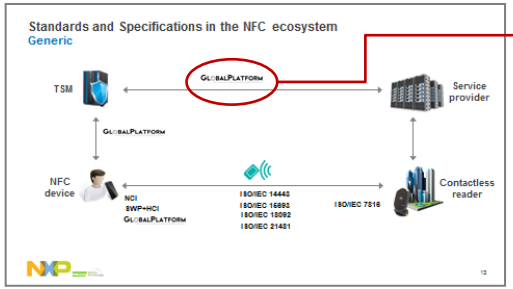
NFC Standards

Public

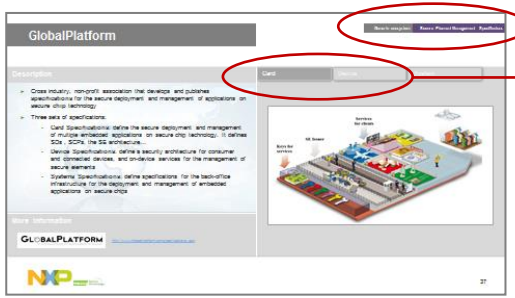
BU Security and Connectivity
February 2015

Presentation instructions

- This presentation follows an specific flow, with navigation tools and non-consecutive slides.
- Use the Main Menu (Slide13) to choose among different NFC ecosystems and Standards.
- Click ⓘ to jump to specific detailed information.
- Use the upper menu to come back to the presentation flow.
- You can navigate through different sections where tabs are available.



Press to see Standard & Specification detailed information



Use menus to navigate

Ckick on the tabs to access different sections

Index

NXP Training Mobile Knowledge

NFC enables a new mobile experience

Card Emulation

Read / Write

Peer 2 Peer

Contactless readers

NFC tags

NFC devices

What is NFC

Near Field Communication is a short-range wireless connectivity technology ***standard***, designed for ***intuitive*** and ***simple*** communication between ***two*** electronic devices.

Some NFC technical data

- Short range (< 10 cm), 13.56 MHz contactless technology
- Standardized by ISO/IEC, ECMA International and ETSI
- Compatible with existing ISO/IEC 14443 and FeliCa contactless card & reader infrastructure
- Reader and card modes possible in the same device
- Device to device connectivity
- Data exchange rate up to 424 Kbps

NFC interactive devices

Card emulation

- Payments
- Transit
- Access
- Identity
- ...

Contactless readers

Read/write

- Product Authentication
- Smart Advertising
- Pairing
- ....

NFC tags

Peer-to-peer

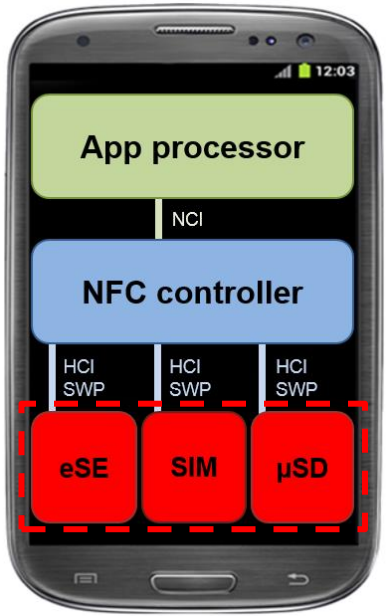
- Automotive
- Social media
- ...

Other NFC devices

The NFC ecosystem

The Secure Element

- A specific IC to handle and store sensitive data
- Used in applications such as payments, transit... (in Card Emulation mode)
- Available in different form factors (eSE, SIM, µSD...)
- Main elements:
  - Non-volatile secure memory
  - Security CPU
  - Crypto co-processors
- Protected by cryptographic keys
  - Only authorized entities can access the SE
- Protected against tampering & attacks
- Certified by third parties according to i.e. Common Criteria
- Same family of products as used in payment cards, e-passports…



Definitions

Standard

A document that provides requirements, guidelines and characteristics that can be consistently used to ensure that materials, products, processes and services are fit for their purpose.

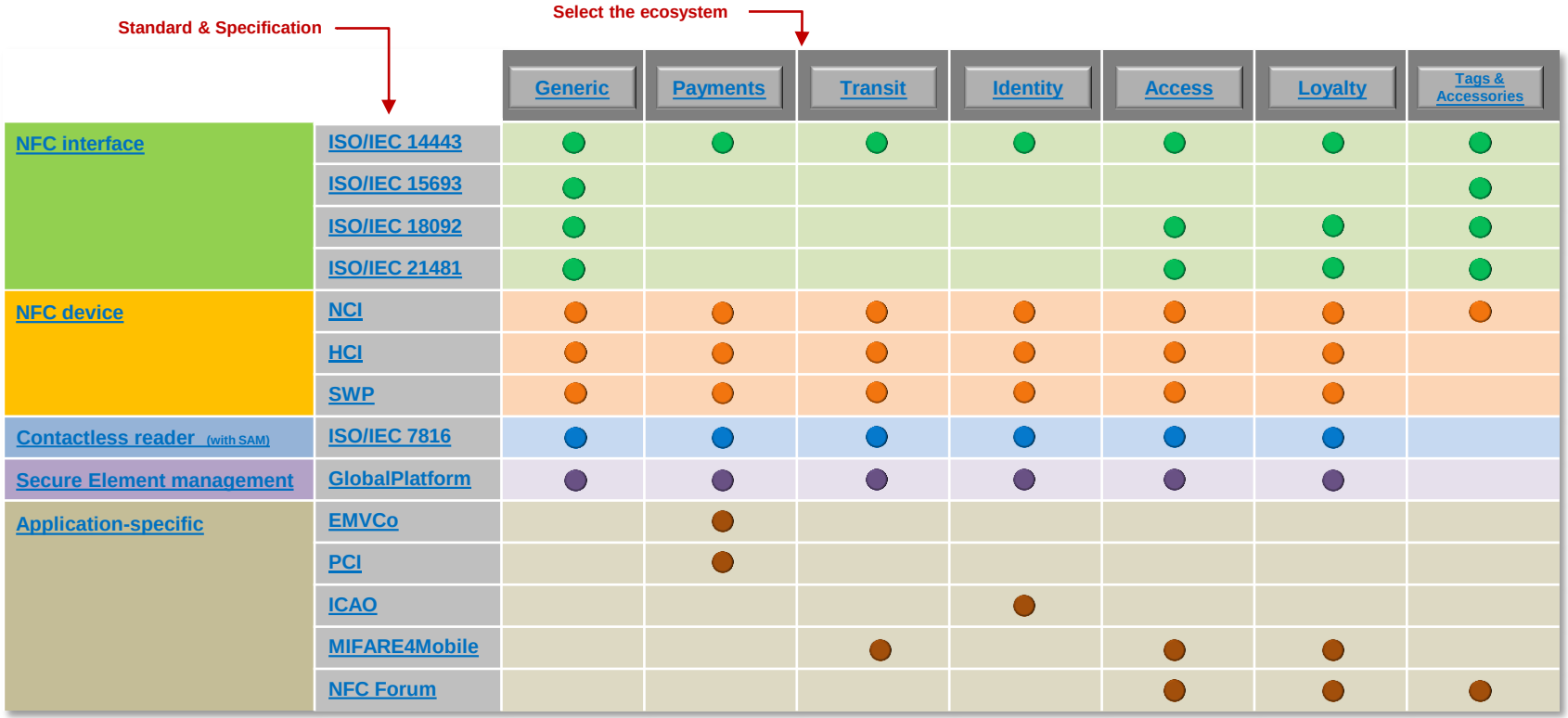
Some entities: ISO/IEC, Ecma International, ETSI…

Specification

A detailed description of technical requirements, usually with specific acceptance criteria, stated in terms suitable to form the basis for the actual design development of an item having the qualities specified in the operational characteristics.

