to the reliability guarantees offered by ISO/IEC 18092 and ISO/IEC 14443 MAC layers). The connection-oriented service adds in-order, reliable delivery, flow-control, and session-based service layer multiplexing.
- LLCP is a compact protocol, based on the industry standard IEEE 802.2, designed to support either small applications with limited data transport requirements, such as minor file transfers, or network protocols, such as OBEX and TCP/IP, which in turn provide a more robust service environment for applications. The NFC LLCP thus delivers a solid foundation for peer-to-peer applications, enhancing the basic functionality offered by ISO/IEC 18092, but without affecting the interoperability of legacy NFC applications or chipsets.

❑ Simple NDEF Exchange Protocol Technical Specification

- The Simple NDEF Exchange Protocol (SNEP) allows an application on an NFC-enabled device to exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device when operating in NFC Forum peer-to-peer mode. The protocol makes use of the Logical Link Control Protocol (LLCP) connection-oriented transport mode to provide a reliable data exchange.

5. NFC Forum specifications overview (3/7)

5.2 Data Exchange Technical Specifications

❑ NFC Data Exchange Format (NDEF):

- The NFC Data Exchange Format Technical Specification provides a standard format for NFC application data and RTD specifications specify the format and rules for building standard record types used by NFC Forum application definitions and third parties that are based on the NDEF data format. Application level specifications are important for use cases that require an exchange of control information, such as smart posters and remote control, because message format is defined and issues that must be considered for implementation are addressed. The RTD specifications provide 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.

❑ Connection Handover (CH) Technical Specification 1.5

- The updated version of the NFC Forum Connection Handover Technical Specification (CH 1.5) is the first NFC Forum specification to take advantage of TNEP. By defining the messaging structure for how negotiated handover operates with a reader/writer and an NFC tag device, CH 1.5 creates the possibility for the development of new solutions pairing NFC with Bluetooth or Wi-Fi when the data to be transferred is large or streamed for a long time. Examples include Bluetooth audio streaming or transfer of a photo between a digital camera or a smartphone over Wi-Fi. Previously, negotiated handover was limited to a P2P connection. CH 1.5 can now use TNEP to allow an additional negotiated handover for a connection between a reader/writer and NFC tag device providing users more control over how they gather and share their information between devices, thereby increasing the security of paired connections. Negotiated Handover using the Reader/Writer mode will be for example used by the new ISO/IEC 18013-5 standard defining the sharing mechanism for mobile driving licensees

5. NFC Forum specifications overview (4/7)

5.3 Tag Type Technical specifications

The specifications for the NFC Forum Type 1/2/3/4/5 Tags provide the technical information needed to implement the reader/writer and associated control functionality of the NFC device to interact with the tags. The new TNEP 1.0 Technical Specification supports the bi-directional exchange of NDEF messages based on the communication protocol used by the NFC Forum Tag devices of Type 2, 3, 4 and 5. The aim of these specifications is to define how NDEF messages are read from and written to NFC tags

- **Type 1 Tag Specification:** defines how an NFC-enabled device in Reader/Writer Mode detects, reads and writes a NDEF Message on a NFC Forum Type 1 Tag. The communication with this NFC Forum Tag type is based on NFC-A Technology.
- **Type 2 Tag Specification:** defines how an NFC-enabled device in Reader/Writer Mode detects, reads and writes a NDEF Message on a NFC Forum Type 2 Tag. The communication with this Forum Tag type is based on NFC-A Technology.
- **Type 3 Tag Specification:** defines how an NFC-enabled device in Reader/Writer Mode detects, reads and writes a NDEF Message on a NFC Forum Type 3 Tag. The communication with this Forum Tag type is based on NFC-F Technology, which is compatible to the Japanese Industrial Standard (JIS) X 6319-4.
- **Type 4 Tag Specification:** defines how an NFC-enabled device in Reader/Writer Mode detects, reads and writes a NDEF Message on a NFC Forum Type 4 Tag. The communication with this Forum Tag type is based on the ISO Data Exchange Protocol (ISO-DEP) which is fully compatible with the ISO/IEC 14443 standard series. This protocol is either based on NFC-A or NFC-B Technology.
- **Type 5 Tag Technical Specification:** defines how an NFC-enabled device in Reader/Writer Mode detects, reads and writes a NDEF Message on a NFC Forum Type 5 Tag. The communication with this NFC Forum Tag type is based on NFC-V Technology.
- **Tag NDEF Exchange Protocol (TNEP) Technical Specification:** the TNEP 1.0 Technical Specification supports the bi-directional exchange of NDEF messages based on the communication protocol used by the NFC Forum Tag devices of Type 2, 3, 4 and 5. The new TNEP protocol offers a simple protocol for NFC IoT devices to exchange data between an NFC enabled phone and the IoT Device. For example, this protocol can be used to configure and read smart meter devices, to control the thermostatic radiator valve or to configure the lightning device in your smart home.

