ASPROM / UIMM 2014

Near Field Communication

NFC

… ou 15 ans de ma vie
résumés en quelques minutes !!

dp-Consulting
Directeur & CTO

Dominique Paret ??

« ex » PHILIPS/NXP SemiConductors *(… que pendant 40 ans ! …)*

Advanced Technical Support Mgr

Emerging Business / Innovation & Systems

Automotive & Identification Markets

***dp*-Consulting, fondateur/CTO depuis 2006**

- *société de Services (Expertises et Consultants) & Formations*

de plus

- enseignant dans de nombreuses écoles d'Ingénieurs (Bac+5 et +6)
- membre des Conseils Scientifiques de plusieurs grandes écoles
- membre de l'AFNOR & l'ISO pour toutes les applications « sans contact » (SC 17/ SC 31 / TC 23 / SC 6 …) et « automobile » (BNA, etc.)
- expert auprès de COFRAC et OSEO/BPI pour tout ce qui est « sans contact »
- membre des groupes EESTEL, Pôle Compét.,GTRF Ministère Transport
- 25 ouvrages tech. (éditions DUNOD, John Wiley, Paraninfo, Acorn, PHEI)

Au Menu … que de la technique

- Bases du NFC
- Principes de fonctionnement du NFC

- Possibilités applicatives
- Technologies du NFC Devices
- Champs applicatifs

- Les problèmes actuels
- Le serpent de mer qu'est la sécurité
- Implémentation en téléphonie mobile
- Proposition HCE

- Conclusions

Pour commencer, deux minutes d'histoire

… déjà que 20 ans d'histoire à 13,56 MHz !

RFID / Carte MIFARE (Mikron, Philips SC)	~1994
Normes ISO 14 443	1999/2000
Début étude NFC (Philips SC, Sony)	1999
Normes NCF IP1 & IP2 ECMA puis ISO	2002
Naissance NFC Forum (Philips SC, Sony)	2004
…….	
Boum téléphonie mobile SAMSUNG	2011
Boum Android'ssss Google	2012
Google Android 4.4 HCE	2014

Bases Physiques

Champ Proche – Near Field

… de la RFID au NFC via les cartes à puce sans contact ….

« Near Field » = de la physique !!

Une onde électromagnétique est caractérisée par sa fréquence « f » et sa longueur d'onde « λ » associée. La relation liant « f » et « λ » est bien connue : $\lambda = v / f = (3 \times 10^8) / f$

Near Field
« champ proche »
(couplage magnétique)
(Biot & Savart law)

< λ / (2 π) <

Far Field
« champ lointain »
(propagation d'onde)
(Maxwell equations)

fonctionnement en :

exemples en RFID

f = 150 kHz	λ = 2 km	« champ proche »
f = 10 MHz	**λ = 30 m**	**« champ proche »**
f = 900 MHz	λ = 33 cm	« champ lointain »
f = 3 000 MHz = 3 GHz	λ = 10 cm	« champ lointain »

NF« C » … et distances de fonctionnement

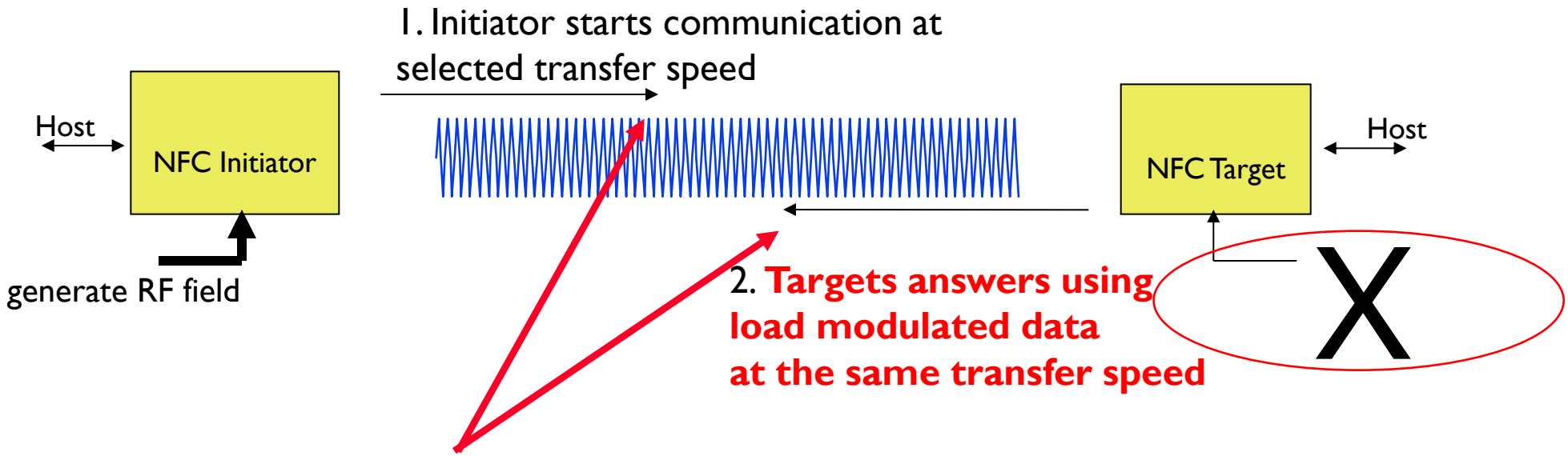
Du fait des contraintes des règlementations RF (ERC 70 03, ETSI 300 330), à f=13,56 MHz, en Near Field, les distances de fonctionnement sont courtes et elles sont réduites à environ 20 cm max

Plus généralement, d'une manière applicative, à cause des contraintes de privacy, environnement, possibilités d'attaques de types MiM, sécurité, etc.) en réalité, **les distances de fonctionnement des applications « NFC » sont ramenées à quelques 3 – 5 cm**

Principes & Techniques spécifiques aux « NFC »

NFC - Communication Modes

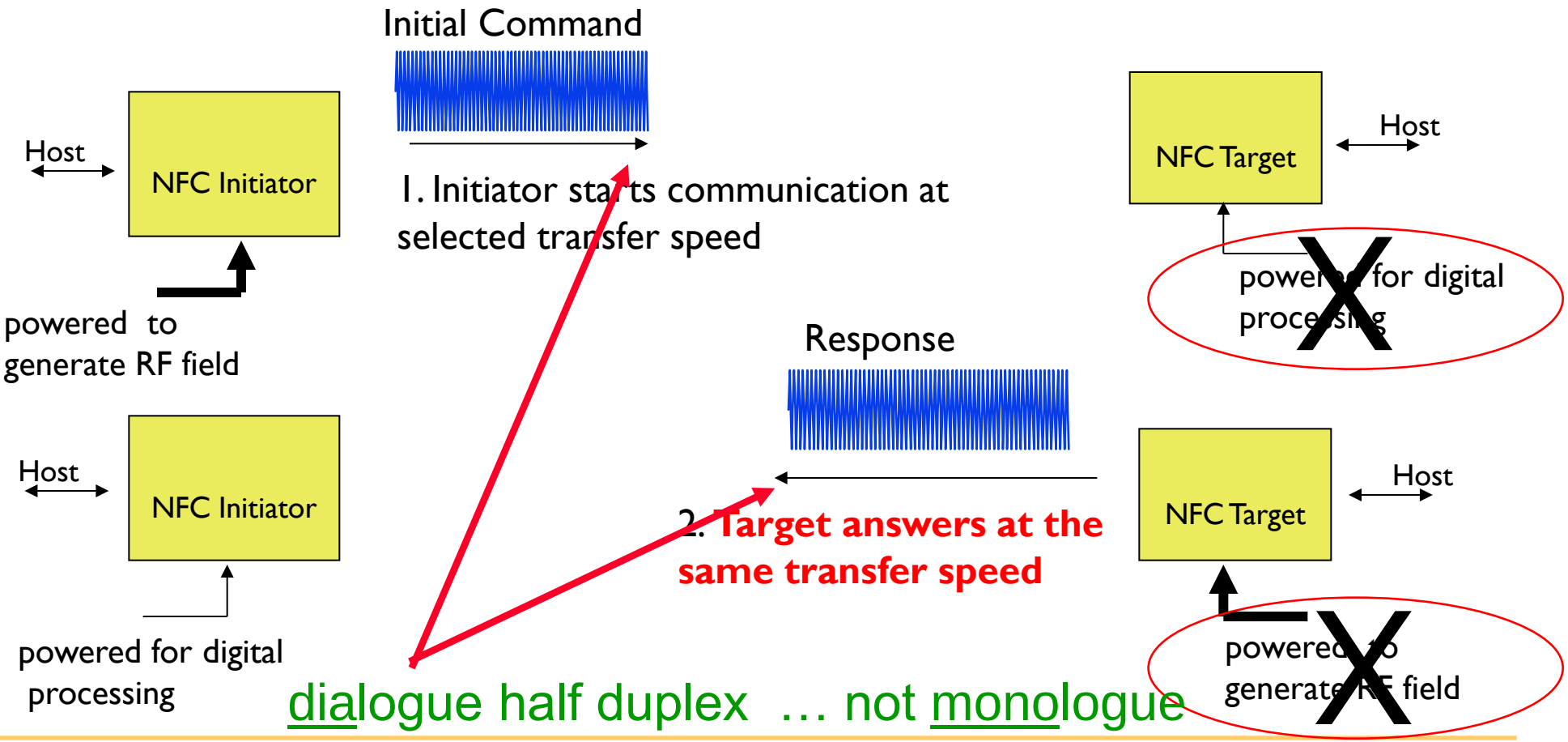
Passive communication mode (… comme les CàP)



dialogue half duplex … not monologue

NFC - Communication Modes

Active Communication mode (... différent des CàP)



dialogue half duplex … not monologue

Near Field Communication versus Smart Card & RFID

- Both Smart Card & NFC are in HF @ 13,56 MHz
- Both Smart Card & NFC are in Near Field

But

- Smart card, only passive (retro mod), data collision

- NFC, passive **or** active, RF **and** data collisions

And, don't forget that

- *RFID all frequency bands, LF, HF, UHF, SHF,*
  Far field, Near field …
  Passive or Active, RF et data collisions, etc.

