springcard®

YOUR EXPERT IN CONTACTLESS SOLUTIONS

WHITE BOOK

RFID, contactless card, NFC.
Understand the convergences and differences to run a project.

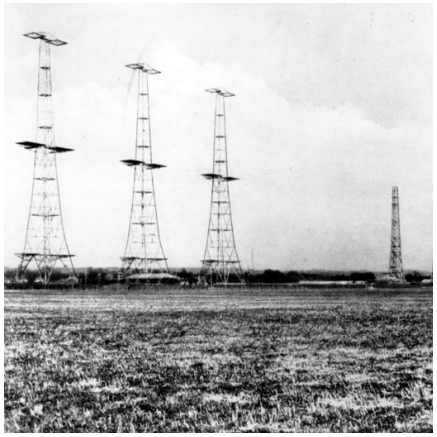
December 2017 CSL17392

SUMMARY

ORIGINALLY WAS THE RADAR...

In years preceding World War II, armies and inventors joined their efforts to create a remote sensing system for planes and ships, the RADAR (**RA**dio **D**etection **A**nd **R**anging).

From the outset of the war, the aerial battle of England highlighted the need to qualify automatically and in a reliable way the echoes displayed on the radar screen: this plane coming across, is it a foe or a friend?



From this vital problematic ensue the quick development of the IFF system (Identification Friend or Foe): an electronic device, embedded in the plane which detects the crossing of a radar beam, and transmit his username in response. This electronic device is called a transponder.

The IFF uses radio waves to identify a mobile object. That establishes the first identification system using radio frequencies (Radio Frequency IDentification, RFID). Across the years, IFF has had derived civilian uses (transponders for airliners) and got secured (cryptography).

The miniaturisation of electronics and the decrease in costs finally allowed the diffusion of RFID in others domains, but the vocabulary still in use today remains marked by the legacy of the military radar system: a base-stations (fixed parts) observes targets (mobile objects), that, technically, are transponders.

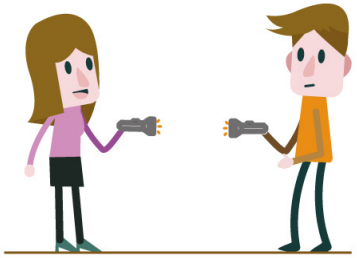
MAJOR POINTS OF AN RFID SYSTEM

ACTIVE OR PASSIVE?

RFID = Radio Frequence IDentification

An RFID system is composed of two parts:
a base station or **interrogator** + a target or **transponder**

These two elements communicate by **radio waves**. The communication mode divides the RFID into two families: the active RFID and the passive RFID.



In **active RFID**: the target has an emitter, and emits his own radio wave. That is typically the case of the plane in IFF system: the transponder answers to the incoming radio wave by issuing his own wave train, on a (potentially) different frequency. That is also the case of the beacons system in BLE (Bluetooth Low Energy): the beacon is an active target, because it sends periodically its information frame, in broadcast, on the 2.4GHz frequency.

In **passive RFID**: the target does not have an emitter. In order to make itself “heard”, it does not have any other choice than alter the interviewer wave. This technique is called backscattering or retro-modulation. For example, a pilot who would stick his arm out of the cockpit window and wave a big flag reflecting waves, would produce on the radar screen a “spot” blinking in an unusual manner. It could be recognized by the base station, without issuing any wave !

RADIO,
BUT AT WHAT FREQUENCY?

For an engineer, “radio” is not an homogenous concept there are techniques and problematics very different according to the radio frequency used. Very low frequencies could propagate very far but they need a huge antenna. High frequencies allow high communication speed (2nd theorem of Shannon), but they are stopped by water and humidity, therefore by the human body...

Between these two extremes, consumption, size and costs criterias will determine which frequency represents the best compromise, according to the communication flow, the practical reach and the directivity wished by the different applications in RFID.