5. NFC Forum specifications overview (5/7)

5.4 NFC Record Type Definition Technical Specifications

Technical specifications for Record Type Definitions (RTDs) and four specific RTDs: Text, URI, Smart Poster, and Generic Control.

- **Record Type Definition (RTD) Technical Specification:** specifies the format and rules for building standard record types used by NFC Forum application definitions and third parties that are based on the NDEF data format. 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.
- **NFC Text RTD Technical Specification:** provides an efficient way to store text strings in multiple languages by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.
- **NFC URI RTD Technical Specification:** provides an efficient way to store Uniform Resource Identifiers (URI) by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.
- **NFC Smart Poster RTD Technical Specification:** defines an NFC Forum Well Known Type to put URLs, SMSs or phone numbers on an NFC tag, or to transport them between devices. The Smart Poster RTD builds on the RTD mechanism and NDEF format and uses the URI RTD and Text RTD as building blocks.
- **NFC Generic Control RTD Technical Specification:** NFC Forum-TS-Generic Control RTD_1.0 has been withdrawn with no replacement.
- **NFC Signature RTD Technical Specification:** specifies the format used when signing single or multiple NDEF records. Defines the required and optional signature RTD fields, and also provides a list of suitable signature algorithms and certificate types that can be used to create the signature. Does not define or mandate a specific PKI or certification system, or define a new algorithm for use with the Signature RTD. Specification of the certificate verification and revocation process is out of scope.
- **NFC Device Information RTD Technical Specification:** defines the Device Information record type which conveys fundamental model and identity identification information.

5. NFC Forum specifications overview (6/7)

5.5 NFC Controller Interface

- A device level specification, the NFC Controller Interface (NCI) Technical Specification defines the interface between an NFC Controller (NFCC) and a Device Host (DH) and addresses issues that must be considered for implementation.

5.6 Application documents

- NFC Forum Application Documents are informative technical documents designed to promote NFC solutions in vertical markets and to foster best practices, by describing proposed solutions based on NFC Forum specifications.
- **Bluetooth Secure Simple Pairing Using NFC:** this Application Document describes the interaction of Bluetooth technology and NFC during SSP in detail. It provides examples of both negotiated and static handover in the most feasible use cases involving the presence of both technologies. Developers will find the examples useful guides for their own work. The document has now been expanded (in June 2014) to include descriptions of how to use NFC for fast and easy Bluetooth low energy out-of-band (OOB) pairing, a key capability of Bluetooth Smart, a version of Bluetooth wireless technology that offers considerably reduced power consumption. T

  The updated Application Document published in June 2019 supports also Bluetooth devices implemented according the Bluetooth Core Specification 5.1 and is extended for Bluetooth Low Energy.
- **Wi-Fi Protected Setup using NFC technology:** the Wi-Fi Protected Setup using NFC technology can be found in the Wi-Fi Simple Configuration Technical Specification on the Wi-Fi Alliance website. Similar to the mechanism described in the Bluetooth Secure Simple Pairing Application Document, the mechanism of the Wi-Fi Protected Setup is based on the Connection Handover Technical Specification from the NFC Forum.

5. NFC Forum specifications overview (7/7)

5.7 Wireless charging

- Wireless Charging allows for wireless charging of small battery-powered devices like those found in many IoT devices, This approach can help avoid the need for a separate wireless charging unit for small devices if the device includes an NFC communication interface. For example, a Bluetooth headset which includes NFC technology for pairing could also use the NFC interface for wireless charging. In this case, the NFC antenna is used to exchange the pairing information and to transfer power.
- This NFC specification uses the 13.56 MHz base frequency and leverages the NFC communication link to control the power transfer. NFC technology is unique in that it allows the transfer of power to an NFC tag to enable communication by providing a constant carrier signal. The WLC specification extends this communication functionality of NFC technology to enable wireless charging. The WLC specification ensures a safe charging process between two NFC-enabled devices in either static or negotiated modes. Static mode uses standard radio frequency (RF) field strength and provides a consistent power level. Negotiated mode uses a higher RF field supporting four power transfer classes of 250, 500, 750 and 1000 milliwatts.

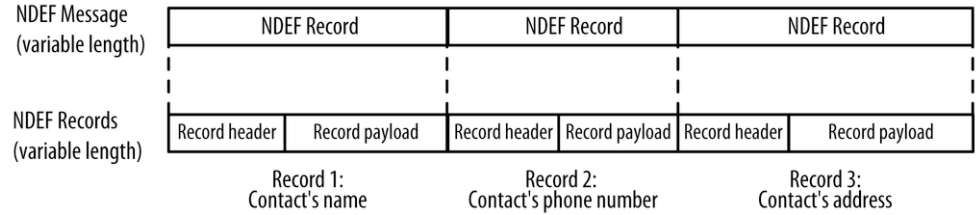
5.8 NFC Money Transfer (NMT) Candidate Technical Specification