Les normes et standards

- Les **« normes NFC »** (… en 2002 !!)

Normes	ECMA 340 & 352
(ouvertes)	ISO 18 092 - **NFC IP1** (~ISO 14 443A & Felica)
	ISO 21 481 - **NFC IP2** (~ISO 14 443A-B & Felica, ~ISO 15 693)
	ISO 22 563 tests (ISO 10376-6 ++)

- Les « autres standards autour du monde NFC »

Standards	NCF FORUM
(propriétaires)	~ETSI (… SWP)
	EMVCo ……
	GSM A

Stop !!!

- **C'est là où s'arrête le vrai terme « NFC »,**

- Là où commence le monde des applications basées sur NFC

- Tout le reste « is blabla !! ….. »

- **SVP, arrêtons les gargarismes marketing et commerciaux avec le terme NFC à toutes les sauces !!**

Possibilités Applicatives

- Les possibilités applicatives :

  - Les 4 cases physiques génériques

  - Les 4 cases applicatives

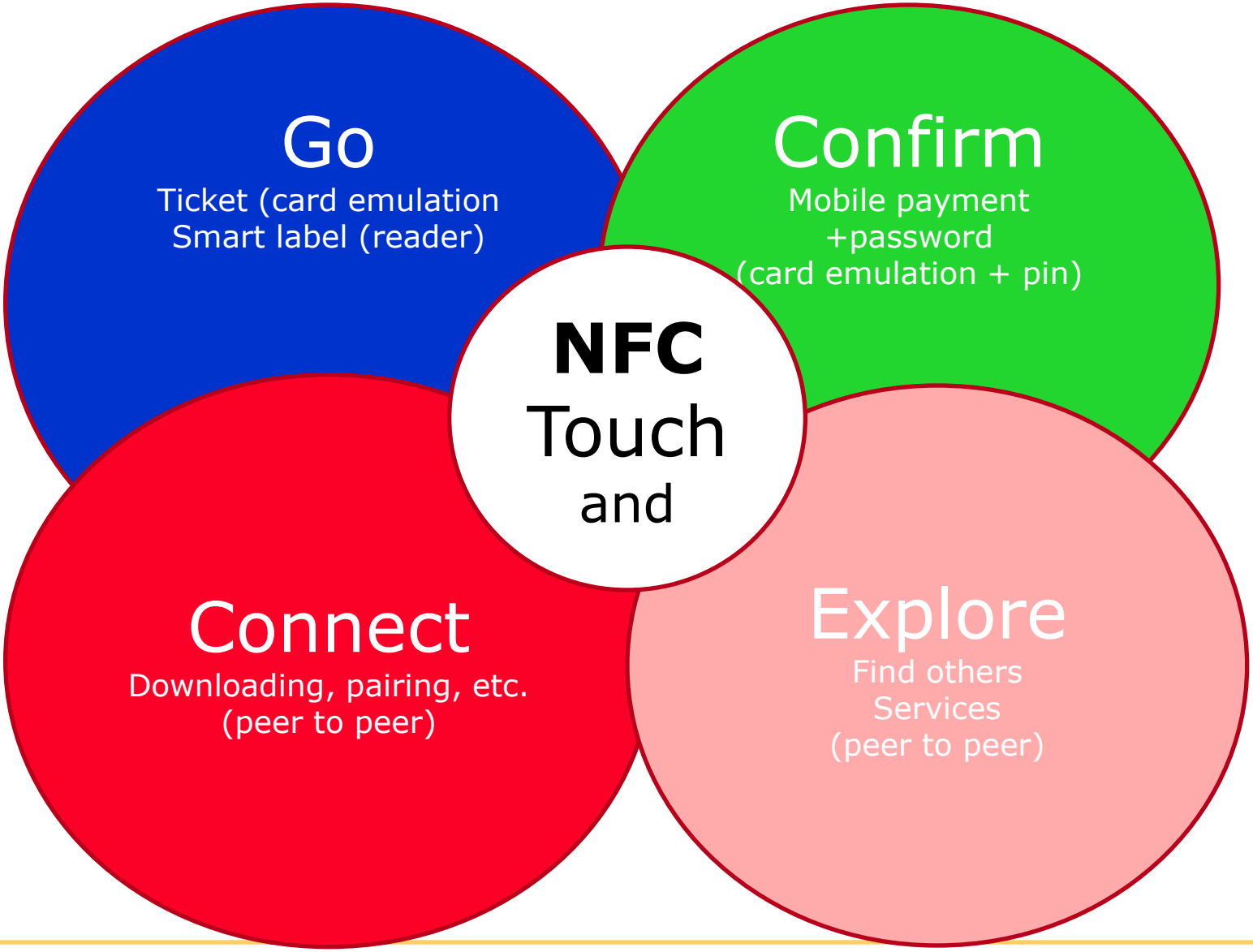
Les 4 cases physiques

Les principes de fonctionnement normalisés

Supply versus tag to interrogator communication

Tag to base station **com.** / **Supply**	via load modulation retro modulation / back scattering	Via transmitter
No battery on board	**Passive** Batteryless	**Active** Batteryless
Battery on board	**Passive** Battery assisted	**Active** Battery assisted

Les 4 cases applicatives



Touch & Go

« Touch & Go » suite à la présentation d'un « NFC device » on déclenche une action sans en confirmer la validation.

Dans ces cas l'utilisateur ne nécessite que de présenter à la base station (interrogateur, lecteur) l'élément (NFC Device, ticket, jeton, badge, cartes, téléphone mobile, tabets, etc.) contenant par exemple un code d'accès, pour

Touch & Confirm

« Touch & Confirm » nécessitent de présenter à l'interrogateur un NFC device possédant une interface home machine (écran, clavier, etc. par exemple) au travers duquel l'utilisateur doit effectuer une action / un geste volontaire pour confirmer l'interaction en entrant un code ou un mot de passe ou encore ou juste acquiescer/valider la transaction.

Touch & Connect

« Touch & Connect » est celui dans lequel on met en relation, face à face, deux NFC devices de façon à ce que ceux ci soient capables d'établir entre eux une communication et un transfert de données par exemple de type « peer to peer »

Touch & Explore

« Touch and Explore » est celui dans lequel les NFC Devices peuvent proposer à l'utilisateur plusieurs fonctions.

Le consommateur sera alors en mesure d'explorer les capacités d'un appareil pour découvrir les fonctions et les services proposés.

Conséquences Applicatives

17h 30

Les 3 modes principaux de fonctionnement des NFC devices

- **« Writer / Reader »**

- **« Peer to Peer », NFC device to NFC device**

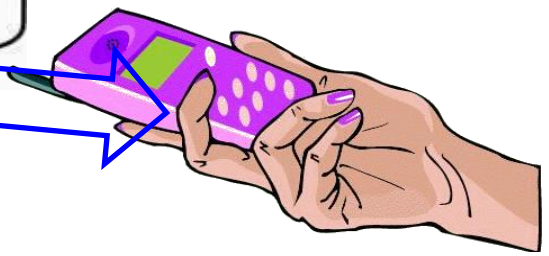
- **Emulation de cartes à puce … mais lesquelles**

NFC Device :

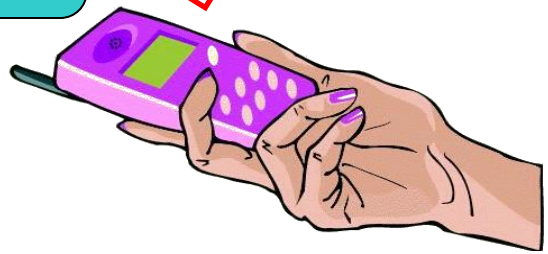
Card Emulation

Device-to-Device

Reader



Contactless Card / Tag



champs d'applications du NFC

… notamment, parmi le large éventail des possibilités applicatives

- celles à émulation de cartes passives battery assisted

- celles à émulation de cartes passives télé alimentée

- familles de produits aptes à satisfaire les normes ECMA / ISO

Technologies du « NFC device »

du « Citadin 2.0 »

« Form factor » des NFC devices du « Citadin 2.0 »

- fob / carte / badge / ticket / jeton / clés /clé USB / …
- avec clavier ayant une fonction oui/non
- avec clavier et écran
- avec clavier + écran + intelligence
- avec clavier + écran + intelligence + autres RF
- couteau suisse incluant ….. + WiFi, Bluetooth, Zigbee, capteur image, position, accélération, gyro, mouvement, compas, proximité, température, humidité, baromètre, … …machine à café, brosse à dent, etc. et re etc.

- Bref, … **“The Ultimate Man Machine Interface”**

“The Ultimate Man Machine Interface”

… vous les avez tous reconnu !!!