But beyond these technical criterias, **RFID is above all constraints by the regulatory requirements**. In most of countries around the world (if not all of them), the radio spectrum is not a free resource. Some frequency bands are restricted to authorities and military, others are restricted for specific uses (generally valued by licences and fees : radio-broadcasting, television, mobile phones...). Only a few bands are of free use, and free of charge. These are call ISM bands (industrial, scientific, medical) and are a dozen, scattered across the entire spectrum.

Even on these “free” bands, everything is not allowed. You have to coexist with other users of the band (electromagnetic compatibility) and never exceed the limits defined by the medical authorities regarding the exposure of people to electromagnetic fields.

MAJOR POINTS OF AN RFID SYSTEM

Few actors of communication regulation

arcep

ARIB
Association of Radio Industries and Businesses

CEPT ECC
Electronic Communications Committee

ETSI

FCC Federal Communications Commission

ITU International Telecommunication Union

ACTIVE RFID

HOW TO AVOID REINVENTING FOR NOTHING?

In the late 2000, active RFID was the realm of closed-loop systems, each of them based on a protocol that is more-or-less proprietary, more-or-less secure, most of them loading heavily their ISM channel (433MHz, 868MHz or 2.4GHz).

Two variables changed the situation: **the development of wireless networks protocols with low bitrates** and low consumption (IEEE 802.15.4, Zigbee, Thread) and of the Bluetooth Smart also called «Low Energy» (BLE).
the decrease in costs and consumption of chips implementing these protocols.

Why embarrass yourself with an active system that will only do RFID, when wireless networks can offer the same services and allow other uses?

Thus, it became extremely frequent to use standard protocols of wireless networks for identification applications. A well-known example is the iBeacon, a mid-range system using BLE (2.4GHz ISM band).This convergence highlighted new uses, such as in-door geolocation and the interaction with mainstream products, like smartphones. For longer ranges, technical innovation rejuvenated 868 MHz band, now operated by protocols like LoRa and SigFox. More recently, the WiFi alliance decided to follow the same movement with the HaLow protocol.

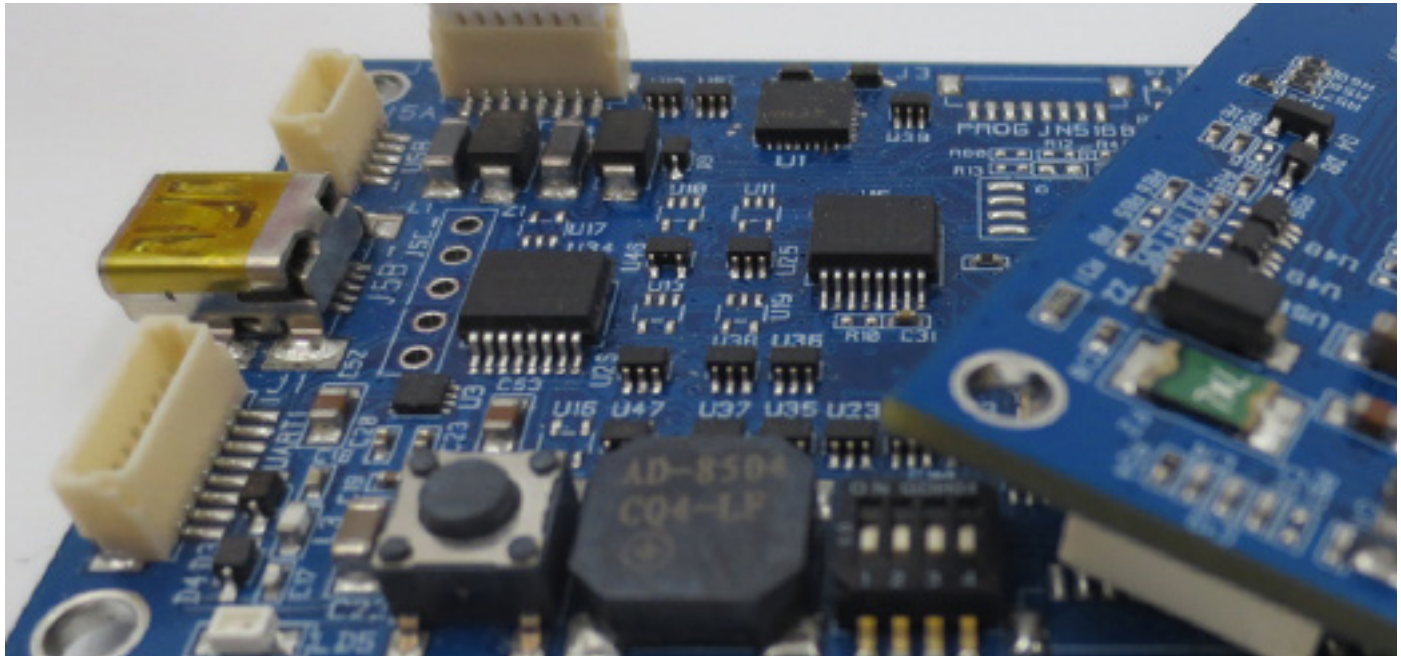
Therefore it became impossible to distinguish the “RFID uses” of the active communication technologies from the other uses of these same technologies.