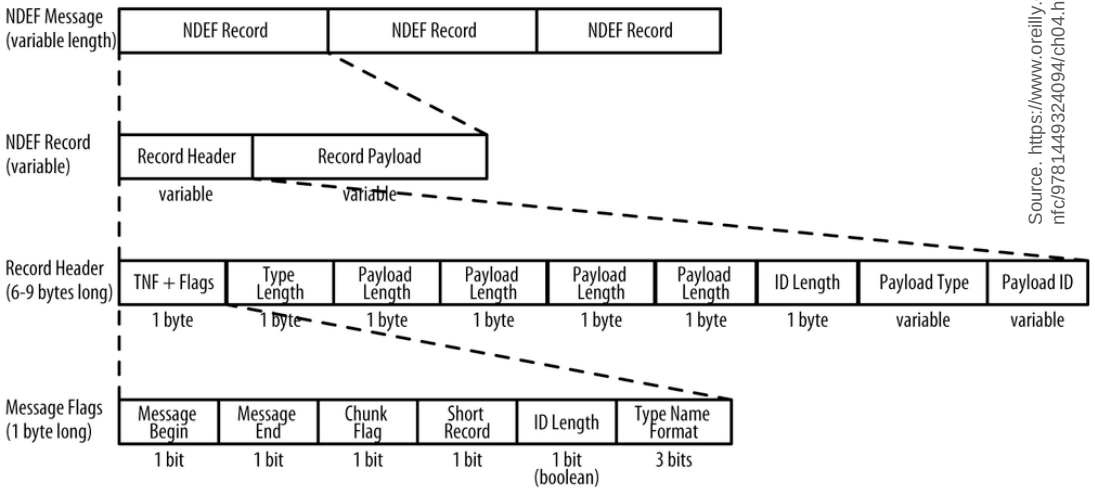
- The NFC Money Transfer (NMT) Specification defines the functions that enable two NFC Forum Devices to transfer money – such as passing money to an individual or paying a bill in a convenience store. This specification defines Money Transfer (MT) protocols, the corresponding message structures for those protocols, and the NFC Forum Well Known Types used in those messages.
- The NMT Specification gives payment service providers and consumers the opportunity to take advantage of the simple and secure NFC-based payment solutions already in use worldwide as an alternative to QR code-based solutions. The NMT solution improves the speed and efficiency of the payment process by eliminating the need for a camera or scanner used in QR code-based solutions. It provides an open framework which can be easily used by payment service providers to map their already defined data exchange for QR code-based payment solutions with NFC communication. The specification works between all NFC-enabled devices such as smartphones, readers and tags.

#6 NFC Data Exchange Format (NDEF)

6 NFC Data Exchange Format (NDEF) (1/2)

- NDEF is a binary format structured in messages
- Each NDEF message can contain one or more record
- MB: message begin; ME: message end
- NDEF record = Record header + Record Payload
- Each NDEF message MUST be sent or received in its entirety.
- The NDEF parser deconstructs the NDEF message and hands the payloads to a (potentially different) user application
- NDEF records can encapsulate documents of any type : MIME (RFC 2046); URI (RFC 3986), NFC_FORUM_RTD: Smart Poster ...; EXTERNAL_RTD (proprietary).
- NDEF record consists of : Type Name Format (TNF) + flags, Payload length, Payload Type, Payload ID, and Payload.
- TNF tells how to interpret the Payload Type
- Payload Type tells how to interpret the Payload Record





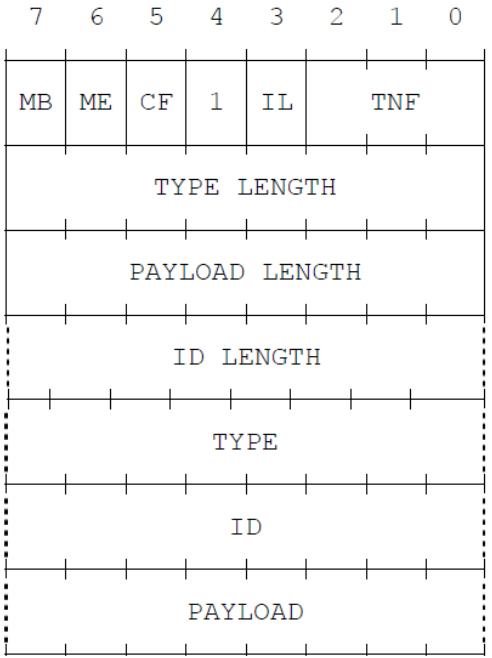
Source. https://www.oreilly.com/library/view/beginning-nfc/9781449324094/ch04.html