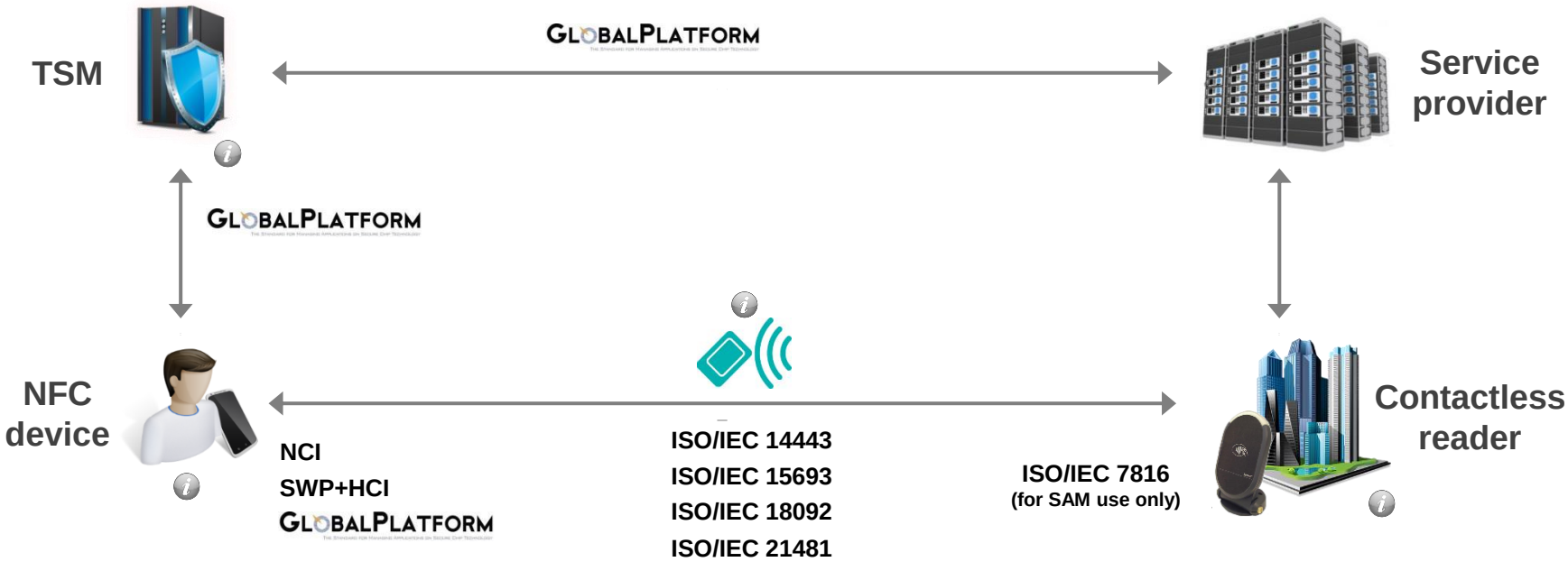
Some entities: NFC Forum, GlobalPlatform, EMVCo, MIFARE4Mobile…

NFC Standards and Specifications - Main Menu



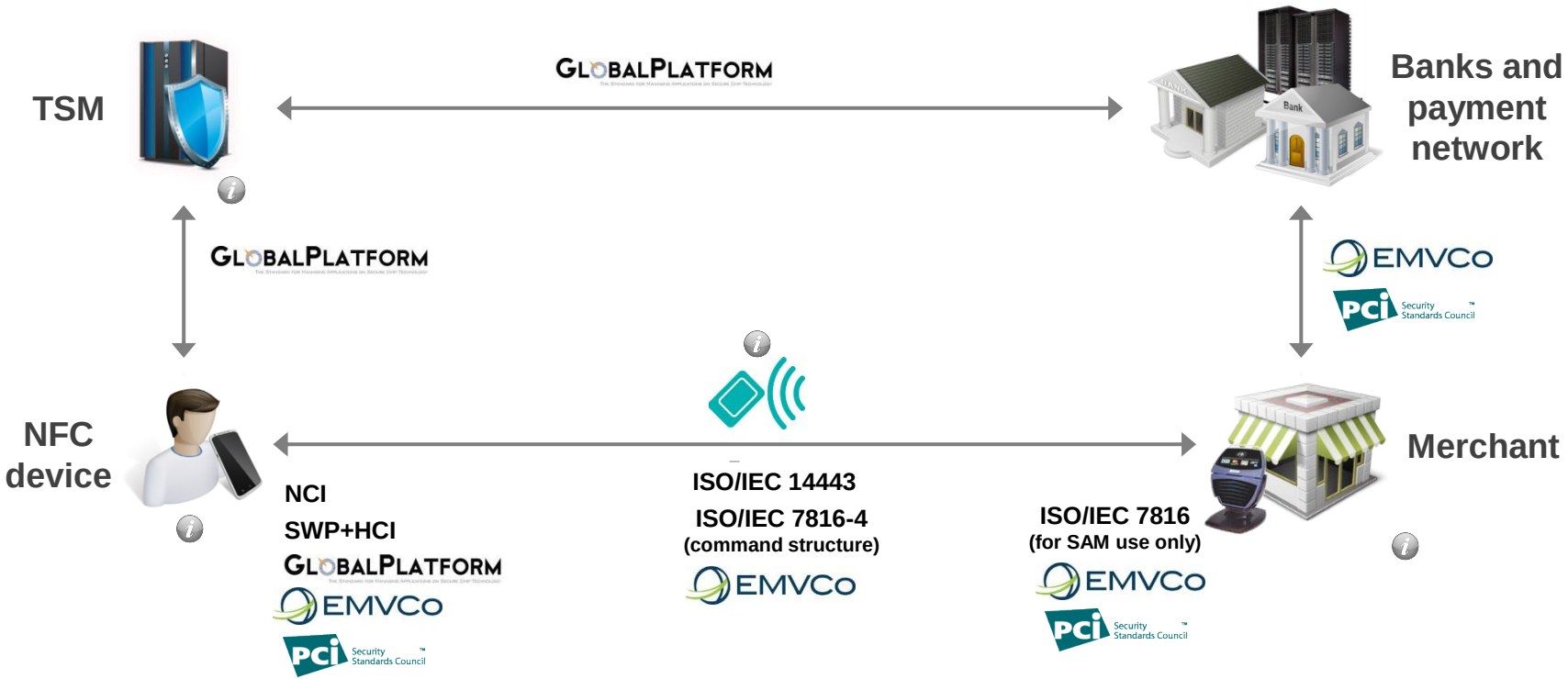
Standards and Specifications in the NFC ecosystem

Generic



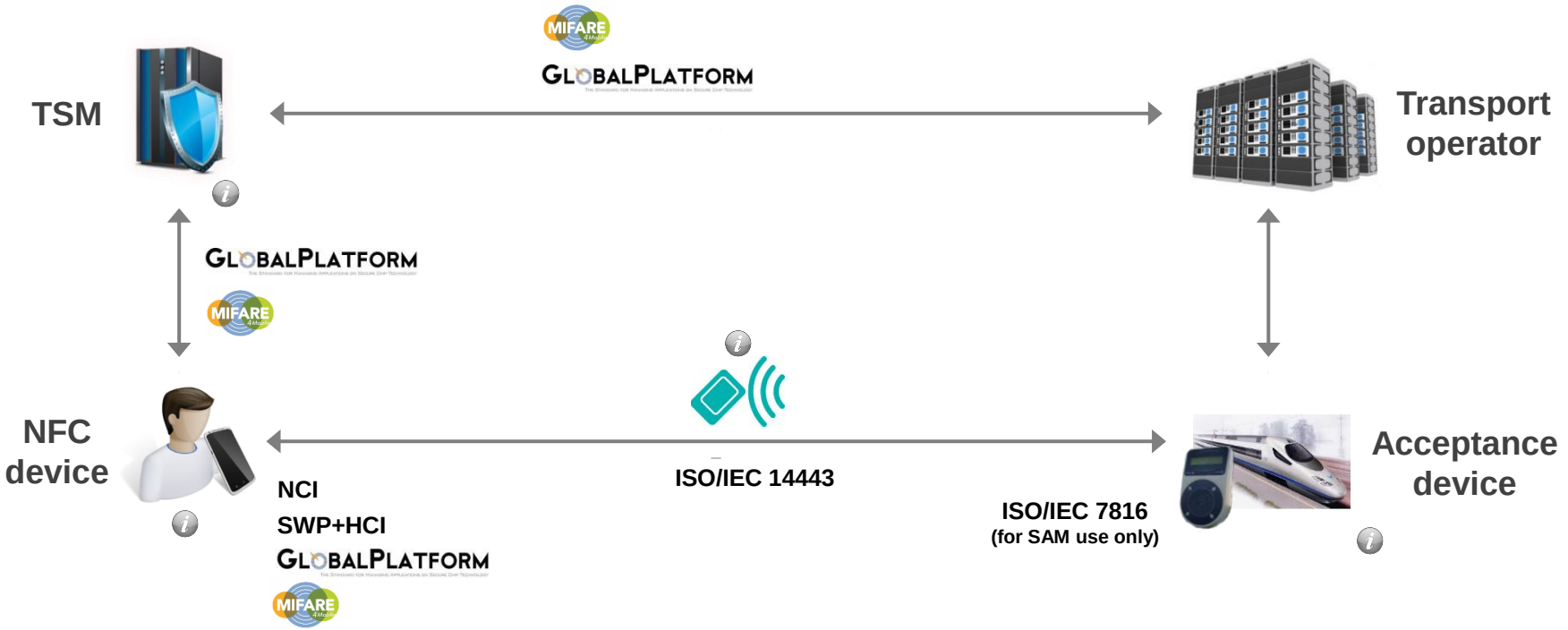
Standards and Specifications in the NFC ecosystem