Les « SmartPhones » et
les « Tablettes » NFC !

Three Main NFC Application Categories

Card Emulation Mode

Transactions:

Mobile payment, Ticketing, Access control, Transit, Top-ups, Toll-Gate

Peer-to-Peer Communication

Connectivity:

Data transfer: Fast, easy & convenient device association, setup & configuration

Reader Mode

Service Discovery:

Content distribution, Information access, Smart advertising

Mono « NFC device »

A NFC device (ex: phone: one single communicating device)

Champs Applicatifs

... et les soucis qui arrivent ...

SVP … NE PAS ou PLUS CONFONDRE !!!
… Eviter les confusions !!!

- Le « NFC » … ce n'est que de la pure physique

- « NFC IP1 & IP2 (ISO 18092 & 21481) » … sont des protocoles de communication fonctionnant en NFC, à 13,56 MHz

- Utilisations…ssss générales des protocoles NFC IP1 & IP2
  (… et par la même occasion souvent avec spécifications NFC Forum)

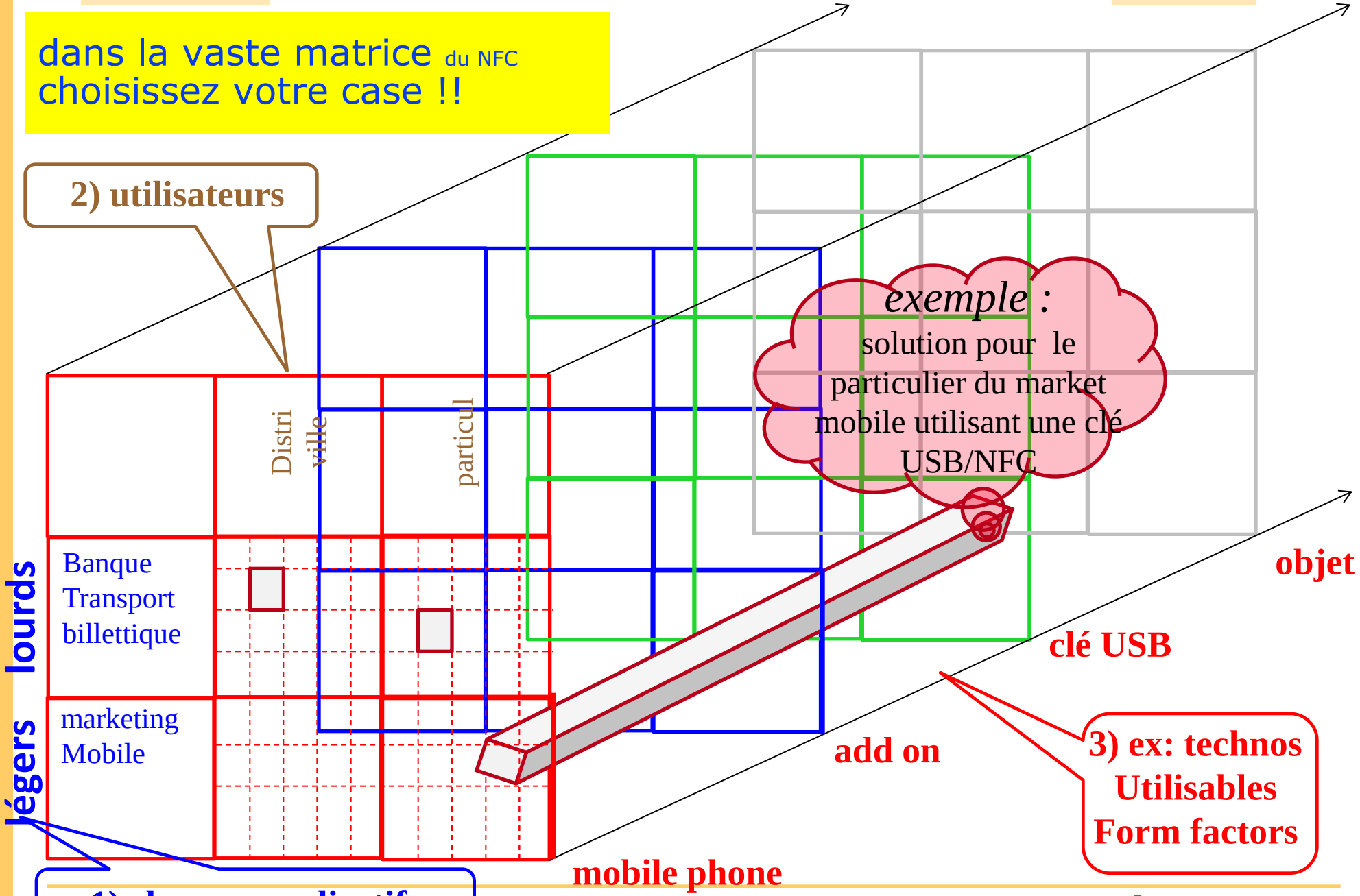
CA, C'EST LE « NFC » !!

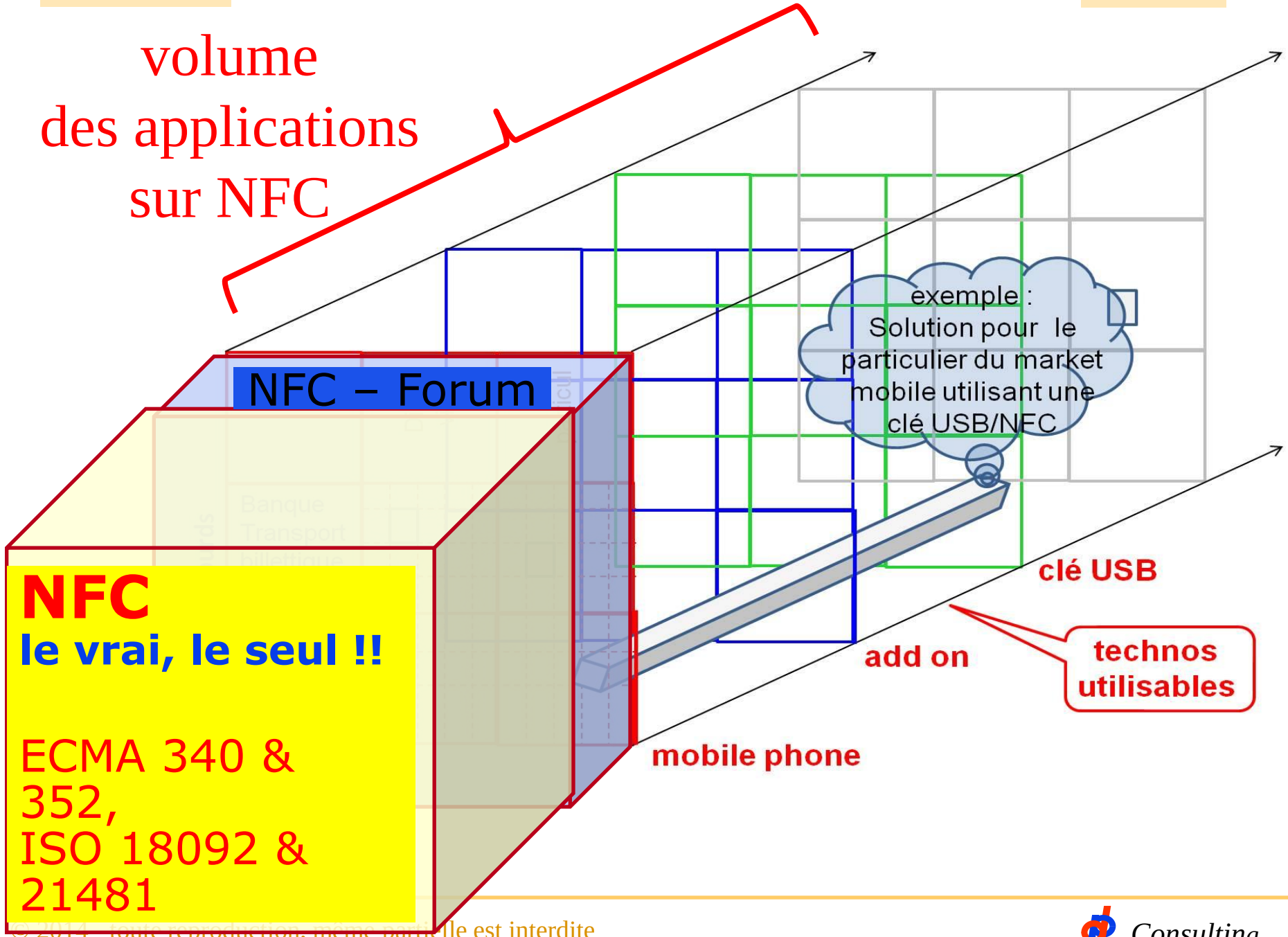
- Utilisations…ssss spécifiques des protocoles NFC IP1 & IP2 en téléphonie mobile

- Utilisations des NFC IP1 & IP2 à des applications…ssss bancaires &/ou transports à l'aide de téléphones mobiles

CA, CE SONT DES APPLICATIONS SUR DU NFC

dans la vaste matrice du NFC
choisissez votre case !!