Throughout the rest of this document, we will focus on the passive RFID; the reader curious to deepen the subject of active RFID will found at SpringCard several achievements based on BLE.

SpringCard guides you through the unification of NFC and BLE uses

ACTIVE RFID

Development platfotm BLE Twist'N'Blue from SpringCard



PASSIVE RFID

HOW TO CHOOSE?

The needs evolve. The systems must evolve too.
The need for contactless badges appeared in the 80's linked with the applications for access control and vehicle downtime. They use 125 kHz band. The systems deployed then showed a wide variety of proprietary protocols and products.

In the 90's, security considerations have increased in fields of transportation and payment, leading to new needs. The volume of data exchanged increased. Progressively, implemented systems gathered around the smartcard world to standardise and concentrate on the 13,56 MHz frequency band.

115/135 KHz
1980's Badges

Anti-démarrage
RFID animale

13,56 MHz
SpringCard
focus

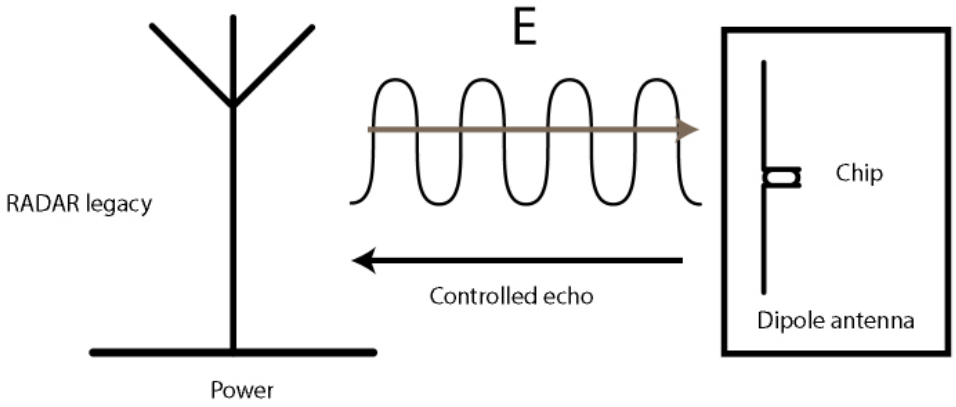
868/910 MHz
UHF - «long»
distance

Logistic
Inventory

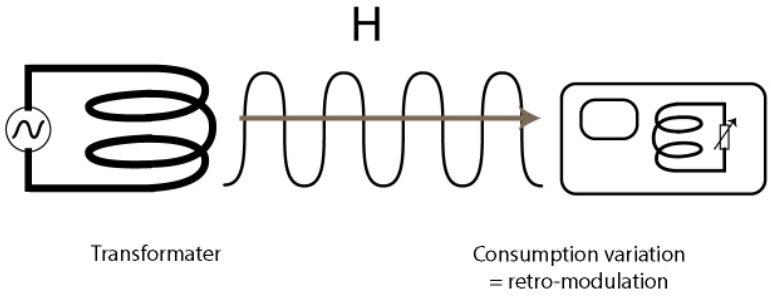
NEAR FIELD
OR FAR FIELD?