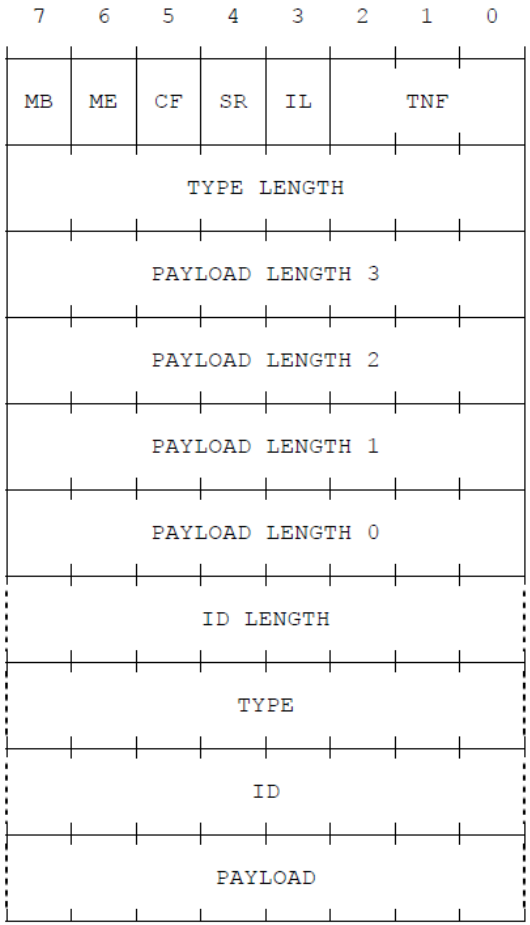
NDEF Message						
R_1 MB=1	…	R_r	…	R_s	…	R_t ME=1

6 NFC Data Exchange Format (NDEF) (2/2)

Type Name Format	Value
Empty	0x00
NFC Forum well-known type [NFC RTD]	0x01
Media-type as defined in RFC 2046 [RFC 2046]	0x02
Absolute URI as defined in RFC 3986 [RFC 3986]	0x03
NFC Forum external type [NFC RTD]	0x04
Unknown	0x05
Unchanged (see section 2.3.3)	0x06
Reserved	0x07

- CF : Chunk Flag indicates order of a chunked payload
- SR : Short Record. If set (=1) ⇒ Payload length is a single octet (0<payload filed size<255)
- IL : ID Length : if set ⇒ the ID_LENGTH field is present in the header as a single octet

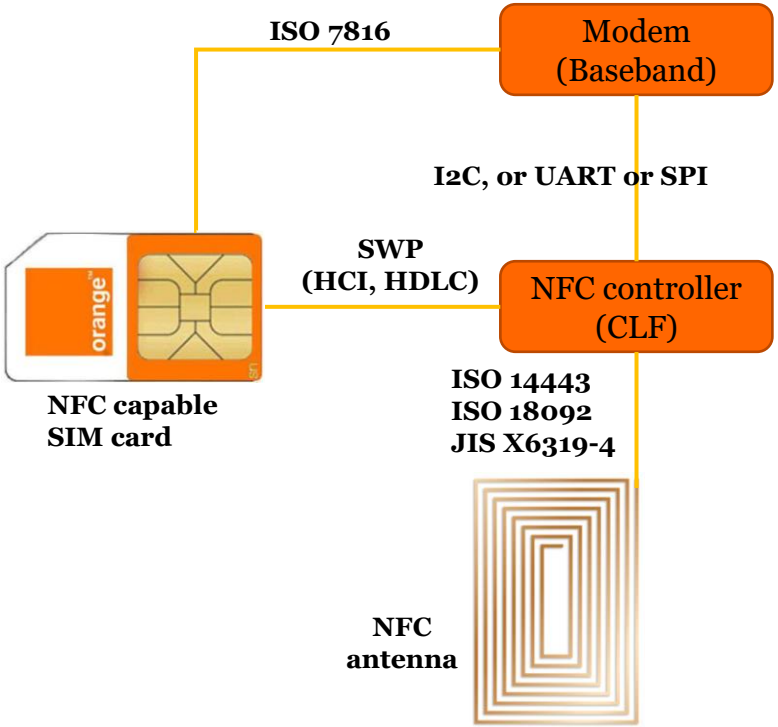




#7 NFC implementation within mobile terminals

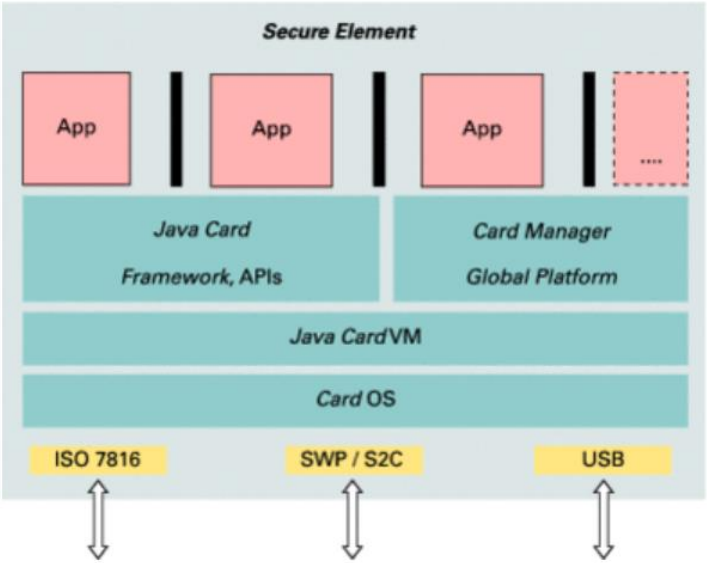
7.1 Involved interfaces and protocols for SIM-centric implementation

