UNIVERSITE PARIS-EST MARNE-LA-VALLEE

MASTER 2 SYSTEMES D'INFORMATION ET APPLICATIONS WEB

LA TECHNOLOGIE NFC

RAPPORT D'ETUDE

ALCIME MATTHIEU

GHARTOUCHENT MALEK

RACHED NIHAD

PROFESSEUR : SIMON ELRHARBI

MASTER 2 SIAW 2012-2013

Table des matières

LA TECHNOLOGIE NFC

DECOUVRONS L'UTILITE DES APPLICATIONS DE LA NFC

1. INTRODUCTION

1.1. CONTEXTE

Le mobile est de plus en plus présent dans notre environnement. Pour beaucoup d'entre nous, il nous réveille le matin, nous permet de savoir comment nous habiller après avoir étudié la météo, nous accompagne dans les transports, nous permet de rester en contact avec nos amis, réels et virtuels, nous donne l'impression de rester en contact avec le monde réel qu'il soit personnel ou professionnel en lisant les informations ou nos mails, nous permet de nous évader le temps d'un jeu, d'un film ou d'une playlist musicale, et beaucoup d'autres activités liées à chacun d'entre nous.

Demain, nous achèterons de plus en plus de services et de produits avec nos mobiles et nous continuerons d'interagir avec nos amis, proches, collègues et puis avec notre environnement, la maison, la voiture ou la ville. Tout cela porte le nom générique d'Internet des objets.

Se faisant, nous laissons des traces sur l'Internet, plus ou moins volontairement. Ce dernier terme est important. Plus ou moins volontairement. En Ile-de-France, le passage à un valideur des transports en commun est enregistré (sauf dans le cas d'une carte Navigo Découverte) ainsi que le passage au péage sur l'autoroute ou à l'Eurotunnel. Nous laissons des informations sur Facebook, LinkedIn ou sur Foursquare. La simple utilisation de GMail, gratuit pour l'utilisateur, se fait en échange de l'autorisation implicite que nous donnons à Google d'utiliser les informations contenues dans nos mails. Les commentaires sur les blogs, sur Amazon, sur TripAdvisor, sur Twitter, les photos sur Flicker ou Instagram, toutes ces données sont réutilisées. Google et Apple ont même été récemment pris la main dans le pot de miel en enregistrant des données de géolocalisation à l'insu des utilisateurs, pour évidemment de bonnes raisons. Google toujours qui à travers sa stratégie produit et service, cherche à reproduire dans le monde réel, le modèle efficace appliqué au monde virtuel. Un dernier exemple, Paypal et d'autres sociétés souhaitent suivre le consommateur entrant dans un magasin à l'aide d'une géolocalisation indoor, capable de connaitre la position du consommateur à un mètre près dans le magasin, pour pouvoir lui proposer des services.

Nous partageons donc bien plus d'informations que nous le pensons, de nouveau, plus ou moins volontairement, et tout cela va enrichir des bases de données sous le terme générique de big data (qui n'est pas sans rappeler la notion de big brother). Ces informations vont faire le bonheur économique de nombreuses sociétés, les premières étant Google, Apple ou Amazon. Cet Internet des Objets est un surtout Internet des données (données générées par l'interaction avec les objets et leur représentation numérique), à la fois dans le sens anglais « data » – données numériques que « given » – donné (du verbe donner) ; nous donnons nos données qui sont récupérées et exploitées par d'autres.

C'est ici qu'intervient la NFC.

La technologie NFC, est née grâce au couplage de la technologie RFID (Radio Field Identification : Technologie d'identification par radiofréquence) avec les cartes à puces. RFID est un système d'identification sans contact utilisé depuis longtemps dans un but de traçabilité. La technologie NFC opère lorsque la portée communication n'excède pas une dizaine de centimètres et permet aux terminaux communicants d'échanger des données des formats plus évolués (cartes de visite, les contacts téléphoniques, etc.), contrairement à la technologie RFID. Cette courte portée nécessite un acte conscient de la part de l'utilisateur pour établir une communication contrairement à des technologies comme Bluetooth par exemple.

Le choix de la technologie NFC sur les téléphones portables est guidé par plusieurs motivations liées à l'usage grand public du téléphone portable à l'heure actuelle et par divers types d'applications NFC envisageables dans le domaine de la santé.

En effet, depuis quelques années l'informatique a changé. L'intégration de plusieurs technologies (Réseaux 3G, 3G+ et 4G, services de géolocalisation (GPS), NFC, etc.) dans le téléphone portable l'a transformé en un outil multiservice incontournable dans notre vie quotidienne.