PASSIVE RFID

Far field



Near field



The tag is a dipole antenna; its size is mandated by the wave length.
The operating range depends on the strength of the emitter and the sensitivity of its receiver. It goes from 50 cm to several meters (1.5 feet to a few yards).
The directivity is weak.

The practical reach depends on the surface of the two antennas.
The directivity is important.
In the axis, it goes from 5 cm to 1.5 m. (2 inches to 5 feet)
The regulatory limits (strength/modulation rate) reduce the operating range at high bitrates.

FOCUS ON 13,56 MHz

The frequency of 13,56 MHz is the best compromise, when you take into account:

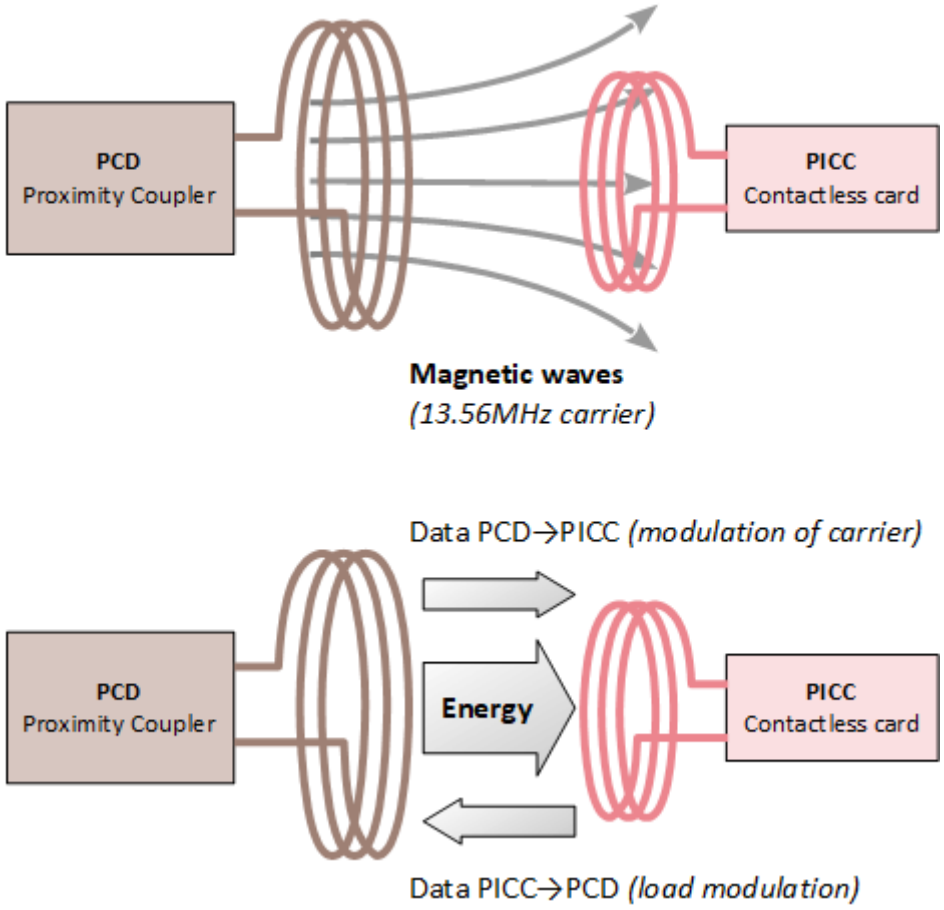
- the need for a communication flow that allows you to conclude a transaction in a reasonable time (ex : validation of a transportation card in 150 ms)
- the need to get through organic materials (user hand)
- the need to respect the regulatory power and size
- the benefit of choosing a frequency band licence-free, available in the entire world
- the state of the art in electronics allowing miniaturisation, minimum consumption and a price answering market expectations

It is the technology chosen by the smartcards experts for proximity and vicinity contactless cards.