Vue de l'utilisateur

- Appli.ouvertes, propriétaires, sectorielles, intersectorielles

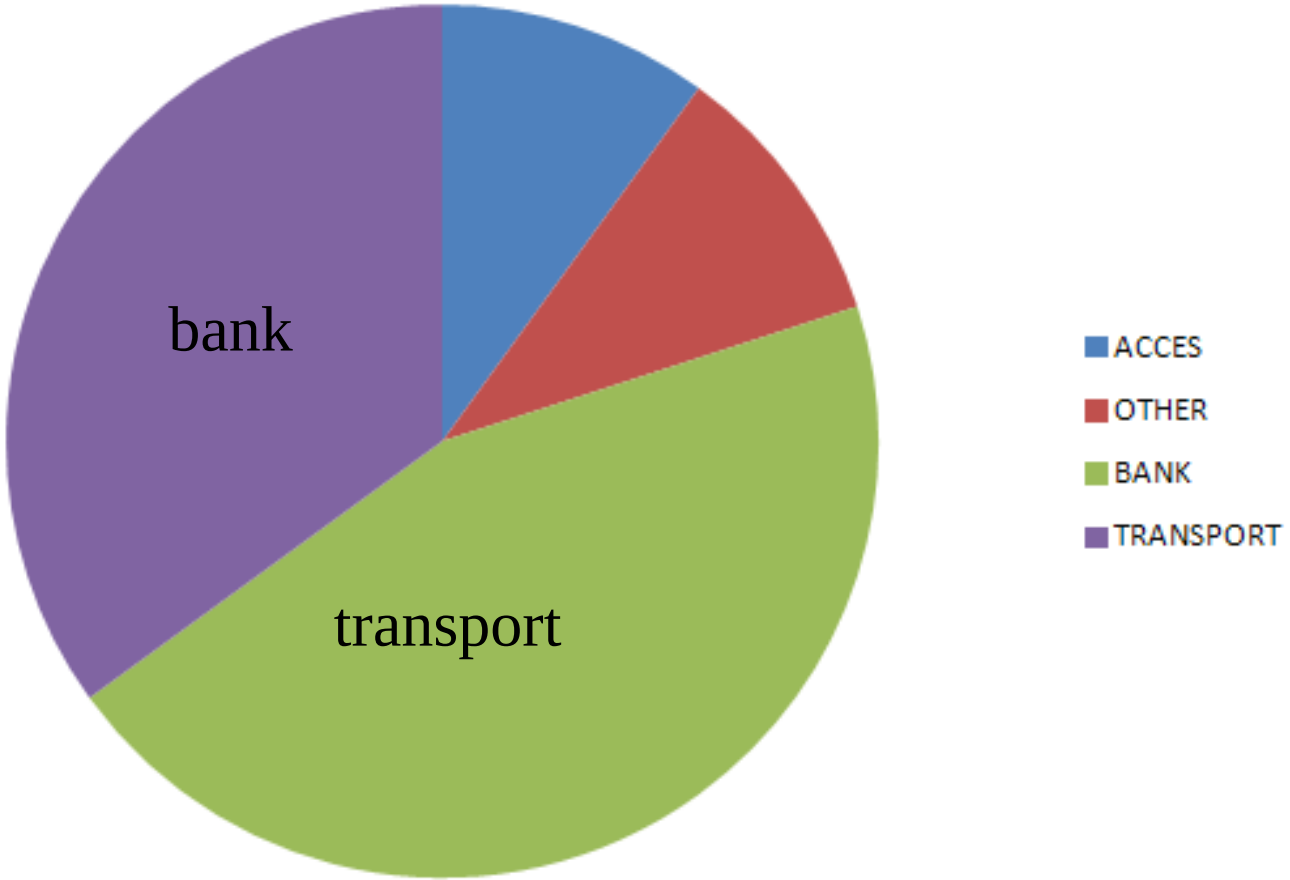
ouvertes	…	
propriétaires	automobiles	BMW, Audi
sectorielles	bancaires,	EMVCo,
	transport,	AFIMB
	aviation,	IATA
intersectorielles	paiement, transport, accès, etc. exemples : VILLES, TERRITOIRES	

- Les applications basées sur le NFC en téléphonie mobile
  - Paiement, transports, aviation, accès, etc.

- La structure (complexe) des applications basées sur le NFC en téléphonie mobile
  - Secure Element
  - SIM, SWP, HCI and Co
  - Applications Multi Sectorielles
  - Sécurités / attaques / …
  - TSM
- Les nombreuses autres applications basées sur le NFC
  - Médical, Grand Public, Automobile, etc.

2014 –répartition du marché NFC

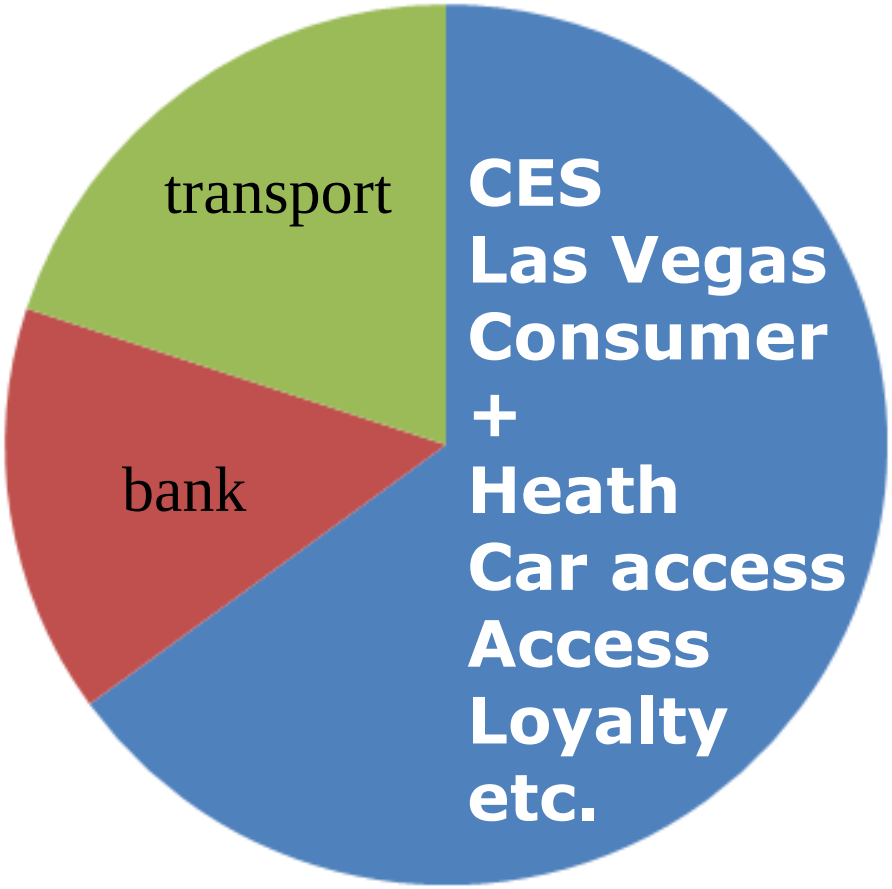
Applications Bancaires / paiement et transport fonctionne au travers des téléphones mobiles



Après 2020 –répartition du marché NFC

Applications bancaires et transports ont augmenté … mais les autres applications NFC se sont fortement déployées !

C'est la cible totale qui intéresse les fabricants de composants !!!!



Hors banking
Hors transport

Les segments de marché

- Consumer (TV, cameras, etc.)
- Domestic appliances (refrigerators, washing machine, etc.)
- IT (PC)
- Mobile Phone
- Monetic
- Tracking (Supply Chain and Item Management)
- Communication, Pub,
- Social
- Medical,
- etc.

l'immense champ d'applications

L'éventail des modes de communications « actifs » et « passifs » du concept NFC et toutes les variantes d'alimentation possibles « batteryless » et « battery assisted » permettent d'envisager de très nombreuses applications du NFC et ce, dans de nombreux marchés aux acteurs, aux intérêts économiques, et usages très spécifiques … donc à de très nombreux problèmes architecturaux, techniques, sécuritaires, etc. à résoudre … et nous ne sommes qu'au début de l'histoire du NFC !!

Quelques exemples applicatifs urbains

- Contrôle d'accès à des locaux en accès réservé (salle de réunion, entreprise, salle de cours, etc.) ;

- Lecture d'une carte de visite électronique avec un PDA ;
- Echange de profils entre deux utilisateurs d'un réseau social ou de niveaux de jeux en rapprochant ("tapant") les deux téléphones (mode pair-à-pair) ;
- Synchronisation de signets Internet et de contacts entre un PDA et un téléphone portable ;

- Récupération de la clef WIFI d'un point d'accès en approchant son « périphérique NFC » de la borne de diffusion.

- Paiement utilisant une carte bancaire sans contact, ou un appareil mobile sur un terminal de paiement sans contact ;

- Paiement du parking à une borne acceptant le paiement sans contact à l'aide de son terminal mobile NFC ;

- Achat et validation sans contact d'un titre de transport ou d'un billet d'entrée à un spectacle avec son mobile ;

- Lecture d'informations produits (prix, composition, allergie, etc.) en magasin ;
- Gestion de coupons de réduction dans un magasin,
- Gestion de points de fidélité chez les commerçants (*couponing*) ;

- Accès et démarrage d'un véhicule à l'aide de son téléphone mobile ;

Les problèmes actuels

… de différentes natures …

Mélanges et confusions de normes proches … mais en fait très différentes

A ce jour, trop de personnes confondent le sens précis des termes NFC, cartes à puce sans contact, RFID et ce que cela représente … et, pour suivre la mode ambiante, baptise le tout NFC … ce qui crée sans arrêt une grande confusion sur le terrain.