Actuellement, la technologie NFC connait un intérêt grandissant de la part des industriels en particulier ceux du domaine de la téléphonie qui l'ont intégrée dans de nombreux Smartphone grand public. Les applications sont nombreuses allant du paiement électronique à l'horodatage en passant par de la localisation.

1.2. FONCTIONNEMENT

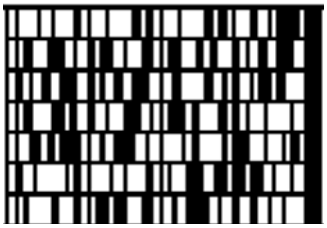
Les technologies de marquage et de traçabilité ont connu ces dernières années une évolution considérable rendue possible par la conjonction de la dématérialisation des processus de suivi, de la baisse des coûts des supports et des capacités de traitement de l'information.

Ces technologies sont nées des besoins industriels visant à doter chaque élément (objets ou groupes d'objets physiques sous forme de stock ou de flux, les objets numériques, les entités vivantes, animales et humaines) d'un identifiant unique pouvant le distinguer des autres.

Les étiquettes à codes et code-barres (imprimés linéaires, linéaires empilés, etc.) (cf. Figure II.1 a, b et c) font partie des plus anciennes de ces technologies

A) code EAN-13(linéaire)

B) code DataMatrix



C) code 49(linéaire empilé)

Figure II. 1 Les technologies d'identification de codes à barres

*EAN : European Article Numbering.

Suite aux limites que présentent ces étiquettes (nécessité d'une visibilité directe de moins d' 1 mètre, capacité de mémorisation limitée, sont non modifiables, etc.), elles sont inadaptées dans un nombre croissant de cas où le besoin de traçabilité ou d'identification se fait sentir(les grandes entreprises manufacturières, les industries agroalimentaires, etc.).Pour pallier à ces limites, d'autres technologies d'identification dont fait partie la technologie RFID ont été développées.

NFC est une application de la technologie RFID (Technologie d'identification par radiofréquence). Cette technologie comprend trois grandes familles qui se distinguent principalement (mais pas uniquement) leur fréquences de fonctionnement et par la distance de lecture entre le lecteur et l'étiquette. LF pour Low Frequency, HF pour High Frequency, et UHF pour Ultra High Frequency.

La technologie RFID (Radio Frequency Identification), ou identification par fréquence radio (on parle aussi parfois de smart tags (étiquettes intelligentes)), est née du besoin de traçabilité[1]. Elle combine le principe des codes-barres et celui de l'indentification par cartes à puce sans contact.

Au code-barres elle reprend, en le modernisant, le principe de doter tout objet d'un code d'identification unique UID (Unique ID) qui peut être lu par une machine. A la carte à puce sans contact, elle reprend la possibilité de lire des informations, voire de faire effectuer un traitement, à distance. Ainsi, cette technologie permet par exemple d'identifier un objet en mouvement et dans une position quelconque.

ARCHITECTURE D'UNE INFRASTRUCTURE RFID

Une infrastructure [1] complète de RFID comprend les étiquettes ou tags, appelées aussi les transpondeurs, les lecteurs ou encodeurs et l'intergiciel (middleware) comme le montre la figure II.2 ci-après.

[1] La traçabilité est définie par l'ISO 8402 comme étant "l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'un article ou d'une activité, ou d'articles ou d'activités semblables au moyen d'une identification enregistrée".