Starting from this page, the document only deals with 13,56 MHz.

PASSIVE RFID ON NEAR FIELD

PASSIVE RFID



The magnetic field emitted by the coupler not only provides a power supply to the card, but is also carrying data in both directions:
The coupler modulates its carrier to send its orders, the card uses load-modulation to answer.

This principle of operation is summed up as passive RFID on near field:
For scientists, near field is the part of the space where the distance between both antennas is smaller than wave length. In fact, we use magnetic field rather than electric field. It is passive RFID because the card retro-modulate, it has no emitter.

*PCD: Proximity Coupling Device
PICC: Proximity Inductive Coupling Card

PROXIMITY CARD

HF RFID & PROXIMITY CARD

RFID HF and proximity smartcard are based on the same technical principles. They set themselves apart by the volume of data at stake. When the data volume is low, we will talk more about HF RFID, whereas when the data volume is important or when the security requirements is high, we will talk about contactless smartcard.

The questionof data volume and security is essential because it defines the architecture of the system that will use the card.

- 1 -

The card stores little or no data (only its lot number). It is little or not secured which reduces its cost. The system is based on a central database.

- 3 -

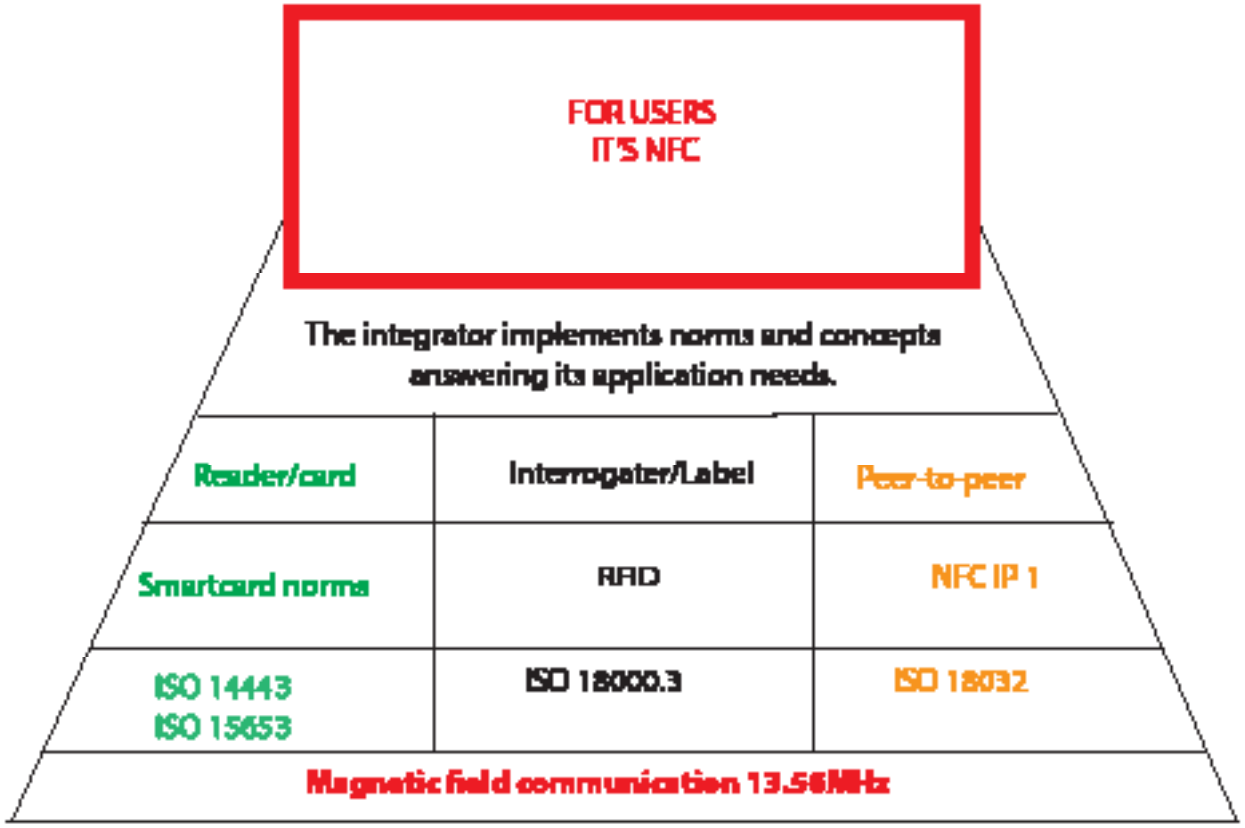
A mixed system alows running with or without network, according to the security level wished and the network availability.