- ISO 7816-4 protocol for communication between the device modem and the SIM card (secure element), based on exchanging APDUs (Application Protocol Data Units)
- Single Wire Protocol for communication between the NFC Controller (CLF = Contactless Frontend) and the secure element. It's based on the Host Control Interface (HCI). HDLC (High-Level Data Link Control) protocol is used for controlling data transmission between the NFC interface and the secure element. SWP, HCI and HDLC are a well defined in ETSI standards
- Inter Integrated Circuit (I2C) orUniversal Asynchronous Receiver Transmitter (UART) or Serial Peripheral Interface (SPI) for communication between the device processor (Modem/Basebad) and the NFC controller.
- In top of NFC Forum, GSMA guarantees the supervision and harmonization of NFC implementation on mobile terminals. Its specifies NFC requirement for devices and Operating systems makers.
- GSMA (GSM Association) represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.



7.2 Secure Element (SE)

- The Secure Element (SE) hosts one or more applications commonly called “Cardlet” with their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities.
- SE is tamper-resistant platform (electronic Chip, microcontroller.
- Different form factors of SE: embedded and integrated SEs, SIM/UICC, smart microSD as well as smart cards.
- Provides a strong security for applications that hosts . Example : bank payment applications, transport transit, etc).
- A NFC service = UI application (Midlet) + Cardelet (in the SE)+ Back-end management (ex. TSM=Trusted Service Manager)

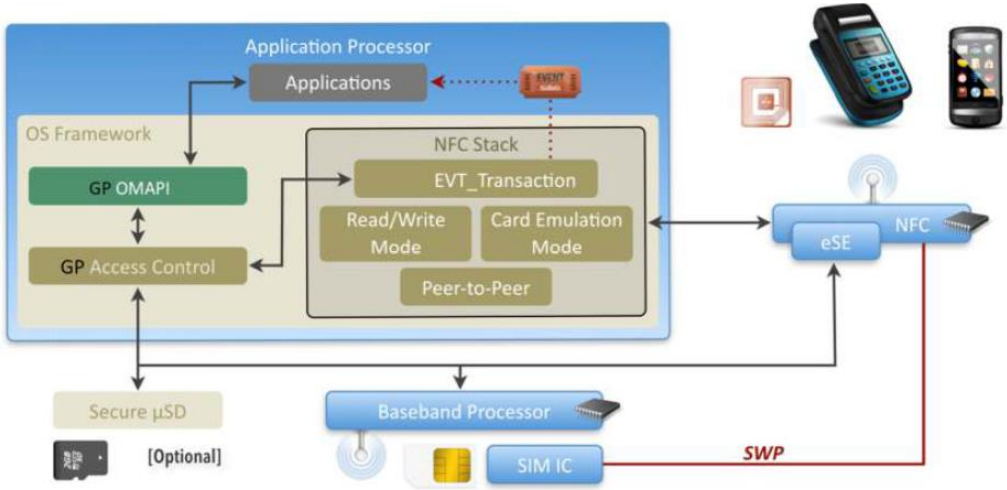


Source. Techniques de L'ingénieur

- A NFC service = UI application (Midlet) + Cardelet (in the SE)+ Back-end management (ex. TSM=Trusted Service Manager)
- TSM is a neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element on mobile phones.
- Java Card systems is an orchestrator platform (“Operating System”) within the SE that sets communication interfaces (ex. with CLF) and offers the secure and interoperable execution of multiple applications from different providers in a single constrained resource chip by maintaining tightness and the highest security certification levels and compatibility with standards.
- GlobalPlatform: a standard that provides secure external access to SE.