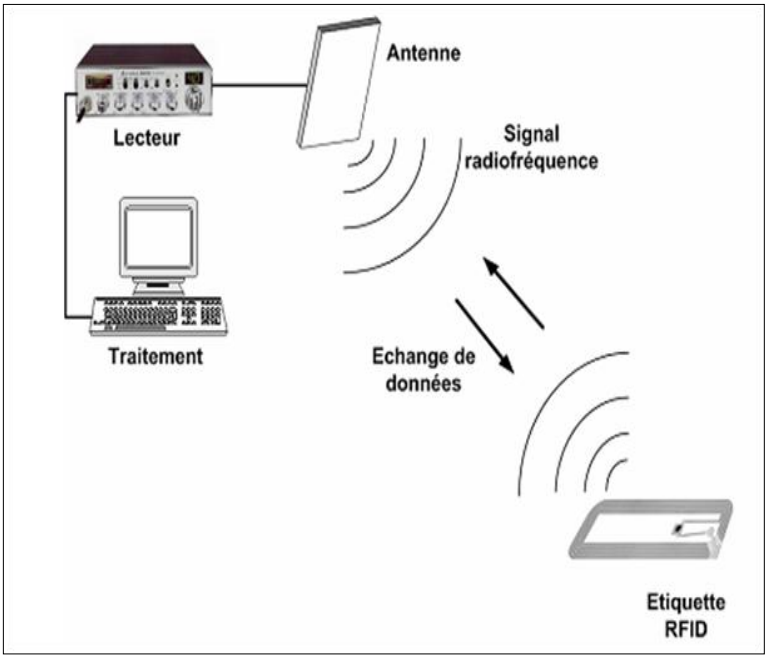


Figure II. 2 Infrastructure RFID

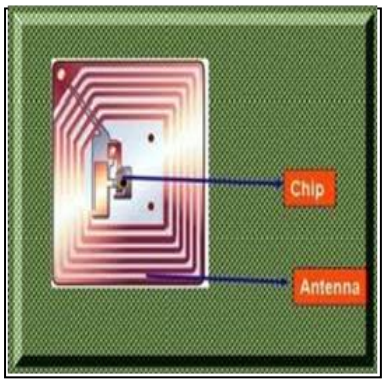


Figure II. 3 Etiquette RFID

L'intergiciel permet d'intégrer le flux des données dans le système d'information(SI) de l'entreprise.

Un Tag RFID (voir figure II.3) comprend une antenne associée à une puce électronique qui lui permet de recevoir et de répondre aux requêtes radio émises depuis le lecteur.

L'échange d'information entre le lecteur et le tag s'effectue par des techniques de lecture électromagnétiques (radiofréquence) et non par lecture optique, comme c'est le cas pour le code à barres par exemple.

TYPES DE TAG RFID

Un tag RFID peut être actif ou passif.

Un tag RFID est ''actif'' lorsqu'il est équipé d'une source d'énergie (interne ou externe) pour alimenter complètement ou partiellement son circuit ou son antenne. Cette énergie lui permet de pouvoir rester en activité pour lire ou envoyer des données. Un tag actif est plus complexe est plus cher. Sa durée de vie est en général conditionnée par celle de sa source d'énergie.

Contrairement à un tag actif, un tag passif ne contient pas sa propre source; l'énergie est fournie par le lecteur au moment de la lecture selon le principe suivant : Lorsque des ondes radio provenant du lecteur rencontrent un tag passif, il se forme un champ magnétique autour de l'antenne du tag (principe d'induction magnétique).

Le tag est ainsi alimenté par ce champ et peut coder et envoyer les données qu'il contient dans sa mémoire au lecteur. Les tags passifs sont moins complexes et moins chers que les tags actifs. Ils ont en général une longue durée de vie.

Les tags RFID peuvent également se classer selon les bandes de fréquences dans lesquelles elles fonctionnent : basse, haute ou très haute. Le débit d'information entre le lecteur et le tag est plus important en fréquence élevée qu'en fréquence basse.

Bande	*LF*	*HF*	*UHF*	*UHF (haute) et SHF*
Fréquence	125KHz à 133kHz	3.25MHz, 8.2MHz et 13,56MHz	440MHz, 860 à 960MHz	2.45MHz et 5.8GHz
Distance d'utilisation maximale	2 à 3m	1 à 5m	<12 m USA <6m Europe	<2.30m USA <0.81m Europe
Limites de fonctionnement	Peu sensibles aux perturbations électromagnétiques industrielles	Faiblement sensible aux perturbations électromagnétiques	Sensible aux perturbations électromagnétiques. Peut être perturbé par les autres systèmes UHF à proximité	Fortement sensible aux perturbations électromagnétiques réfléchies par le métal et absorbées par l'eau