- 2 -

The terminal should be fast and 100% autonomous. All data are stored in the card. Their securing is an essential point.

NFC : WHAT IS IT?

NFC



The magnetic field 13.56MHz is the common technical base on which three different uses are found:
- the use reader+card «classic», eventually reader+card emulation
- the RFID use, for tracability and inventory applications
- the use peer-to-peer, still embryonic and linked with smartphones.

According to its application, the integrator focuses most of the time on one implementation mode, but he can also mix them.

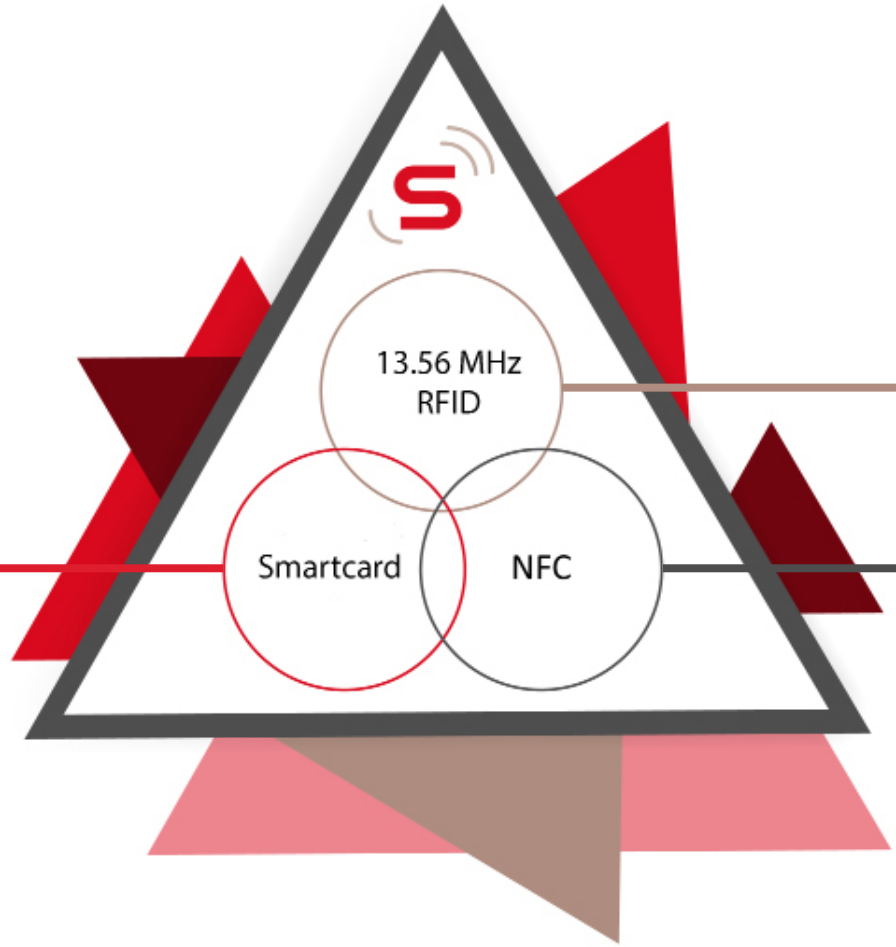
The unifying and simplifying marketing vision tends to gather this wide technical panorama under one label identified by users as «NFC».