7.3 Generic Device Requirements

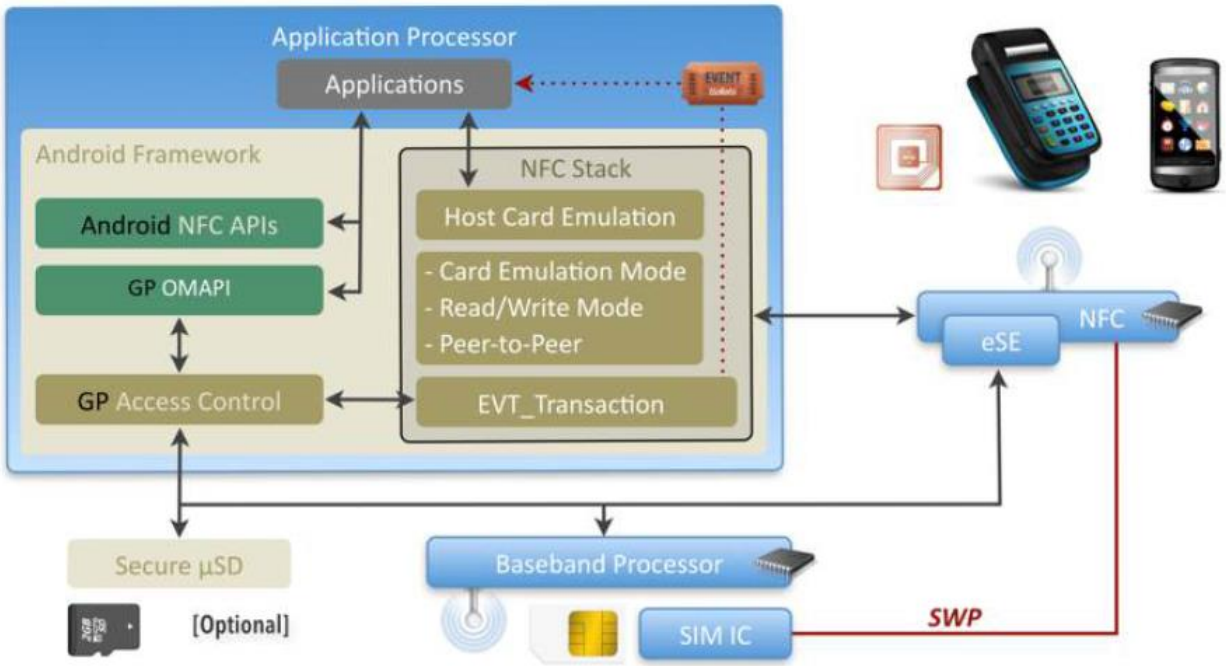
- The NFC Stack is driving the NFC Controller and is providing software APIs that enables:
  - Management of Multiple SEs (activation, deactivation, routing, etc.)
  - Management of the NFC events
  - An external API available for 3rd party applications to manage reader/writer mode, Peer to Peer mode and Card Emulation mode from Device
  - An internal API to provide a communication channel with an embedded SE (eSE) for APDU exchanges.



- SE Access API provides a communication channel (using APDU commands) allowing 3rd party apps running on the Mobile OS to exchange data with SE Applets. This API provides an abstraction level common for all SEs and could rely on different low level APIs for the physical access:
  - RIL (Radio Interface Layer) extension for accessing the UICC
  - Specific libraries for communicating with other eSEs
- In order to implement security mechanisms (e.g. SE Access Control), the SE Access API uses Mobile OS mechanisms such as UIDs or application certificates to identify the calling application.

7.4 NFC implementation in Android OS

- Host Card Emulation mode (HCE) ⇒ a software based card emulation
- Supports also others SEs (eSE, UICC or Secure microSD). UICC = Universal Integrated Circuit Card
- GlobalPlatform Open Mobile API to access to the different SEs applets (eSE, UICC, microSD.



7.5 Multiple Card Emulation implementation schemes

1. Secure Element SIM-based


- ❑ UICC is a highly secure hardware chip with OTA deployment capabilities
- ❑ Do not require network connectivity and works also when user equipment (UE) is OFF.
- ❑ Managed by the Mobile Network Operator (MNO) and is independent from the device makers.
- ❑ Embedded SIM (eSIM) is expected to have the same implementation like in the SIM
- ❑ Notion of Issuer Security Domain (ISD ⇒ managed only by the MNO), Suplementary Security Domain (SSD ⇒ domain accessible for the service provider or Trusted Service Manager =TSM)

2. Secure Element device-based (eSE)

- ❑ Dedicated tamper resistant chip soldered inside the devices with security levels similar to SIM cards.
- ❑ Works without connectivity.
- ❑ Independent from the MNO.
- ❑ Solution specific to each manufacturer and starts to be available on the recent smartphone devices.
- ❑ Opportunities for manufacturers to onboard within their proprietary (Apple Pay, Samsung Pay, Huawei Wallet, etc).

3. HCE-based (with cloud backend)

- ❑ Software solution running on the OS, available since Android 4.4. Services are independent from MNO or manufacturers).
- ❑ Security challenges: requires service backend deployment with improved security and needs frequent network connectivity.
- ❑ Example of service : Orange bank (since Jan 2020), Google Pay.