Tableau II. 1 Les principales fréquences utilisées en RFID

TROIS MODES DE FONCTIONNEMENT DU NFC

Le mode émulation de carte

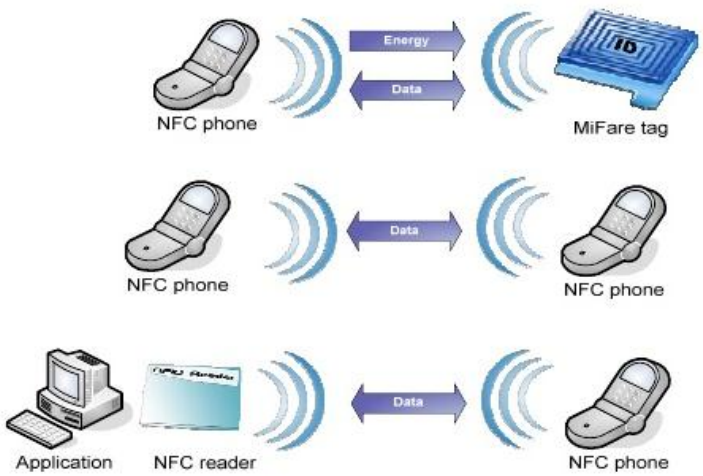
Dans le mode émulation de carte, dit passif, le terminal mobile se comporte comme une carte à puce sans-contact. Dans le cas où le terminal mobile est un téléphone mobile compatible, la carte SIM de l'opérateur *peut* être utilisée comme élément de sécurité en stockant des informations cryptées. Les usages sont multiples: paiement, billettique spectacle ou transport (ex. : Navigo), couponing, contrôle d'accès... Le mobile, par ses fonctionnalités étendues (IHM, connexion réseau, capacité de traitement), enrichit considérablement les services basés sur des cartes.

Le mode lecteur

Le terminal mobile devient un lecteur de cartes sans-contact (mode actif) ou de « radio-étiquettes » (étiquettes électroniques). Ce mode permet de lire des informations en approchant son mobile devant des étiquettes électroniques disposées dans la rue, sur des abris bus, des monuments, des affiches... ou sur des colis, des produits ou sur sa carte de visite (vCard)...

Le mode pair-à-pair

Ce mode permet à deux terminaux mobiles d'échanger de l'information, par exemple des vCard, des photos, des vidéos, de l'argent, des tickets, etc. Un appareil doté de la technologie NFC est capable d'échanger des informations avec des cartes à puces sans contact mais également avec d'autres appareils dotés de cette technologie.



1.3. NORMES

En plus des téléphones portables, la technologie NFC est présente dans divers dispositifs tels que les cartes à puce, les lecteurs de cartes, etc. Pour obtenir l'adoption des consommateurs de cette technologie, les acteurs concernés(les fabricants, les opérateurs, les développeurs, etc.) doivent travailler en étroite collaboration et les applications doivent être interopérables. Cela nécessite donc une accréditation à partir des organismes de normalisation qui ont la responsabilité principale d'assurer l'interopérabilité des différents dispositifs NFC.

Les principales normes NFC sont éditées par les organismes suivants:

- ISO/IEC (International Organization for Standardization / International Electro-technical Commission);
- ECMA (European association for standardizing information and communication systems) [2];
- ETSI (European Telecommunications Standards Institute).

La figure suivante illustre l'organisation des normes issues de ces organismes pour la technologie NFC.

[2] Avant 1994, ECMA était connu sous le nom de « European Computer Manufacturers Association.

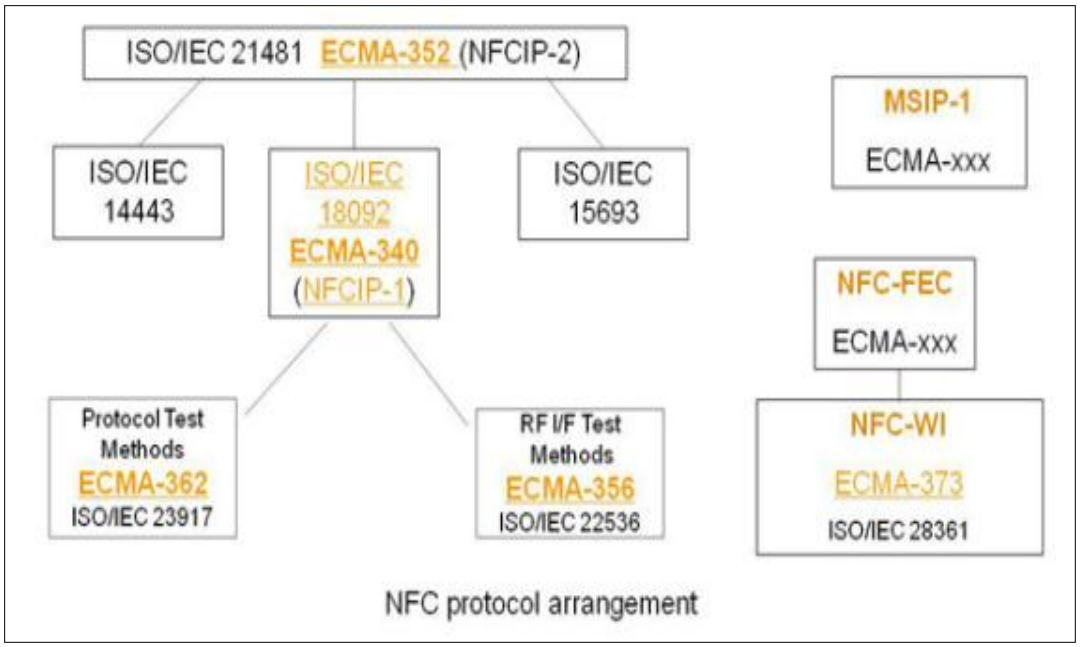


Figure II. 2 Les principales normes de la technologie NFC.