Souhaitons que la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes mette son nez là-dedans au plus tôt pour éviter les publicités mensongères qui trompent le consommateur que nous sommes tous !!

Comment mesurer les performances et où et comment les certifier – conformance -

Pour savoir si des produits sont dignes de porter le nom de « NFC » il faut les tester (!),

- pour les couches « Basses » OSI selon les normes ISO IP1 (18 092) et IP2 (21 481) et ISO 17 025 dans des laboratoires indépendants accrédités en France par le COFRAC et,

- si nécessaire, pour les couches « Hautes » de l'OSI selon les laboratoires « propriétaires » du NFC Forum

Environnements hostiles des applications

loading effects (incidence de la target sur l'initiator)

L'environnement métallique d'un smartphone (boitier, écran, batterie, etc.) n'a pas du tout la même incidence qu'une simple carte à puce en plastic sur le champ magnétique produit par un Initiator, d'où **loading effect**.

De même, le facteur de forme du NFC Device a une très forte incidence sur le loading effect et ses performances

Repenser le mécanisme de rétro modulation,

Dans le cas usuel d'utilisation NFC, en « card emulation » si chère aux dispositifs de paiement via smartphones, la présence d'environnement hostile a une forte incidence sur la rétro modulation par modulation de charge.

La « modulation de retour Active », en fin de normalisation à l'ISO, sera d'un grand secours.

Présences de shunts

Les fortes variations des valeurs de champs magnétiques des bases stations / initiators (de 1,5 à 7,5 A/m) dans la zone possible de fonctionnement imposent l'emploi d'élément shunt dans les circuits intégrés pour en limiter les conséquences … qui ont un effet néfaste sur le loading effect et la retro modulation et le bon fonctionnement de la communication en technologie de champ proche

Interopérabilités applicatives

On ne peut terminer cette présentation sans évoquer les problèmes d'interopérabilités fonctionnelles entre branches applicatives.

En effet les contraintes sectorielles des Banques (EMV) sont par beaucoup d'endroits antinomiques de celles des Transports (AFIMB, CEN) ou bien encore de celles de l'Automobile (EMC, Wireless Power), ou celles des Villes et Territoires, etc. … et vice versa !

Interopérabilités applicatives

Ces problèmes surgissent sont difficilement surmontables lorsque l'on envisage d'utiliser un mono NFC Device (par exemple un « smartphone ») pour satisfaire toutes les applications … sans compter les autres problèmes économiques (écosystèmes, ROI, etc.)

… mais ceux-ci sortent largement du cadre de cet exposé technique et c'est une autre histoire !

- Interopérabilités, conformités, certifications, etc.

- Empilement de temps de développement, de tests, de conformités, de temps de tests de conformités, de coûts (… sans compter pour certains les chères adhésions*)

ISO NFC IP1 / IP2 et tests de conformance

NCF Forum* et de tests de conformance

CA, C'EST LE « NFC » !!

ESTI … SWP HCI

GSM A*

Global Platform*

EMVCo*

AFIMB

CA, CE SONT DES APPLICATIONS SUR DU NFC

OS Android ……etc.

EXEMPLES

Le serpent de mer*

! La sécurité du NFC !

** On qualifie de « serpent de mer » un projet ou un sujet qui revient fréquemment alors que sa mise en application, son développement ou son aboutissement ne semble pas arriver ou bien être repoussés continuellement … depuis ~ 2004, … ça ne fait que 10 ans !!!*

J'en ai *marre* d'entendre cette phrase !

Ne pas confondre :

- « NFC (sans contact) » ou « applications sur NFC »
- « Couches basses » ou « couches hautes » OSI
- « NFC », et que les applications bancaires & paiements

De plus, se rappeler que depuis longtemps les liaisons cartes sans contact bancaires sont en accord avec les **Critères Communs** CC, (normes ISO 15408) et sont de niveaux EAL5, 5+, 6 et 6+ !!!!!!!!

Par contre, qui définit la « cible de sécurité », verrouille, détient et est responsable la sécurité ??

Bonne question

Architecture hard du « NFC device » choisi
Qualité du soft de l'appli
Conformité / Homologation / certification

NFC, architecture and Secure Element (SE)

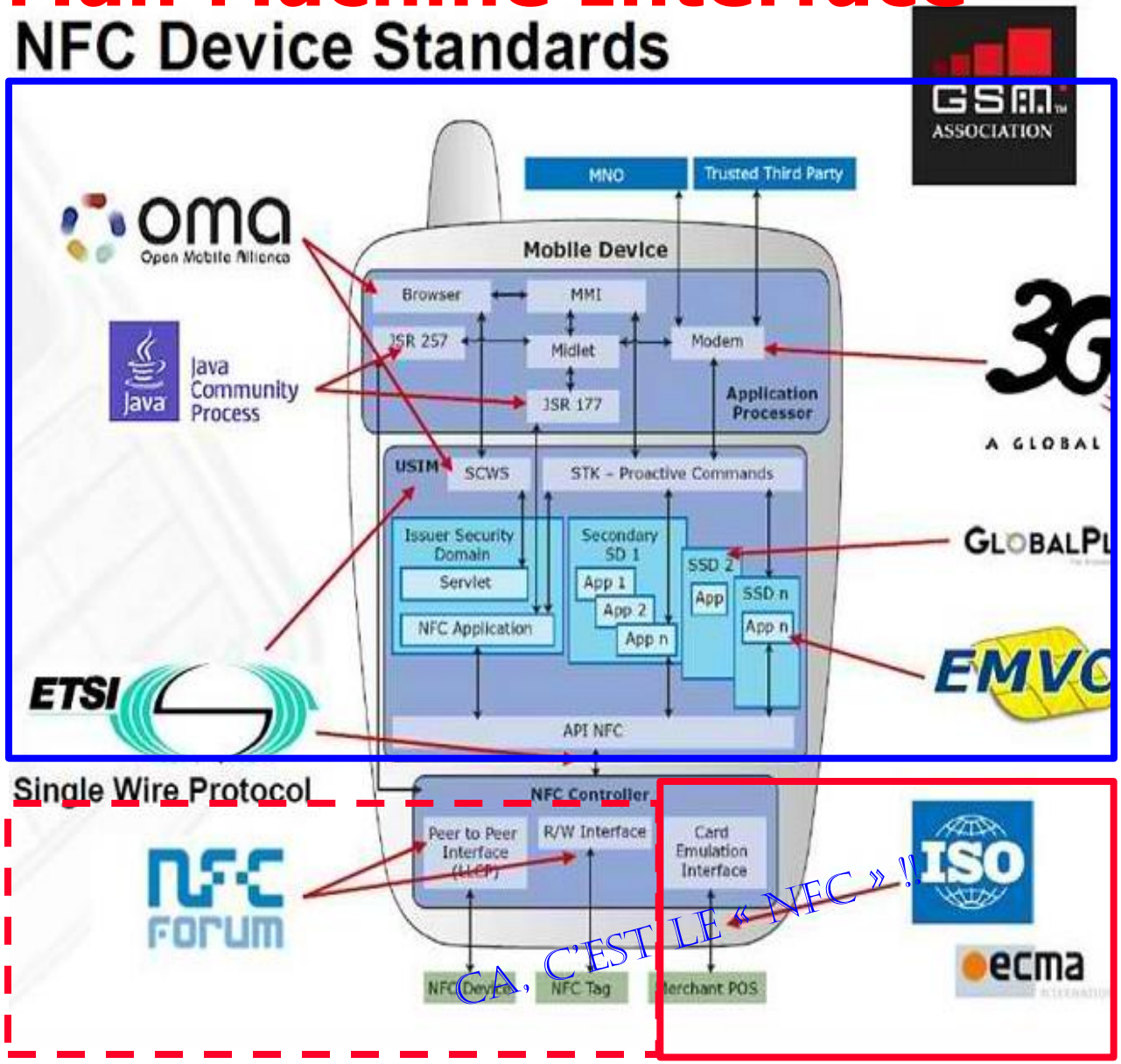
Quelques petits retours en arrière qui ont leur importance !

Juste pour être clair et afin de rafraichir la mémoire aux nouveaux venus, donc, once upon a time, depuis 1995 (vingt ans déjà)

… les papotages d'architectures pour téléphones mobiles ont débuté vers l'an de Grâce 2004 !!

"The Ultimate Man Machine Interface"

NFC Device Standards



SE solutions

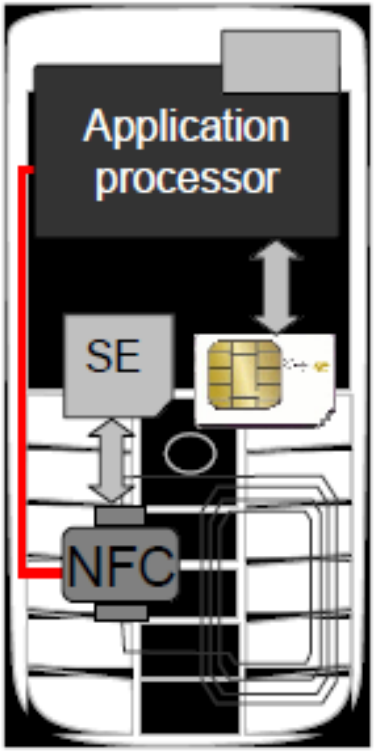
Various SE solutions have been introduced to the industry for enabling NFC based systems. The most preferred and used SE options for an NFC enabled mobile phone are:

- Embedded hardware in a mobile device as an integral, non-removable part of the device.