Payments



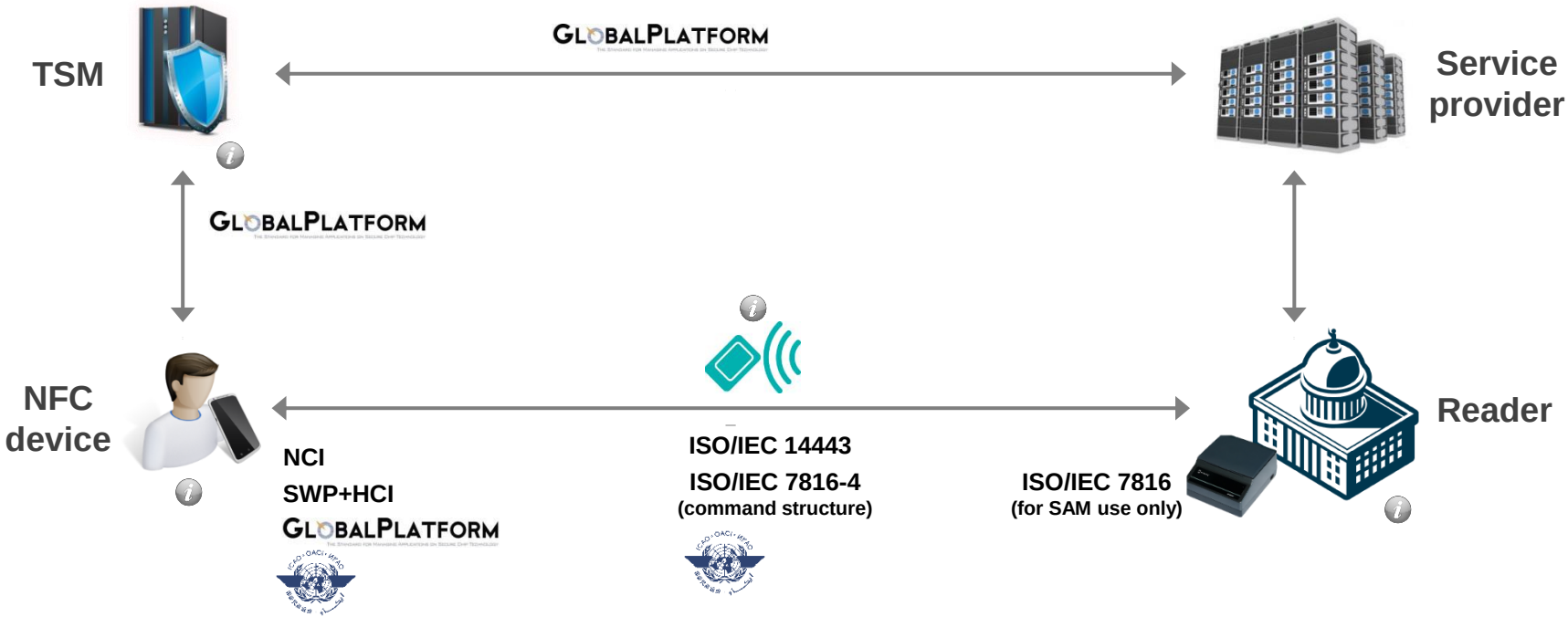
Standards and Specifications in the NFC ecosystem

Transit



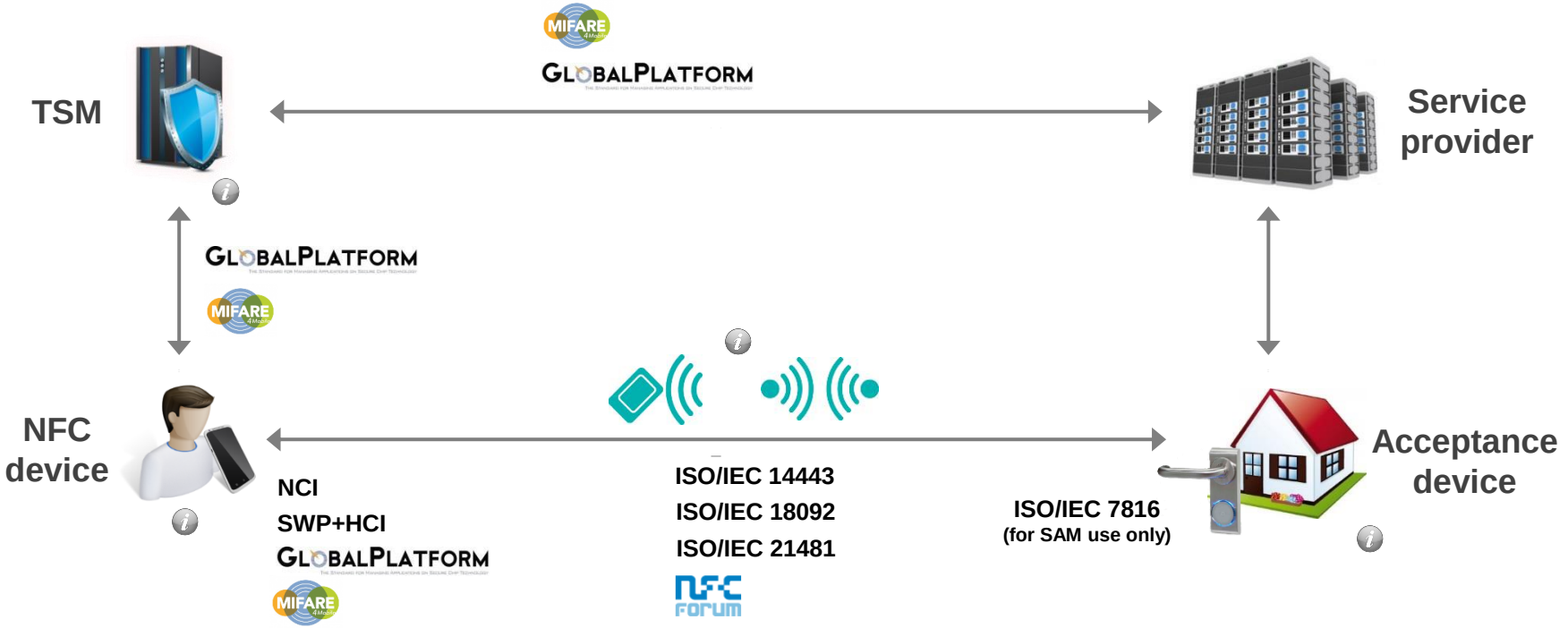
Standards and Specifications in the NFC ecosystem

Identity



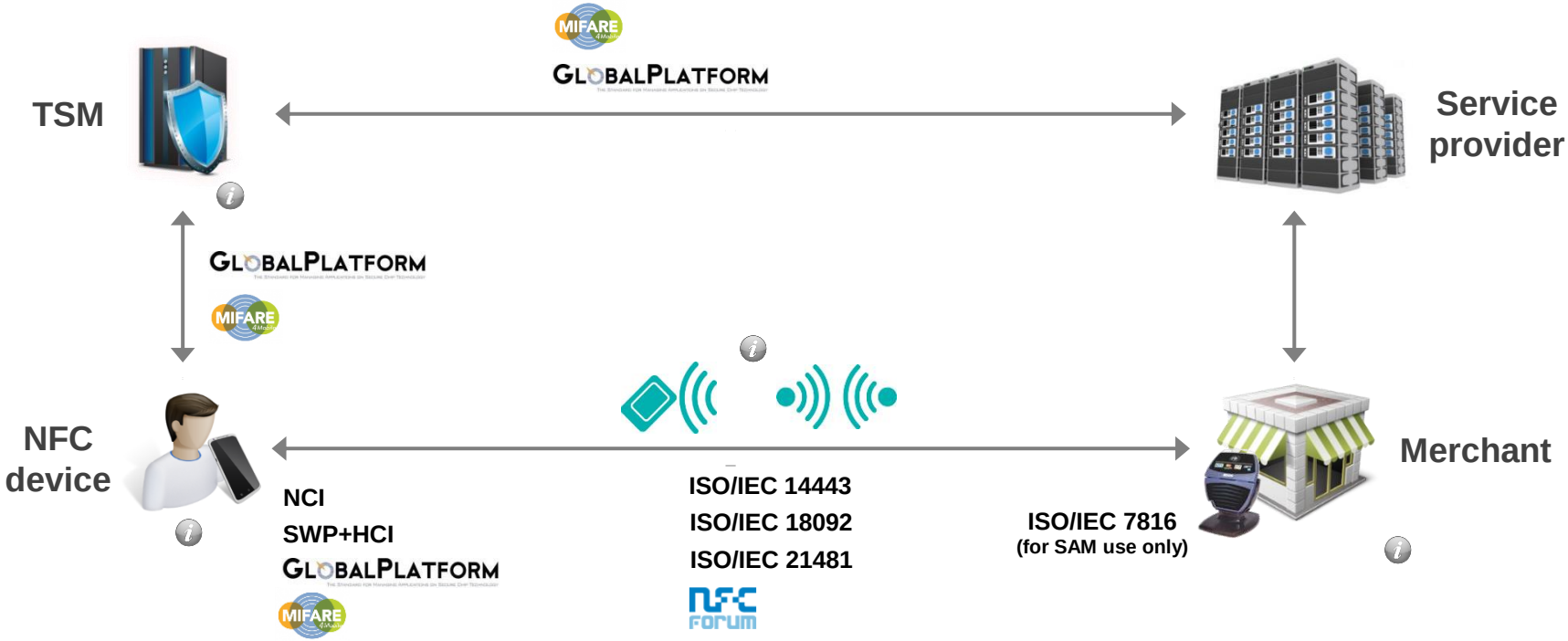
Standards and Specifications in the NFC ecosystem

Access



Standards and Specifications in the NFC ecosystem

Loyalty



Standards and Specifications in the NFC ecosystem

Tags & accessories

NFC device

NCI

ISO/IEC 14443
ISO/IEC 15693
ISO/IEC 18092
ISO/IEC 21481

Tags

Accessories

NCI

Other NFC devices

NFC interface Standards

The **NFC interface Standards** are those that describe the communication through the NFC Interface (RF field, coding, protocols, commands...).