13,56 MHz BAND

THE DIFFERENT FACETS OF MAGNETIC COMMUNICATION AT 13.56 MHz

- Payment -
- Paid services -
- People identification -

- ✓ High data volume
- ✓ Crucial security
- ✓ High costs for security (crypotgraphy, PIN, biometry)



- Objects identification -

- ✓ High number of tags
- ✓ Very small tag cost (disposable)
- ✓ Low data volume
- ✓ Little or no security

- Mainstream uses -

- ✓ Open data
- ✓ Peer-to-peer communication
- ✓ BlueTooth and Wifi integration

NORMS OF 13,56 MHz

13,56 MHz BAND

Qualified standardisation committee	Norms linked with NFC and RFID	Frequently used vocabulary
smartcard	ISO 15693 «vicinity» ISO 14443-A & ISO 14443-B «proximity»	coupler - *integrated circuit card* (ICC)
RFID & logistics	ISO 18000-3 «RFD HF»	*Base station* Interrogator - tag
network	ISO 18092 «NFC IP1»	issuer + target

The norm ISO 15693 covers the need for hands free badges. It arises from a working group around Philips Semiconductors (NXP) and Texas Instruments.
The norm ISO 18000-3 M1 is a copy.

There are two norms ISO 14443, arising from working group actions and none could prevail on another.
The -A is the result of a working group in Austria around MIFARE (Mikron then Philips Semiconductors then NXP) and the -B is a counter-proposal from Innovatron (Roland Moreno Technologie, SNCF, RATP).

The norm ISO 18092 «network» resume the major points of norm 14443-A (NXP) and of the Felica card (Sony). It introduces an active mode where partners, interfering in communication, emit a wave at 13,56 MHz in turn.

13,56 MHz BAND

SECTORAL STANDARDS 1/3

NFC FORUM : WHAT IS IT?

NFC Forum is an association initially founded by Philips / NXP, Sony and Nokia in order to promote the use of communication technologies at 13,56 MHz to the mainstream public.

ACTIONS OF NFC FORUM

Under the influence, especially of telephone operators, NFC Forum brings homogenisation of ergonomics and lightering of the mess of cabled logic cards. It also contributes to the convergence of current specification in smartphones with EMV/Transports benchmarks in order to popularize smartphones, as a mean of payment and unique transportation ticket.

However, NFC Forum could not resist to the temptation of re-writing its own version of norms 14443 and 18092, which eliminates latest innovations.

NFC FORUM TAGS

NFC Forum tags are memories, readable in NFC, that contain readable open data: a link for a website or an application, a business card, WiFi parameters of a «guest» network... Smartphones supporting these NFC tags bring an additional comfort with respect to 2D barcode used until now for the same use.

SECTORAL STANDARDS 2/3

13,56 MHz BAND

EMV

EMV is an association that designs the frame of reference for credit card payment. It has been founded by Europay, Mastercard and Visa and it covers 3 technical aspects:

- Card/coupler interoperability, called Level 1 (L1)
- Card application/terminal application interoperability, called Level 2 (L2)
- Terminal/bank server interoperability

SpringCard products proceed at Level 1 (L1), which is divided in two areas:

- the analogical area is based on constraints of practical reach, therefore we deduce field level, reader sensitivity, and a constraint on antenna shape and surface
- the formal (digital) area that ensures communication strength and coexistence of readers and cards from different sources and generations.