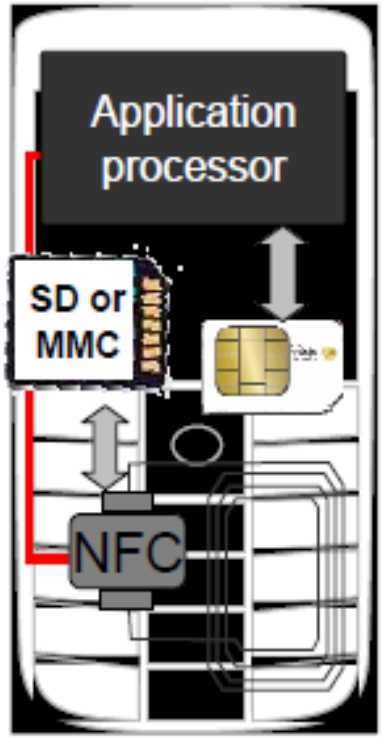
- Secure Memory Card (SMC) as a secure storage area in a removable smart card.

- UICC (… SIM) as a physical smart card and maybe the most popular one.

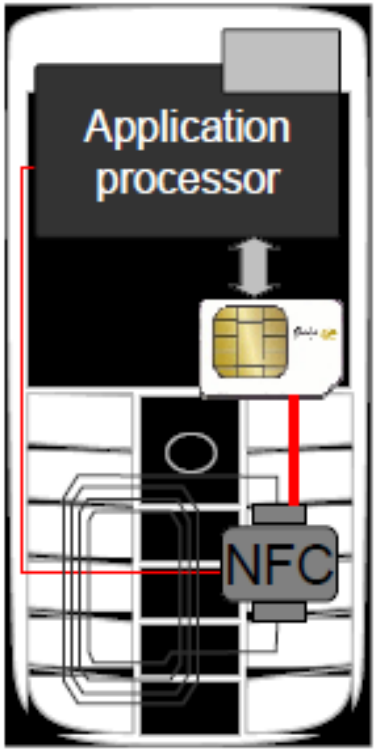
Secure element embedded in the phone



SD or MMC card hosting the application



SIM centric solution



… mais, dans le même temps …

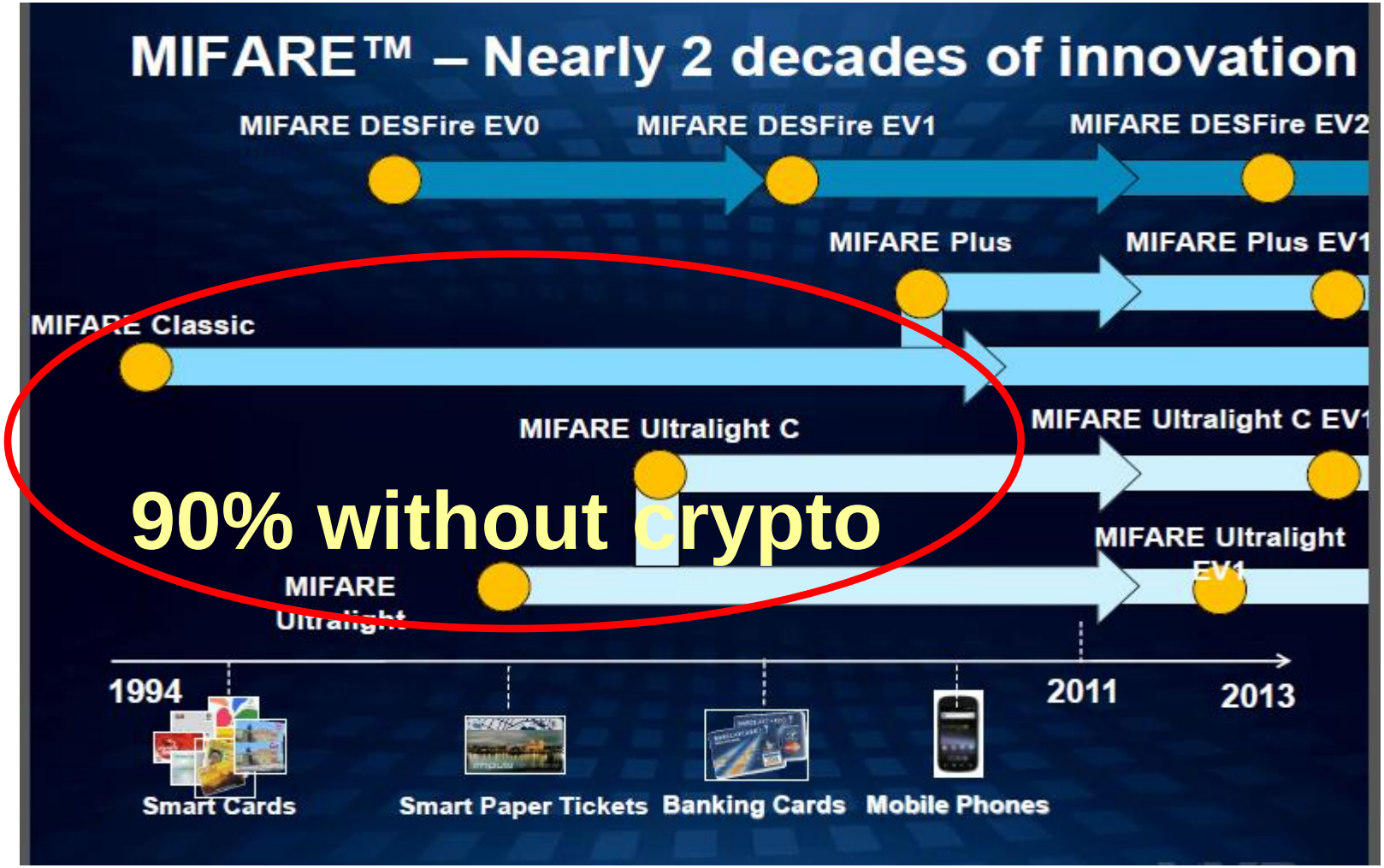
May 2013

90%
Contacless
Card
Without
Crypto !!

MIFARE™ is leading in many other applications

90% without crypto

Loyalty	Event Ticketing	NFC Tags	Micro Payment	Road Tolling	Student Cards
					
Increased customer engagement through convenience ► Cardholders earn points to get discounts and advantages ► Loyalty points are securely stored on the card for offline earning and spending	Contactless technology enhancing the experience ► Stadium access, micro payments, parking and membership services ► Seasonal cards and single tickets ► Anti counterfeiting and black listing	Convenience for NFC interconnections and smart information sharing ► Ideally suited to the broadest range of industries ► Interactions require no more than a simple touch	Speed and security for closed loop micro payments ► Fast cashless transactions ► Suitable e.g. for shops near subway stations, canteen payments or loyalty cards	Fast and reliable way to pay for the highway ► Cost efficient way to collect money for highway operators. ► Pre-paid and postpaid cards solutions possible. ► Convenience for drivers	Reliable multi-application solution ► Physical access to university and student home buildings ►Micro payment for student restaurants ►Logical access to PCs and services
Air Asia frequent flyer card (2Mpcs/year) German blood donor card (1,5Mpcs/year)	Season tickets of Manchester United, Real Madrid and Bayern Munich Tickets for the soccer world championship	Explosive growth with smart posters, store advertising and access to content download	Indonesian theme parks (1,5Mpcs/year) BeShiBa card HongKong (1 Mpcs/year) Vietin Bank (1 Mpcs/year)	KGS Road tolling Turkey (3Mpcs/year) Touch'n'Go Malaysia (2Mpcs/year)	European Campus Card Association using MIFARE (5Mpcs/year) Growing number of Chinese campus cards using MIFARE



May 2013

Contactless card not used for paiement but 70 % with proprietary crypto

Activities	Technologies							
	NFC – A *based on ISO 14 443 - A*				NFC- B *based on ISO 14 443 - B*	NFC – F *based on JIS X6319-4*		
Listen, RF Collision Avoidance, Technology Detection, Collision Resolution	*based on ISO 18 092 - NFC IP 1*				*based on ISO 21041 NFC IP 2*	*based on ISO 18 092 - NFC IP 1*		
Device Activation	**NFC**-DEP Protocol *based on ISO 18 092*	Technologies Subsets						**NFC**-DEP Protocol *based on ISO 18 092*
		Type 1 Tag Platform	Type 2 Tag Platform	Type 4A Tag Platform	Type 4B Tag Platform	Type 3 Tag Platform		
		Produits industriels et protocoles hérités						
		Topaz	*Mifare UL*	*ISO 14 443 - A*	*ISO 14 443 - B*	*FeliCa*		
Data Exchange		Protocoles de communication						
		Type 1, 2, and 3 Tag Half-duplex Protocol		**ISO**-DEP Protocol *based on ISO 14 443 (- 4) and EMV_CLESS*		Type 1, 2, and 3 Tag Half-duplex Protocol		
Device Deactivation								

conclusions

0 - … et il y en a encore beaucoup d'autres fabricants !!!

1 - ce sont des cartes sans contact simples (sans crypto)!