They are generic for all kinds of applications.

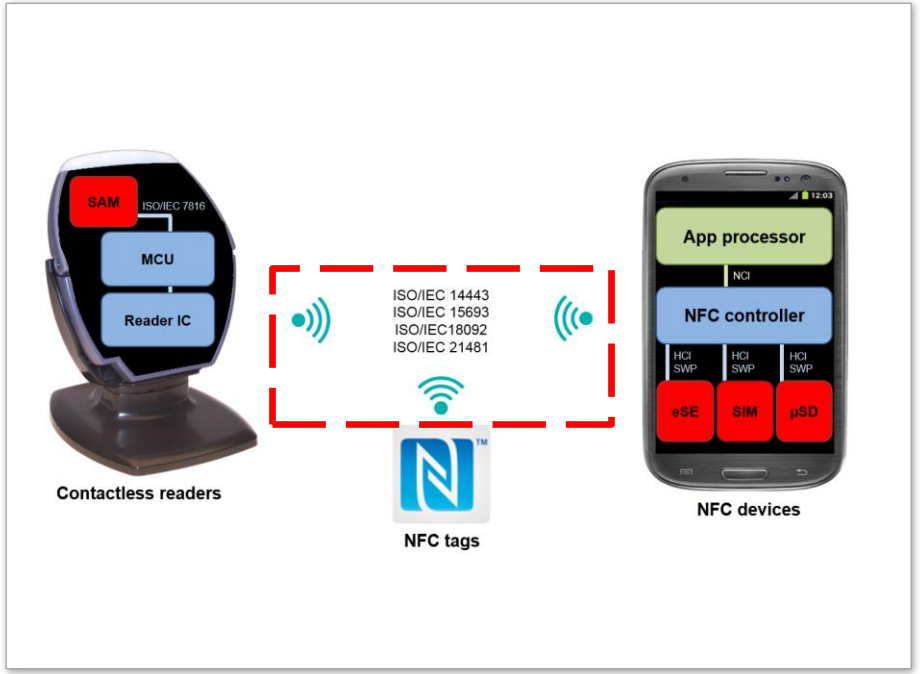
The main standards are:

ISO/IEC 14443
(the international standard for proximity contactless cards)

ISO/IEC 15693
(the international standard for vicinity contactless cards)

ISO/IEC 18092
(compliant with ISO/IEC 14443-A and FeliCa cards and readers)

ISO/IEC 21481
(includes ISO/IEC 18092, ISO/IEC 14443 and ISO/IEC 15693 standards)



ISO/IEC 14443

Description

- It standardizes the communication between proximity contactless cards and readers
- It describes the antenna characteristics, RF magnetic field, communication signal interface and general protocol flow
- It defines 2 types of communication signal interfaces: type A and type B
- Divided in 4 parts:
  - Part 1: Physical characteristics
  - Part 2: Radio frequency power and signal interface
  - Part 3: Initialization and anti-collision
  - Part 4: Transmission protocol
- Used in applications such as payments, transit, eID...

More information

http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942

Contactless card

ISO/IEC 15693

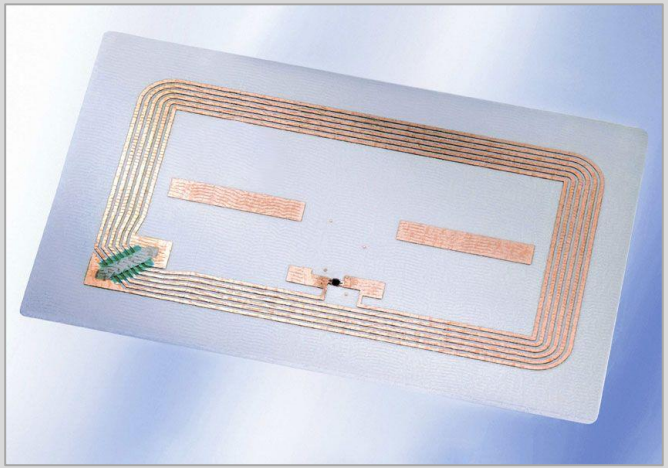
Description

- It standardizes the communication between vicinity contactless cards and readers
- It defines the physical characteristics of the cards, RF magnetic field, communication signal interface and general protocol flow
- Divided in 3 parts:
  - Part 1: Physical characteristics
  - Part 2: Air interface and initialization
  - Part 3: Anti-collision and transmission protocol
- Used in applications such as book tagging in libraries, ski ticketing...

More information

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39695

Vicinity card



ISO/IEC 18092

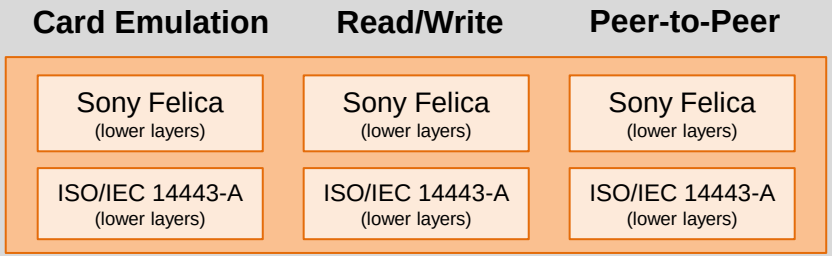
Description

- Also covered in **ECMA-340** and **ETSI TS 102 190**
- It standardizes the communication between two NFC devices at analog and digital level
  - It defines the RF magnetic field, communication signal interface and general protocol flow
- It is based on the lower layers of **ISO/IEC 14443-A** and **FeliCa**
- Peer-to-peer mode was introduced with this standard
- It defines two communication modes: **active** and **passive**
- It defines a common low-level protocol for the 3 modes of operation (it does not distinguish among them)
- It defines the initialization conditions for the data rates of 106, 212 and 424 kbps

More information

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56692
http://www.ecma-international.org/publications/standards/Ecma-340.htm
http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17787

Contained Standards



ISO/IEC 21481

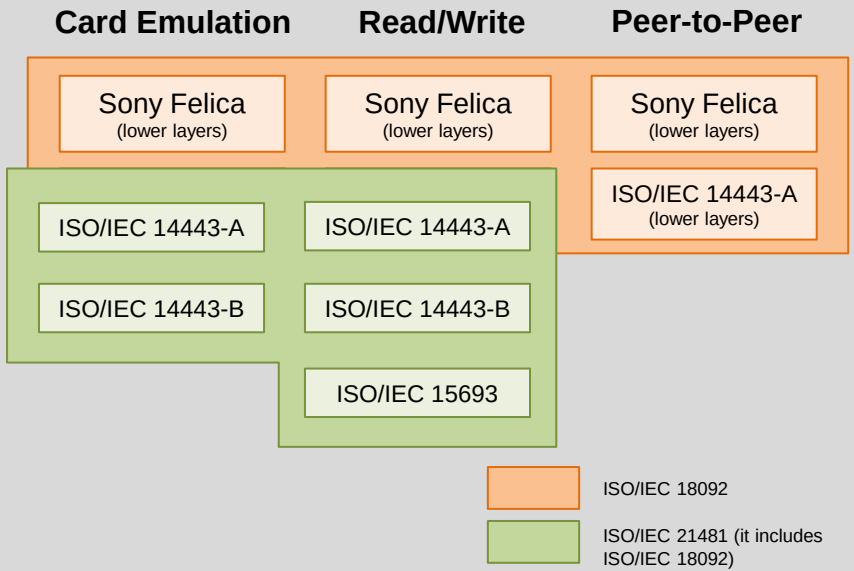
Description

- Also covered in **ECMA-352** and **ETSI TS 102 312**
- It includes **ISO/IEC 18092**, **ISO/IEC 14443** and **ISO/IEC 15693**
- It defines 4 modes for the NFC device:
  - NFC mode (ISO/IEC 18092 device)
  - PCD mode (ISO/IEC 14443 reader)
  - VCD mode (ISO/IEC 15693 reader)
  - PICC mode (ISO/IEC 14443 card)
- It specifies the mode selection mechanism, designed not to disturb any ongoing communication at 13.56 MHz (the discovery loop)

More information

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56855
http://www.ecma-international.org/publications/standards/Ecma-352.htm
http://www.etsi.org/deliver/etsi_ts/102300_102399/102312/01.01.01_60/ts_102312v010101p.pdf

Contained Standards



NFC device standards and specifications

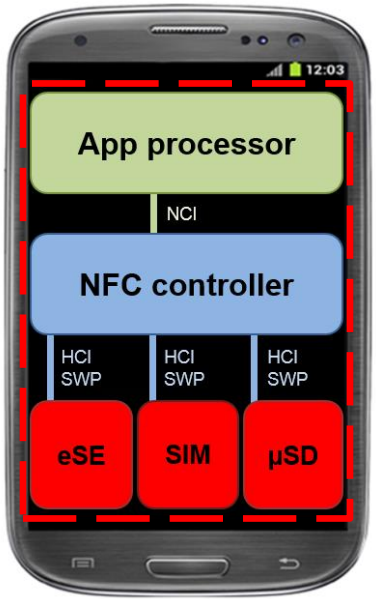
The **NFC device** standards and specifications are those that describe the key NFC related communication channels within the device.