7.6 AID routing principles (1/2)

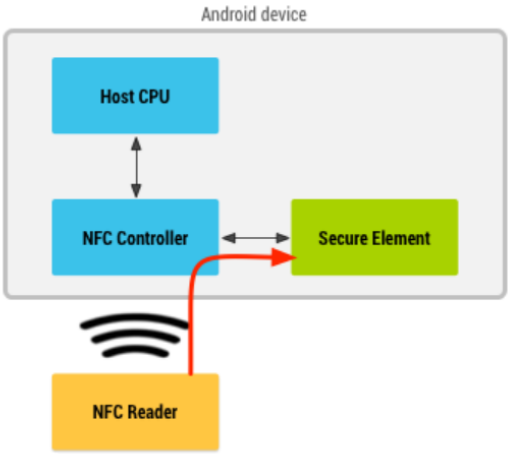
1. Application ID (AID)

- When the user taps a device to an NFC reader, the system needs to know which service the NFC reader wants to talk to
- ISO/IEC 7816-4 specification defines a way to select applications with their corresponding application IDs (AID)
- An AID consists of up to 16 bytes and is composed of two components :
  - Registered Application Identifier (RID) – Example: Visa's RID is A000000003.
  - Proprietary Application Identifier Extension (PIX) – The PIX represents the application.
- When emulating cards for an existing NFC reader infrastructure, the AIDs that those readers are looking for are typically well-known and publicly registered. Example: the AIDs of payment networks such as Visa and MasterCard).
- A NFC app developer needs to register/declare AIDs that identify its new service (application).
- The registration procedure for AIDs is defined in the ISO/IEC 7816-5 specification
- In some cases, an HCE service may need to register multiple AIDs to implement a certain application (Group of AIDs)
- AID groups and categories : Android supports two categories : CATEGORY_PAYMENT (covering industry-standard payment apps) and CATEGORY_OTHER (for all other HCE apps).

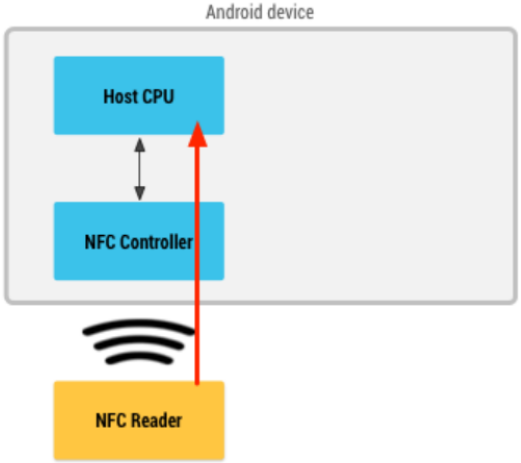
Product	RID	PIX	AID
Visa (i.e., Visa Debit or Visa Credit)	A000000003	1010	A0000000031010
Visa Electron	A000000003	2010	A0000000032010
Visa Interlink	A000000003	3010	A0000000033010
Plus	A000000003	8010	A0000000038010

7.6 AID routing principles (2/2)

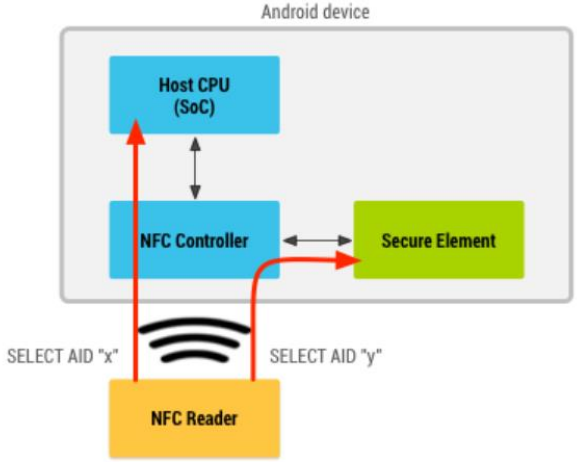
2. AID Routing / Routing table



NFC card emulation with a secure element.



NFC card emulation without a secure element.



Android operating with both secure element and host-card emulation.

7.7 Device certification process (1/2)

- GCF (Global Certification Forum) is a certification organization that ensure the right implementation of NFC within NFC enabled devices.
- GCF = active partnership between mobile network operators, mobile device manufacturers and the test industry
- GCF certification process is based on technical requirements as specified within dedicated test specifications provided by the 3GPP, NFC Forum GSMA, EMVCo, and others.
- NFC technology is covered by two test certification plans : Supports UICC-NFC Services & Supports SWP/HCI they are mainly based on the following stantards specfifications.
  - GSMA TS 26 and 27 specifications (respectively : NFC Handset Requirements & NFC Handset Test Book).
  - ETSI TS 102 230UICC-Terminal interface; Physical, electrical and logical test specification
  - ETSI TS 102 384 Smart Cards; UICC-Terminal interface; Card Application Toolkit (CAT) conformance specification
  - ETSI TS 102 694-1 Smart Cards; Test specification for the Single Wire Protocol (SWP) interface
  - ETSI TS 102 695-1 Smart Cards; Test specification for the Host Controller Interface (HCI);
  - 3GPP TS 31.121 UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification; Mobile Equipment (ME) conformance test specification;
  - (3GPP TS 31.124Universal Subscriber Identity Module Application Toolkit (USAT) conformance test specification
- GSMA NFC specifications and requirements are based/linked to NFC Forum specfifications
- GCF certification is not mandatory but can be requested by the MNO or any market channel. It's also a selling argument for device manufacturers