2 – elles sont réellement ISO 14 443 (au moins -2 -3)

3 – elles fonctionnent sur tous les lecteurs du marché

4 – comment les émuler simplement dans un NFC device spécifique tel qu'un Smartphone archi verrouillé par un operateur et le passage obligé par le SE de sa SIM pour des applications « juteuses »

5 – du fait de l'implémentation des couches du NFC Forum et Google Android 3.x comment ne plus être obligé de faire des acrobaties à dormir debout du style fausse communication P2P au lieu d'un truc archi simple !

Enfin on y arrive ...

… où comment, certains, il y a / depuis 8 ans,
ont mis la charrue avant les bœufs !

(sens figuré) Commencer par où l'on devrait finir, faire avant ce qui devrait être fait après, faire les choses dans le désordre

Ouf, enfin, … retour vers le futur !

HCE
Host-based Card Emulation

October 31st 2013, Google introduced its mobile Operating System, Android 4.4 KitKat including a new NFC - Near Field Communication feature: Host-based Card Emulation (HCE).

D'après le texte officiel ci dessous, sans autre commentaire
http://developer.android.com/guide/topics/connectivity/nfc/hce.html

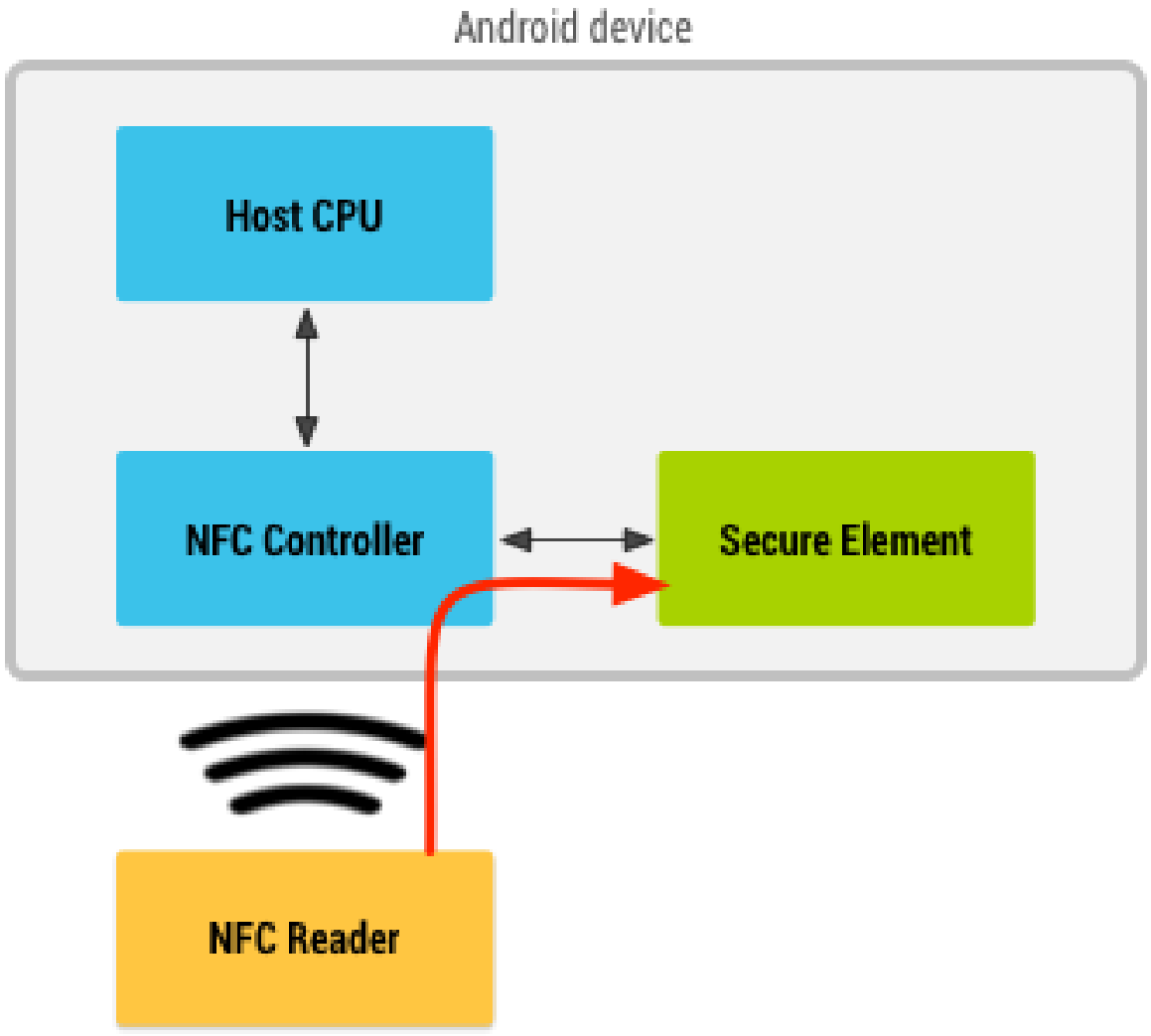
Host-based Card Emulation - HCE

Many Android-powered devices that offer "NFC" functionality already support NFC card emulation. In most cases, the card is emulated by a separate chip in the device, called a *secure element*. Many SIM cards provided by wireless carriers also contain a secure element.

Android 4.4 (KitKat) introduces an additional method of card emulation that does not involve a secure element, called *host-based card emulation*. This allows any Android application to emulate a card and talk directly to the NFC reader.

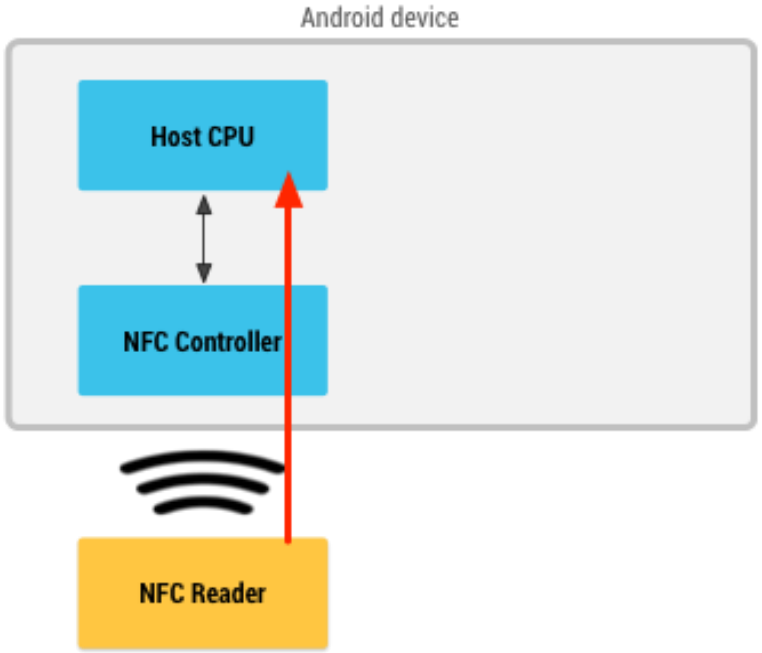
This document describes how host-based card emulation (HCE) works on Android and how you can develop an app that emulates an NFC card using this technique.

Card Emulation with a Secure Element



2- Host-based Card Emulation

When an NFC card is emulated using HCE host-based card emulation, the data is routed to the host CPU on which Android applications are running directly, instead of routing the NFC protocol frames to a secure element.



Specifically, Android 4.4 supports emulating cards that are based on the NFC-Forum ISO-DEP specification (based on ISO/IEC 14443-4) and process Application Protocol Data Units (APDUs) as defined in the ISO/IEC 7816-4 specification.

- *Android mandates emulating ISO-DEP only on top of the NFC-A (ISO 14443-3 Type A) technology*.
- *Support for NFC-B (ISO 14443-4 Type B) technology is optional*.