The main protocol used to **communicate the NFC device main processor with the NFC controller** is:

NCI (NFC Controller Interface)

The main protocols used to **communicate the NFC controller with the secure element** are:

SWP (Single Wired Protocol) + **HCI** (Host Controller Interface)



For all NFC modes

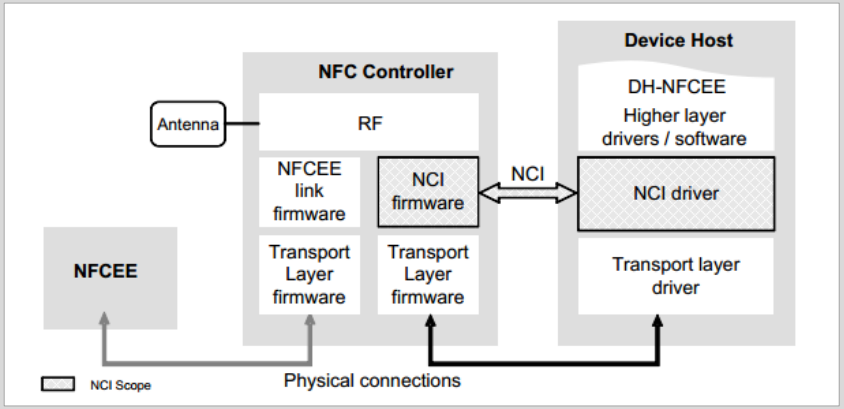
Only for CE mode

NFC Controller Interface (NCI) NFCForum-TS-NCI-1.1

Description

- **NCI** specifies the communication protocol between the NFC controller and the application processor
- It is defined to be independent of the physical and link layers (it can work over SPI, I²C…)
- It provides features to communicate the application processor and the SE
- Divided in 3 logical components:
  - NCI Core
  - Transport Mappings
  - NCI Modules

NCI scope



More information

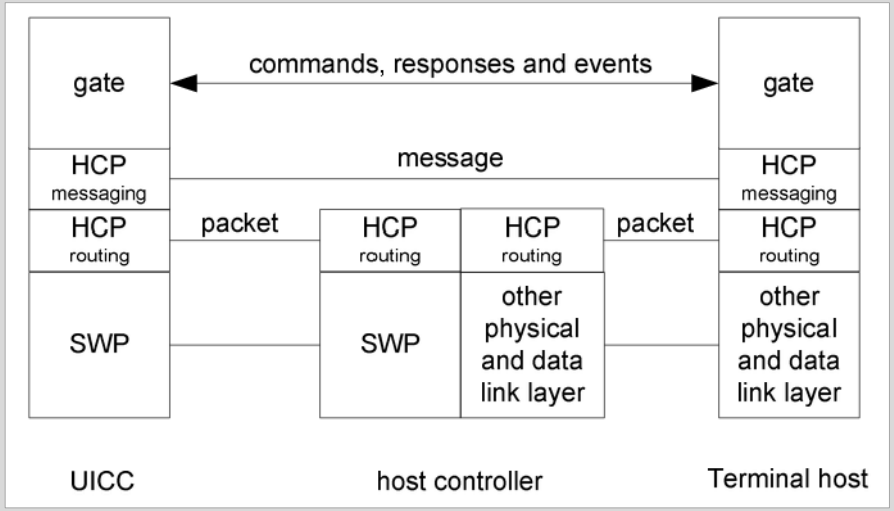
http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

Host Controller Interface (HCI) ETSI 102 622

Description

- **HCI** specifies a logical interface to interconnect the NFC controller and the secure element
- It was originally developed for the communication between the NFC controller and the SIM card
- It defines the network and transport layers
  - It can work over different lower-level protocols, such as SWP, I²C...
- Before the publication of the NCI specification, it was also used to communicate the application processor and the NFC controller
  - Some old NFC controllers still use it in this communication channel

HCI architecture



More information

ETSI World Class Standards

http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=43302

Single Wired Protocol (SWP) ETSI 102 613

Description

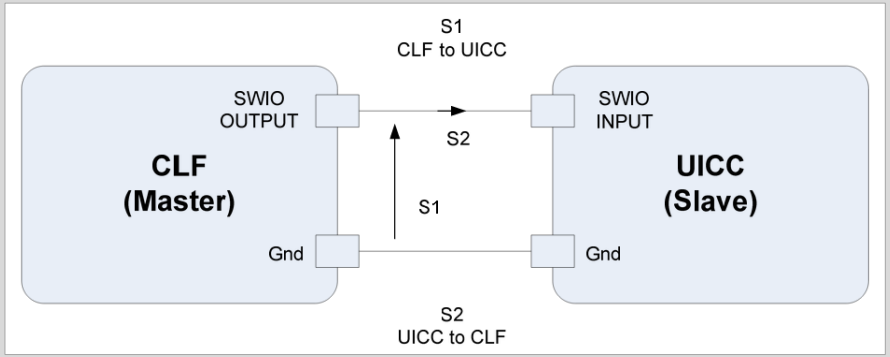
- **SWP** defines the communication interface between the **SIM card and the NFC controller** in the terminal
- It only specifies the **physical and link layers**
- The interface is a bit-oriented, full-duplex, point-to-point communication protocol
  - **Signal S1** is transmitted by a digital modulation in the voltage domain
  - **Signal S2** is transmitted by a digital modulation in the current domain
- For the communication with the embedded secure element, a modified version of the protocol named DWP is used
  - It uses two wires, one for each signal

More information

ETSI World Class Standards

http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=39894

Physical connection



ISO/IEC 7816 (SAM use in Reader)

Description

Most of the communication channels inside a contactless reader follow generic protocols such as SPI or I2C, or proprietary protocols, not in the scope of this presentation.

We address here the specific case of a SAM (Secure Access Module) included in the reader

The SAM is a secure IC, usually with a contact card form factor, used to store secret keys and to perform cryptographic algorithms in secure architectures.

Communication from the MCU and Reader IC to the SAM follows the standard

ISO/IEC 7816

More information

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35168

SAM in a reader | ISO/IEC 7816 Command Structure

ISO/IEC 7816 (SAM use in Reader)

Description

- **ISO/IEC 7816** specifies the communication with contact cards
- It is divided in 15 parts. The main parts are:
  - **Parts 1, 2 and 3**: Define the physical and electrical characteristics and the lower level protocols for contact cards
  - **Part 4**:
    - Defines a request/response protocol
    - Standardizes APDU commands and responses
    - It is independent of the physical interface technology -> It is used for smart cards accessed by contact and contactless methods

More information

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35168

SAM in a reader | ISO/IEC 7816 Command Structure

C-APDU

CLA	INS	P1	P2	Lc	Command data	Le

R-APDU

Response data	SW1	SW2

POS/mPOS Specifications

The **POS/mPOS** Specifications are those that describe the different requirements for a POS/mPOS device.

The main entities that define requirements for these kinds of devices are:

EMVCo

POS/mPOS devices are certified through the Terminal Type Approval process. It defines two certification levels:

- Level 1: electromechanical, logical and transmission protocol requirements
- Level 2: debit/credit application requirements

PCI Security Standards Council

The POS/mPOS device must be certified against all the PCI specifications:

- PCI Data Security Standard (PCI DSS)
- Payment Application Data Security Standard (PA-DSS)
- Point-to-Point Encryption (P2PE)
- Pin Transaction Security (PTS)

Secure element management Specifications

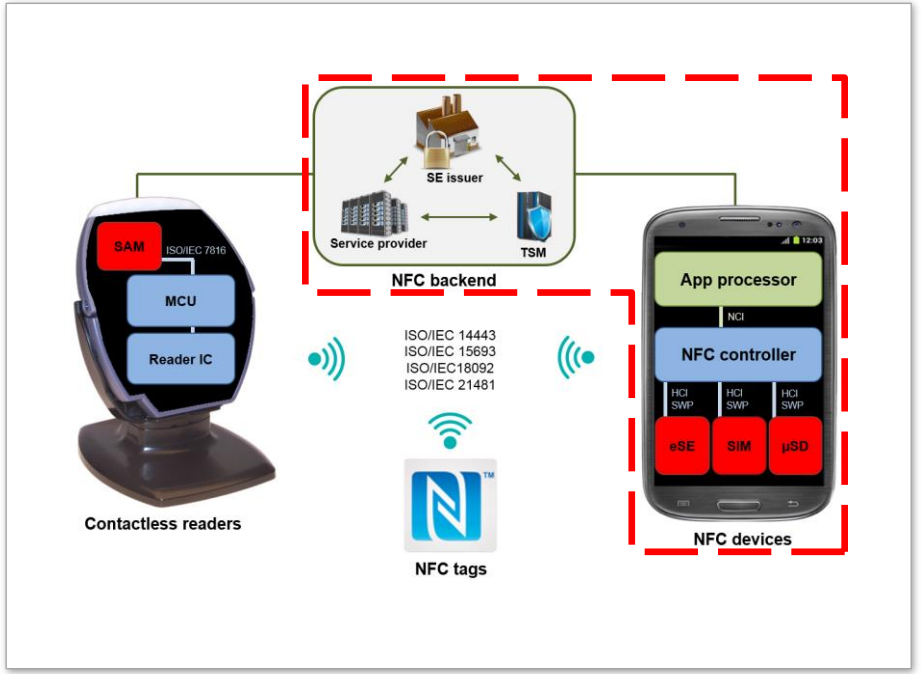
The **Secure Element management Specifications** describe the interactions with the secure element as well as among the different entities in the backend, which allow them to manage the secure element and its apps.