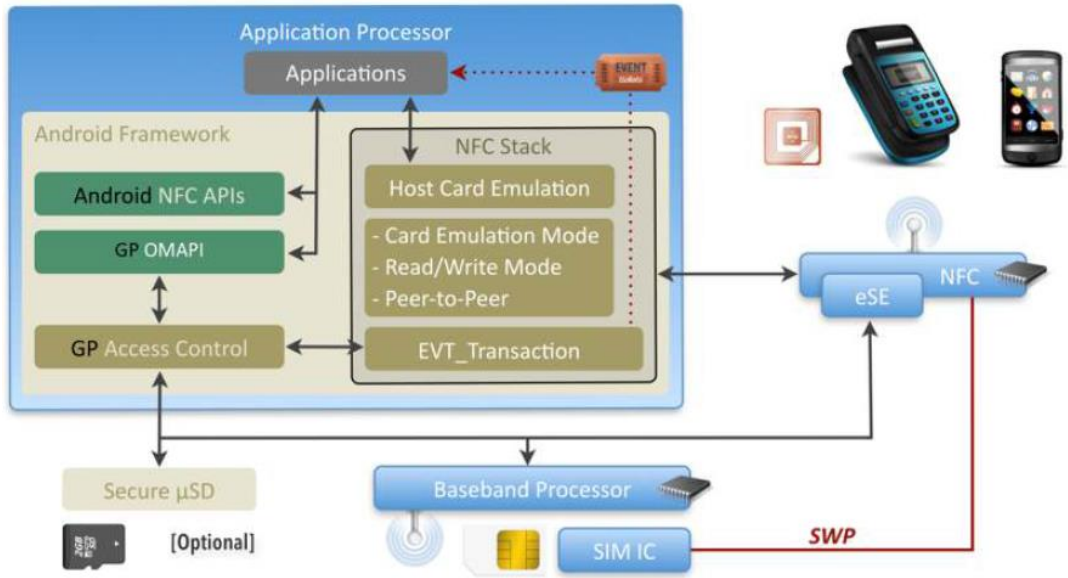
7.7 Device certification process (2/2)

- CEE : Card Emulation Environment
- TEE: Trusted Execution Environment
- PTCRB : a North American certification Forum (equivalent to GCF but less wider).
- UI : User interface

	NFC Components/ Interfaces	Common Criteria	GCF	PTCRB	GlobalPlatform	EMVCo	NFC Forum
Device	NFC Controller		X			X	X
	NFC Analog layers (frontend)		X	X		X	X
	NFC Protocol layers		X			X	X
	UI interaction		X	X		X	
	Access control for TEE				X		
	Access control for UICC and SE		X	X	X		
	Service Management on Secure Element		X	X			
CEE	Coexistence of Multiple Card Emulation Environments (CEE)		X	X		X	
	TEE				X	X	
	SE/UICC	X				X	
	HCE					X	

7.8 Device testing on Android devices

- Access Control verification : access to the secure element with different policy rules
- OMAPI implementation and ensure end-to-end communication between an Android NFC application and a cardlet on the secure element (SIM)
- BIP CATTP protocol implementation that ensure the deployment and maintenance Over the Air (OTA) of an applet on the secure element. TSM is responsible of sending OTA commands to SE.
- SWP/HCI verification ⇒ requires spy tools
- Push Transaction testing. Ensures that a transcation event is pushed by the NFC payment application after a user hands the device over payment terminal.



References

- NFC Forum: https://nfc-forum.org/
- GSMA : https://www.gsma.com/.
- 3GPPandro: https://www.3gpp.org/
- Android Open Source (AOSP) https://source.android.com/
- GCF : Global Certification Forum : https://www.globalcertificationforum.org/about/organisation.html
- GlobalPlatform : https://globalplatform.org/
- Trusted Connectivity Alliance (ex.SIMAliance) : https://trustedconnectivityalliance.org/
- Ali Benfattoum. Techniques de l'Ingénieur. La technologie NFC - Principes de fonctionnement et applications: https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/internet-des-objets-42612210/la-technologie-nfc-s8650/integration-du-nfc-dans-le-telephone-mobile-s8650niv10003.html#niv-sl11216634
- Samia Bouzefrane (CNAM). La technologie RFID/NFC: https://cedric.cnam.fr/~bouzefra/cours/CoursNFC_Bouzefrane_Decembre2013.pdf
- International Standardization Organization : https://www.iso.org/fr/standards.html
- International Electrotechnical Commission : https://www.iec.ch/
- Ecma International - European association for standardizing information and communication systems : https://www.ecma-international.org/default.htm
- Springcard : https://www.springcard.com/en/blog/news/which-type-of-nfc-tag-is-the-most-interesting-for-you

Questions ?

Samir Bellahsene
samir.bellahsene@orange.com