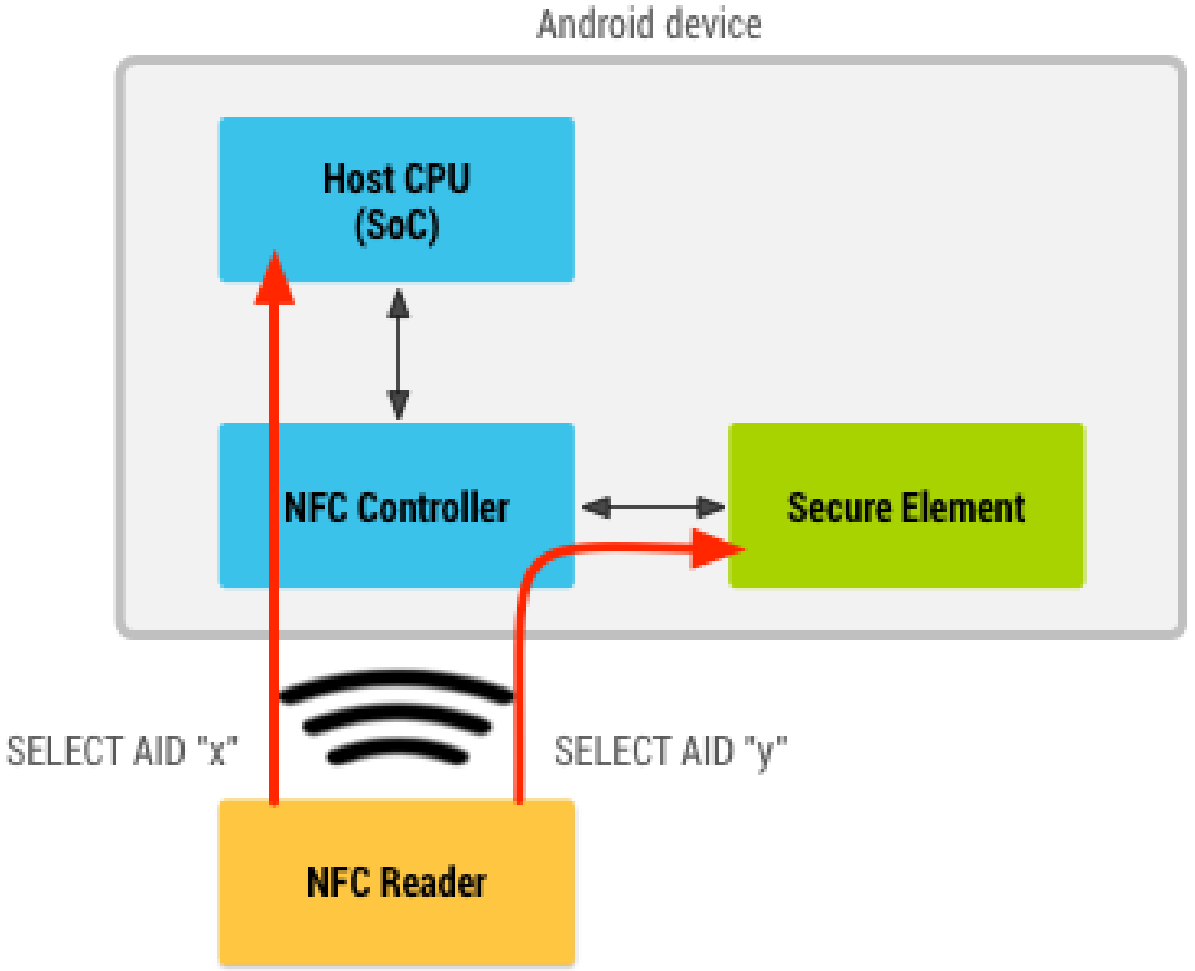
The layering of all these specifications is shown

Coexistence with Secure Element Cards

This section is of interest for developers that have deployed an application that relies on a secure element for card emulation. Android's HCE implementation is designed to work in parallel with other methods of implementing card emulation, including the use of secure elements.

Note: Android does not offer APIs for directly communicating with a secure element itself.

This coexistence is based on a principle called "AID routing": the NFC controller keeps a routing table that consists of a (finite) list of routing rules. Each routing rule contains an AID and a destination. The destination can either be the host CPU (where Android apps are running), or a connected secure element.



HCE and Security

The HCE architecture itself provides one core piece of security: because your service is protected by the BIND_NFC_SERVICE system permission, only the OS can bind to and communicate with your service.

This ensures that any APDU you receive is actually an APDU that was received by the OS from the NFC controller, and that any APDU you send back will only go to the OS, which in turn directly forwards the APDUs to the NFC controller.

Quelques points techniques qu'il ne faut néanmoins pas perdre de vue …

1- L'émulation de carte « dans l'hôte » (HCE) n'a aucune chance de fonctionner lors que le smartphone est éteint (volontairement éteint ou déchargé), alors que dans certaines architectures SIM-centric ou SE-centric il est parfois possible de réaliser une transaction smartphone éteint,

2- Le processeur principal du smartphone *(baseband)* n'est pas un processeur sécurisé. Les applications dont la sécurité est critique (c'est-à-dire lorsque le bénéfice de la fraude est très supérieur au coût de la fraude : paiement, transport public, contrôle d'accès de sites sensibles, documents d'identité...) ne doivent donc pas être implémentées dans ce mode,

3- Les performances (temps de transaction) risquent d'être moins bonnes et surtout moins constantes que dans une mise en œuvre classique au sein d'un processeur sécurisé – qui est par nature indépendant des autres applications s'exécutant sur le smartphone,

4- L'architecture technique repose sur ISO 14443 couche 4, type A, + ISO 7816-4 pour le formalisme des APDUs, et + ISO 7816-5 pour la sélection de l'application par le lecteur grâce à un AID unique. Toute application qui ne rentrerait pas dans ce cadre ne serait pas éligible au portage vers HCE. C'est notamment le cas de certaines mises en œuvre « transport public » françaises dont les lecteurs n'implémentent que l'ISO 14443 type B.

Exemple : NXP en 2014

NXP has updated its PN547 NFC controller's firmware and middleware to provide enhanced support for host card emulation (HCE) transactions.

"NFC to a secure element is ultimately a routing function between the point of sale and the secure element, and when HCE is introduced the dynamics of this routing function are changed,"

"NXP has worked with the main ecosystem players, including Google, to ensure the routing function is performed correctly through changes to our firmware and middleware."

Conclusions

Eviter les confusions !

- NFC … ce n'est que de la pure physique

- NFC IP1 & IP2 (ISO 18092 & 21481 … ce sont des protocoles de communication fonctionnant en NFC, à 13,56 MHz
(… et par la même occasion NFC Forum)

- Utilisations…ssss générales des protocoles NFC IP1 & IP2

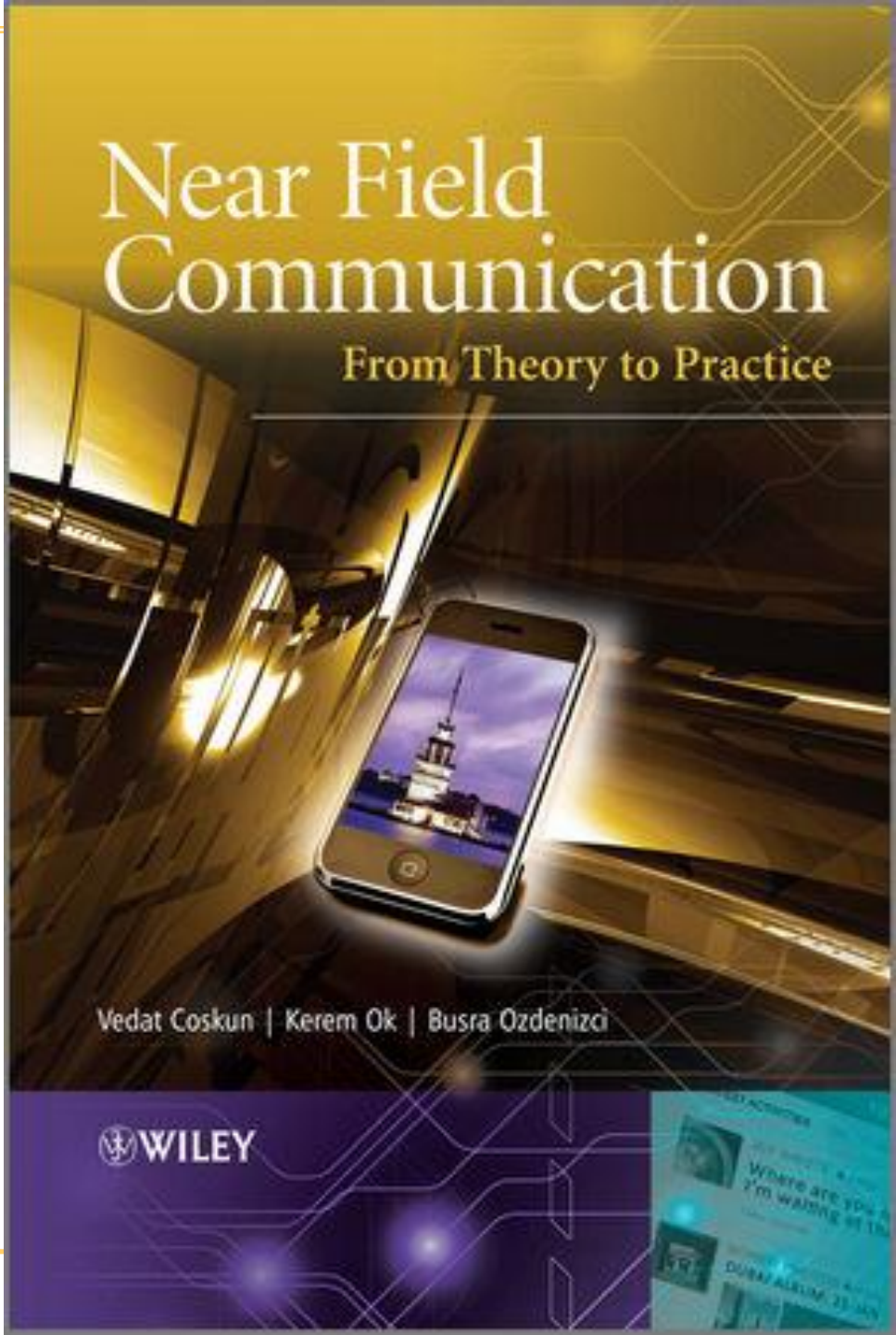
- *Ouvrage écrit par des **Industriels !***

Eviter les confusions !

- Utilisations…ssss spécifiques des protocoles NFC IP1 & IP2 en téléphonie mobile

- Utilisations des NFC IP1 & IP2 à des applications…ssss bancaires &/ou transports à l'aide de téléphones mobiles

- *Ouvrage écrit par des **Universitaires !***



… merci de votre écoute
et bonne et instructive journée !

Dominique PARET

dp-consulting@orange.fr

Dominique PARET

et

Consulting

Formations & Services

vous remercie de votre attention !

dp-consulting@orange.fr