EMV CERTIFICATION

SpringCard products are designed in accordance with EMV L1 certification and they can comply with EMV L1 (setting parameters to activate). However, certification only occur on finishied product, it is the integrator of SpringCard OEM subset that should, if he wants to, certify the complete product. SpringCard provides a technical support to clients who start this initiative.

13,56 MHz BAND

SECTORAL STANDARDS 1/3

IN TRANSPORTS

In the early 2000's, the RCTIF framework has been created by STIF (transportation union of Île de France).
As EMV L1 it covers 2 technical aspects: the analogical aspect (field power, sensitivity, practical reach..) and the formal (digital) aspect. The RCTIF, getting old and being a standard for non-standardised adn obselete technologies, is being replaced, at the european level, by ISO CEN TS 16794 norm. This norm includes itself in a convergence initiative with EMV and NFC Forum.

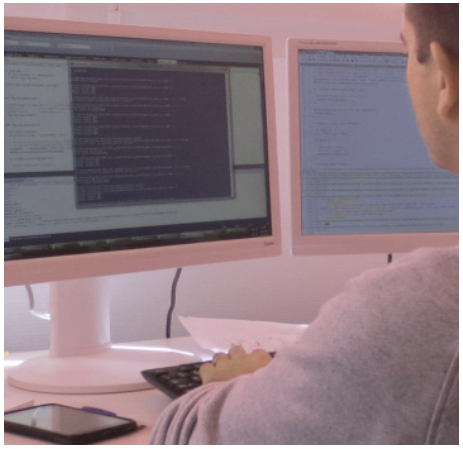
SpringCard products are designed in accordance with RCTIF and ISO CEN TS 16794 normn they can commply with these norms, regarding their settings. As for EMV, certification can occur only on finished products, it is the integrator of an OEM SpringCard subset that should, if he wants to, certify its complete product. SpringCard provides a technical support to clients who start this initiative.

13,56 MHz BAND

3 JOBS

AMO
Assistant to mastery and contracting

Design of systems operating RFID and cards (architecture, integration...)



RESEARCH & DEVELOPMENT

Hardware design for readers / couplers, SDK, Applications

PRODUCTS

Design of ready-to-use readers

ABOUT SPRINGCARD

Educational spirit

This white book is our contribution to the popularization of technologies we implement. If the technical expertise is our matter of specialists, it is necessary that our customers and specifiers master technological choices and constraints, in order to build the solution that will answer their needs at the best cost and highest performance.

Our support is based on an educational spirit : the ideas contributor keeps full control over the implementation of his project. But the industry world shows different problematics submitted to multiple constrints. With SpringCard you are not on your own. Our teams are able to face challenges of performance, compliance with norms and standards, or to support you on applicative implementation of a new service or a specific card.

High level interventions

SPRINGCARD

In 2018, SpringCard will have 18 years of field experience in RFID, NFC and smartcards technologies.
Its engineers possess a strong expertise in the development of strong and efficient buried systems.
They conceive complete architectures executing cryptography and highly secured transactions, around contactless cards or in connected objects world (IoT).
SpringCard realises also forefront implementations for Linux embedded systems, or mobile ones on Android, iOs and Windows.

They gave us their projects

CONDUENT
JCDecaux
DESIGNA
DOM
evolis
IER
NAGRA KUDELSKI
Omnitech security
SAFRAN Morpho
socket mobile
THINFILM Memory Everywhere
xerox

springcard®

YOUR EXPERT IN CONTACTLESS SOLUTIONS

You have a project?
You wish to contact us?

Our team will be pleased to answer you at this address:

contact@springcard.com

or by phone at:

(+33) 1 64 53 20 10

To know more about SpringCard,
visit our website :

https://www.springcard.com