This Secure Element management is done through an entity called **TSM** (Trusted Service Manager). The TSM is a trusted entity that remotely manages the Secure Element and the applications in it on behalf of the Secure Element issuer or the service provider. This way, it is guaranteed that this management is done in a secure way.

The main body that describes how this Secure Element management is done is:

GlobalPlatform

GLOBALPLATFORM



GlobalPlatform

Description

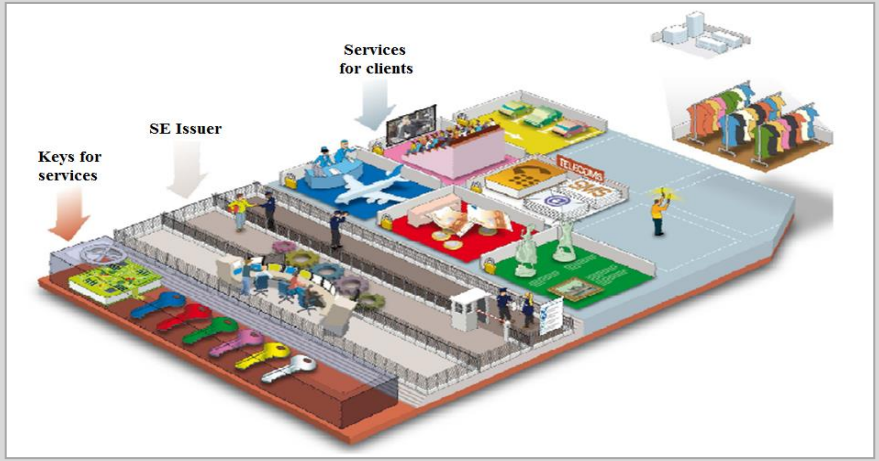
- Cross industry, non-profit association that develops and publishes **specifications** for the secure deployment and management of applications on **secure chip** technology
- Three sets of specifications:
  - **Card Specifications**: define the secure deployment and management of multiple embedded applications on secure chip technology. It defines SDs , SCPs, the SE architecture…
  - **Device Specifications**: define a security architecture for consumer and connected devices, and on-device services for the management of secure elements
  - **Systems Specifications**: define specifications for the back-office infrastructure for the deployment and management of embedded applications on secure chips

More information

GLOBALPLATFORM
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

http://www.globalplatform.org/specifications.asp

Card | Device | System



GlobalPlatform

Description

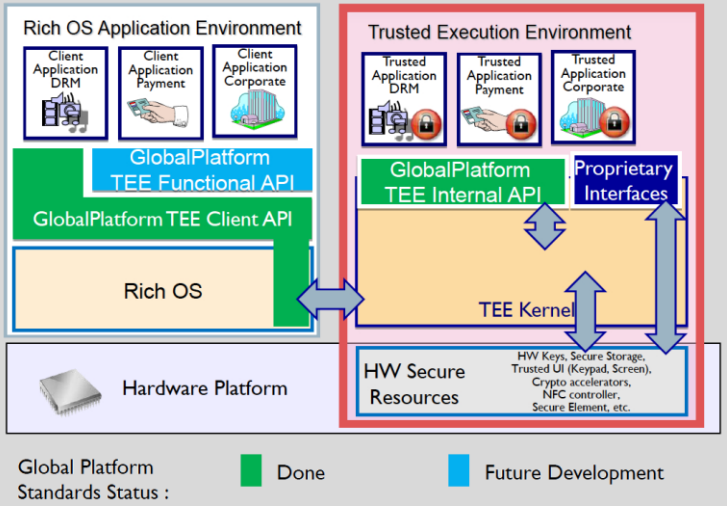
- Cross industry, non-profit association that develops and publishes **specifications** for the secure deployment and management of applications on **secure chip** technology
- Three sets of specifications:
  - **Card Specifications**: define the secure deployment and management of multiple embedded applications on secure chip technology. It defines SDs , SCPs, the SE architecture…
  - **Device Specifications**: define a security architecture for consumer and connected devices, and on-device services for the management of secure elements
  - **Systems Specifications**: define specifications for the back-office infrastructure for the deployment and management of embedded applications on secure chips

More information

GLOBALPLATFORM
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

http://www.globalplatform.org/specifications.asp

Card | Device | System



GlobalPlatform

Description

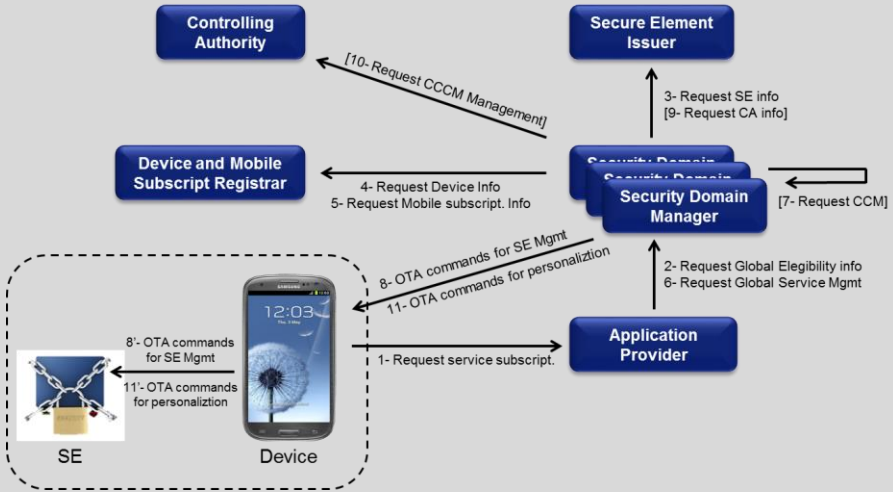
- Cross industry, non-profit association that develops and publishes **specifications** for the secure deployment and management of applications on **secure chip** technology
- Three sets of specifications:
  - **Card Specifications**: define the secure deployment and management of multiple embedded applications on secure chip technology. It defines SDs , SCPs, the SE architecture…
  - **Device Specifications**: define a security architecture for consumer and connected devices, and on-device services for the management of secure elements
  - **Systems Specifications**: define specifications for the back-office infrastructure for the deployment and management of embedded applications on secure chips

More information

GLOBALPLATFORM
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

http://www.globalplatform.org/specifications.asp

Card | Device | System



Application-specific Specifications

The **Application-specific** specifications were developed for a specific type of application (such as payments or identity) and therefore are only relevant to those types of applications.

The main bodies that publish these kinds of specifications are:

For **payment** applications:

- **EMVCo**
- **PCI Security Standards Council**

For **identity** applications:

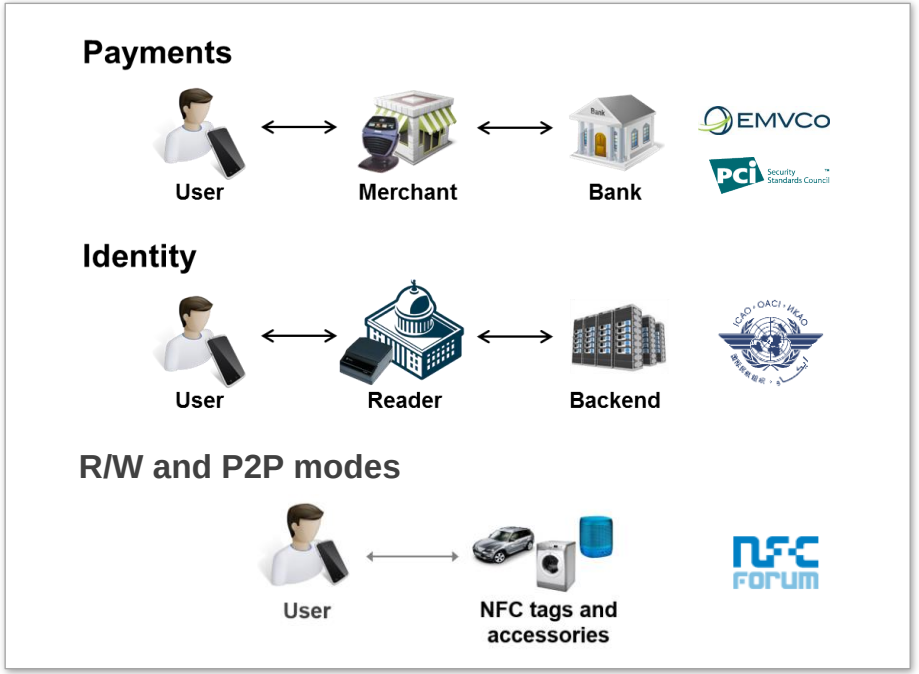
- **ICAO**

For applications based on MIFARE cards:

- **MIFARE4Mobile Industry Group**

For applications that don't use the Card Emulation mode:

- **NFC Forum Specifications**



EMVCo

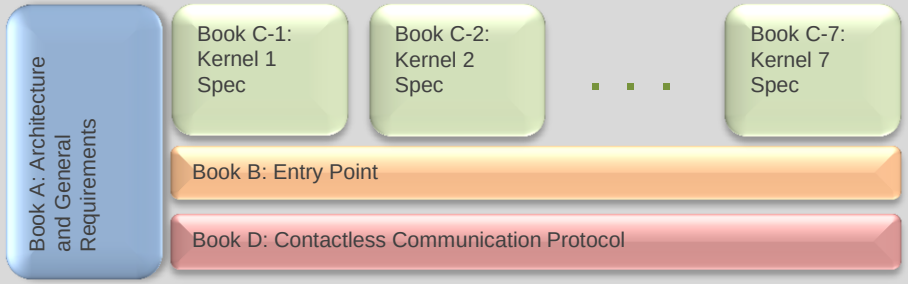
Description

- Public corporation that manages and evolves the **EMV® specifications** and related **testing processes**
- EMV® is a global **standard** for credit and debit payment cards and **financial transactions** based on chip card technology
- Lower layers are based on ISO/IEC 7816 (contact) and ISO/IEC 14443 (contactless)
- The specifications are classified in different “groups”:
  - EMV 4.3 (contact cards)
  - EMV Contactless 2.4
  - Mobile 1.0
  - …
- Different approval tests defined for different devices:
  - Terminal Type Approval
  - Card Type Approval
  - Mobile Type Approval

More information

EMVCo http://www.emvco.com/specifications.aspx

EMV Contactless



PCI Security Standards Council

Description

- Open global forum for the development, dissemination and implementation of **security standards** for **account data protection**
- The **PCI Data Security Standard (PCI DSS)** is their main specification: it describes requirements to store, process or transmit payment cardholder data in a secure way
  - To be PCI compliant requires 3 steps: assess, remediate and report
- Other important specifications:
  - **Payment Application Data Security Standard (PA-DSS)**: for software vendors and other payment application developers
  - **Point-to-Point Encryption (P2PE)**: security requirements and testing procedures for the protection of payment card data
  - **Pin Transaction Security (PTS)**: requirements for all personal identification number (PIN) terminals

More information

PCI Security Standards Council https://www.pcisecuritystandards.org/security_standards/documents.php

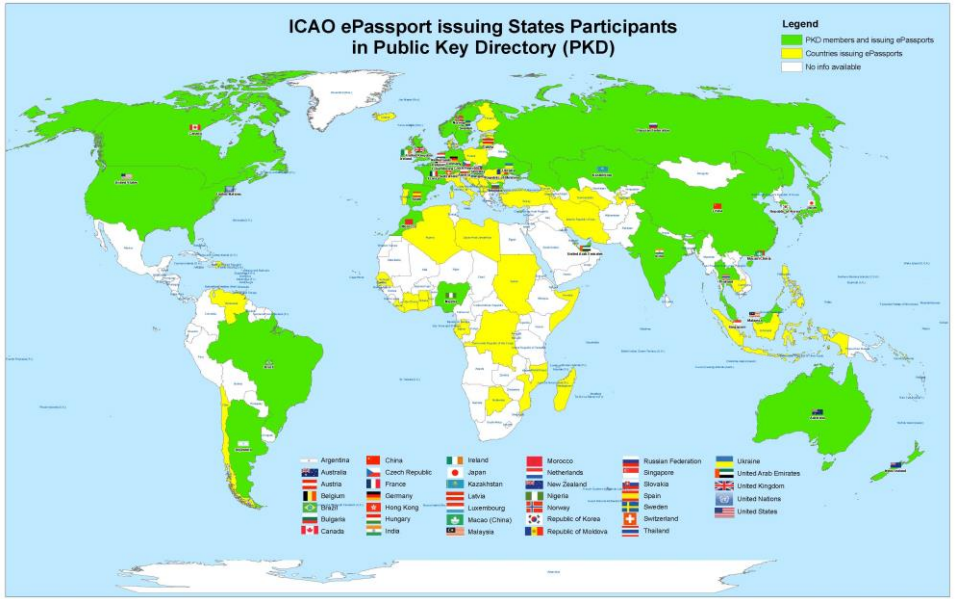
Overview

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

ICAO

Description

- UN specialized agency that develops **international Standards and Recommended Practices** (SARPs) for the **civil aviation regulation**
- Document 9303 contains the ICAO specifications for machine-readable passports, visas and ID cards (Machine Readable Travel Documents, MRTD) used in crossing borders
- It consists of 3 Parts, 5 Volumes and a Supplement:
  - **Part 1 - Machine Readable Passports**
    - **Volume 1**: Passport data stored in Optical Character Recognition (OCR) format
    - **Volume 2**: Passports with biometric identification capability
  - **Part 2 - Machine Readable Visas**
  - **Part 3 - Machine Readable Official Travel Documents**
    - **Volume 1**: Document data stored in Optical Character Recognition (OCR) format
    - **Volume 2**: Documents with biometric identification capability
  - **Supplement**: includes the latest specifications



More information

http://www.icao.int/Security/mrtd/Pages/Document9303.aspx

MIFARE4Mobile

Description

- Industry group that **standardizes** and advances the management of **MIFARE applications** on **NFC-enabled** secure elements, such as SIM cards or embedded secure elements
- MIFARE4Mobile is a set of specifications for the SE (embedded SE, SIM, micro SD) that cover:
  - management of the MIFARE virtual card lifecycle in a mobile handset (Virtual Card Manager)
  - management of MIFARE application lifecycle in a mobile handset (Service Manager)
  - display MIFARE content in the handset screen (Wallet API)
- Used for any MIFARE application that needs to be ported to the smartphone (transit, access, loyalty...)

More information

http://mifare4mobile.org/downloads/specifications_m4m/specifications-v21/

Versions

MIFARE4Mobile 1.01

- Published by NXP in 2008
- Manages a single MIFARE Classic

MIFARE4Mobile 2.1

- Published by MIFARE4Mobile IG in 2013
- Can manage various cards: MIFARE Classic and MIFARE DESFire
- Multiple applications in each of the cards
- Compatible with multiple TSMs
- Supports certification services
- Compliant with GlobalPlatform

NFC Forum ...a global, special interest group (SIG)

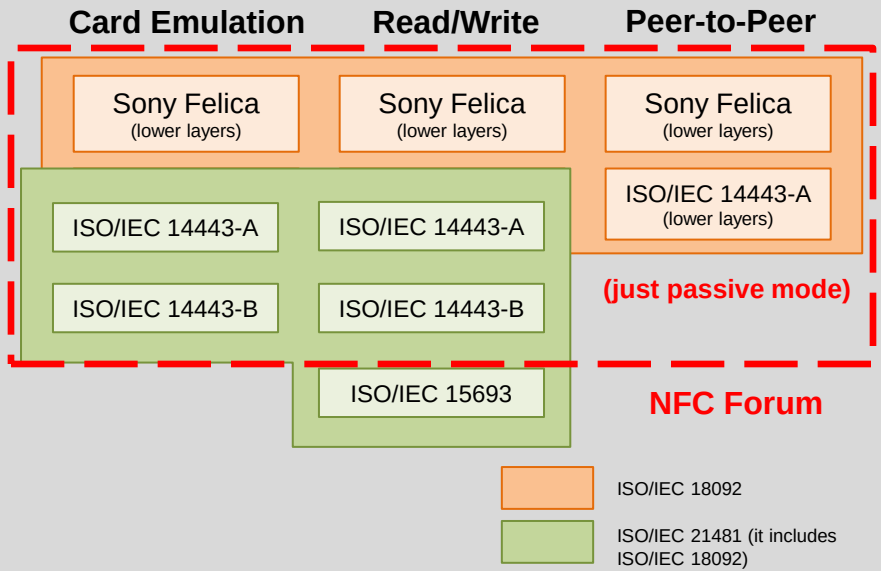
Description

- Non-profit organization established to promote the use of NFC technology in consumer electronics, mobile devices, PCs, and more
- Achieves interoperability between NFC-enabled devices and services through
  - Implementation and standardization
  - Compliance testing and device certification
  - Education of consumers and enterprises
  - Reference designs
- Provides a roadmap for future NFC development
- Focuses on Read/Write and Peer-to-peer modes of operation

More information

http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

Contained Standards | Main Specifications | NFC Forum tags



NFC Forum ...a global, special interest group (SIG)

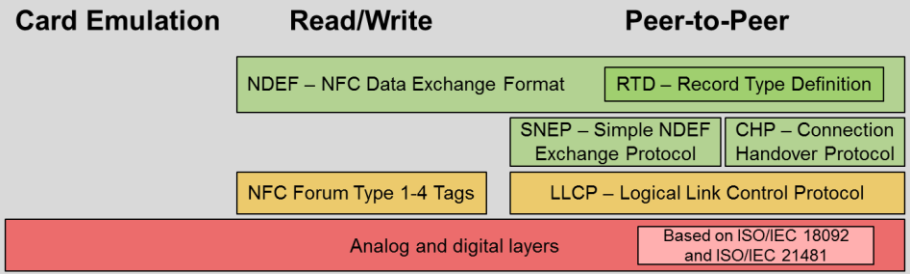
Description

- Non-profit organization established to promote the use of NFC technology in consumer electronics, mobile devices, PCs, and more
- Achieves interoperability between NFC-enabled devices and services through
  - Implementation and standardization
  - Compliance testing and device certification
  - Education of consumers and enterprises
  - Reference designs
- Provides a roadmap for future NFC development
- Focuses on Read/Write and Peer-to-peer modes of operation

More information

http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

Contained Standards | **Main Specifications** | NFC Forum tags



NFC Forum tags: Specifies NFC Forum Tags behavior (command set, memory format…).

NDEF: Specifies a data exchange format for NFC Forum devices and NFC Forum tags.

RTD: 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.

LLCP: Specifies a procedural means for transfer of upper layer information units between 2 NFC Forum devices.

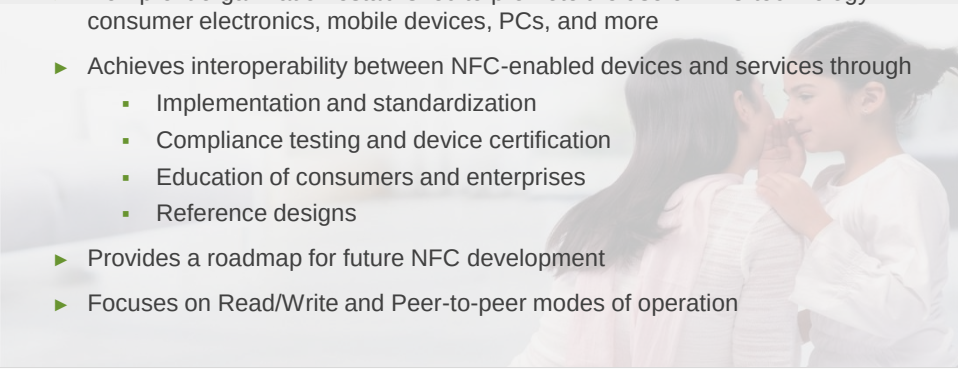
SNEP: Specifies how to exchange NDEF messages over LLCP.

CHP: Combines the simple, one-touch set-up of NFC with high-speed communication technologies, such as WiFi or Bluetooth.

NFC Forum ...a global, special interest group (SIG)

Description

- Non-profit organization established to promote the use of NFC technology in consumer electronics, mobile devices, PCs, and more
- Achieves interoperability between NFC-enabled devices and services through
  - Implementation and standardization
  - Compliance testing and device certification
  - Education of consumers and enterprises
  - Reference designs
- Provides a roadmap for future NFC development
- Focuses on Read/Write and Peer-to-peer modes of operation



More information

http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

Contained Standards | Main Specifications | NFC Forum tags

	Type 1	Type 2	Type 3	Type 4
RF Interface	ISO 14443A-2	ISO 14443A-2	FeliCa	ISO 14443(A&B)-2
Initialization	ISO 14443A-3	ISO 14443A-3	FeliCa	ISO 14443(A&B)-3
Bit rate	106 kbit/s	106 kbit/s	212/424 kbit/s	106-424 kbit/s
Protocol	Specific command Set	Specific command Set	FeliCa protocol	ISO 14443-4 ISO 7816-4
Cost	Low	Low	Moderate	Moderate
Use cases	Tags with small and fixed memory for single applications		Flexible tags with larger memory offering multi-application capabilities.	
Memory type	Memory cards		CPU cards	

NOTE: NFC Forum is currently working on a type 5 tag specification based on the ISO/IEC 15693 standard.

ISO/IEC 7816-4

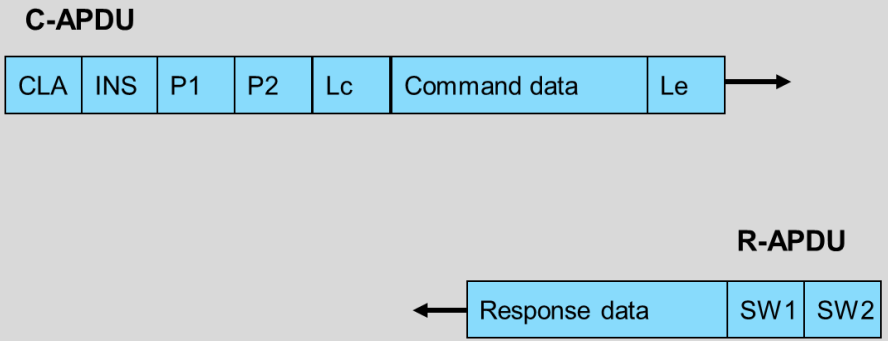
Description

- **ISO/IEC 7816-4** specifies the organization, security and commands for interchange. It defines the following basic features:
  - Contents of command-response pairs exchanged at the interface.
  - Means of retrieval of data elements and data objects in the card.
  - Structures and contents of historical bytes to describe operating characteristics of the card.
  - Structures for applications and data in the card, as seen at the interface when processing commands.
  - Access methods to files and data in the card.
  - A security architecture defining access rights to files and data in the card.
  - Means and mechanisms for identifying and addressing applications in the card.
  - Methods for secure messaging.
  - Access methods to the algorithms processed by the card. It does not describe these algorithms.
- It is independent of the physical interface technology. It applies to cards accessed by one or more of the following methods: contacts, close couple and radio frequency.

More information

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35168

Command structure

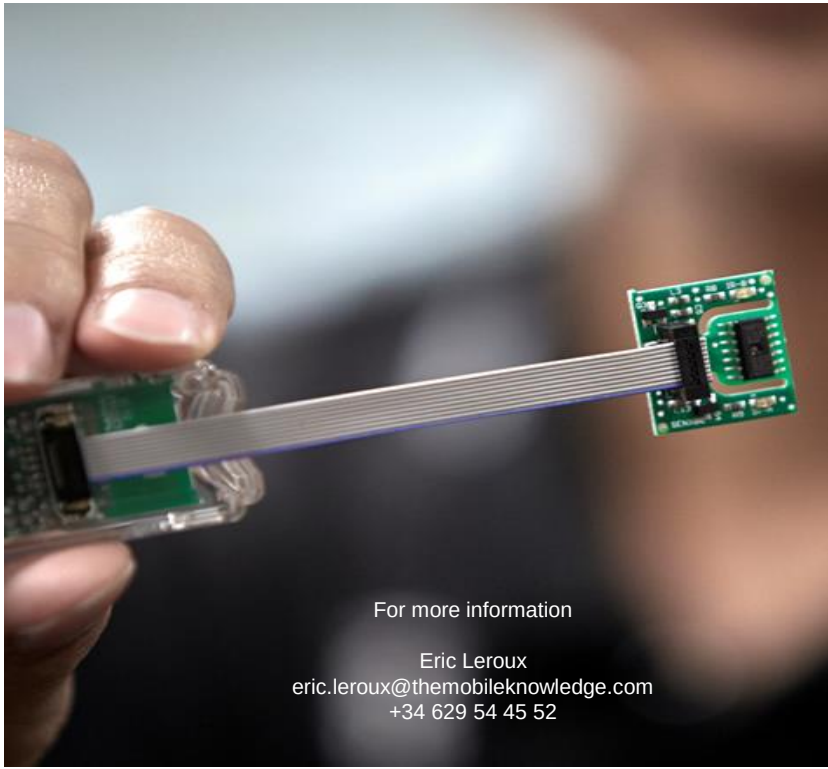


MobileKnowledge

Thank you for your attention

MobileKnowledge
www.themobileknowledge.com

- We are a global competence team of hardware and software technical experts in all areas related to contactless technologies and applications.
- Our services include:
  - Application and system Design Engineering support
  - Project Management
  - Technological Consulting
  - Advanced Technical Training services
- We address all the exploding identification technologies that include NFC, secure micro-controllers for smart cards and mobile applications, reader ICs, smart tags and labels, MIFARE family and authentication devices.



NXP Training Mobile Knowledge

Thank you