En plus de ces organismes, un consortium international connu sous le nom de « NFC Forum » a été créé en 2004 à l'initiative de Sony et Phillips, avec pour objectif principal de promouvoir l'utilisation de la technologie NFC.

Dans le reste de cette section, nous donnerons une vision d'ensemble de ces différentes normes. Un accent particulier sera mis sur certaines spécifications de NFC Forum que nous avons utilisées pour formaliser les échanges de paquets dans notre protocole.

LA NORME ISO 14443

La technologie NFC est une extension de la norme ISO/IEC 14443[2] qui normalise les cartes de proximité (Identification cards - Contactless integrated circuit cards - Proximity cards) utilisant le RFID. Cette extension est formée par un ensemble de normes dont les principales se trouvent sur le schéma de la figure II.4 vue précédemment.

La norme ISO 14443 est divisée en quatre parties :

ISO 14443-1 : spécifie les caractéristiques physiques de la carte

ISO 14443-2 : décrit le Signal radio fréquence(RF) et les signaux électriques

ISO 14443-3 : définit les phases d'initialisation des échanges et de gestion de collision

ISO 14443-4 : définit le protocole de transmission

Pendant la normalisation, deux acteurs industriels majeurs (Philips et Texas Instrument) n'ont pas pu s'entendre sur la façon dont la modulation radiofréquence(en ISO 14443-2) devait se faire. Ils ont opté ainsi pour deux types de dispositifs, nommés Type A (NFC-A) pour Philips et type B(NFC-B) pour Texas Instruments, où chaque carte à puce en général ne supporte qu'un seul de ces types.

Les terminaux utilisés dans cette norme sont de deux types : les lecteurs, appelés aussi les terminaux de couplage de proximité (Proximity Coupling Device:PCD), et les transpondeurs, appelés aussi «Proximity Integrated Circuit Card : PICC ». Un PCD doit être en mesure de supporter les deux types.

LA NORME ISO / IEC 18092 : NFC INTERFACE AND PROTOCOL-1(NFCIP-1)

ISO/IEC 18092[3] a été préparée par ECMA-340 [4] et a été adoptée par le comité technique mixte « ISO/IEC- JTC 1 Information Technology Standards », en parallèle avec son approbation par les organismes nationaux de l'ISO et la IEC. Cette norme spécifie l'interface et le protocole de communication sans fil simple entre deux dispositifs NFC communicants à un taux de transfert de 106, 212 et 424 kbps.

La pile protocolaire NFCIP-1 est basée sur la norme ISO/IEC 14443. La différence principale est un nouveau protocole de commande qui remplace la partie supérieure de la pile ISO/IEC 14443.

Pour chaque session de communication NFC, le NFCIP-1 distingue deux types de dispositifs : l'initiateur (initiator) et la cible (target). Comme leurs noms l'indiquent, le premier initie la communication et envoie les requêtes tandis que le second répond à ces requêtes. Ce mode est similaire à un mode de communication client/serveur.

La norme définit deux modes de communication : mode actif et mode passif. En effet, l'initiateur est toujours un dispositif actif[3].La cible quant à elle peut être un dispositif actif ou passif. Lorsque la cible est un dispositif actif, ce mode de communication est dit « mode actif ».Dans le cas contraire, le mode de communication est dit « passif ».

LA NORME ECMA-352 : NFC INTERFACE AND PROTOCOL-2 (NFCIP-2)

Bien que les normes ISO 14443, ECMA-340 et ISO/IEC 15693[4] opèrent à la même fréquence, elles spécifient chacune son propre mode de communication. La norme ECMA-352 [5] spécifie le mécanisme de détection et de sélection d'un de ces modes de communication afin d'éviter toute perturbation à l'origine d'un dispositif opérant à la fréquence 13.6MHz.

[3] La signification du tag actif et passif est la même que celle donnée en RFID.
[4] ISO/IEC 15693 définit les cartes de voisinages (Vicinity Cards) pour une portée maximale qui varie entre 1 et 1.5m.

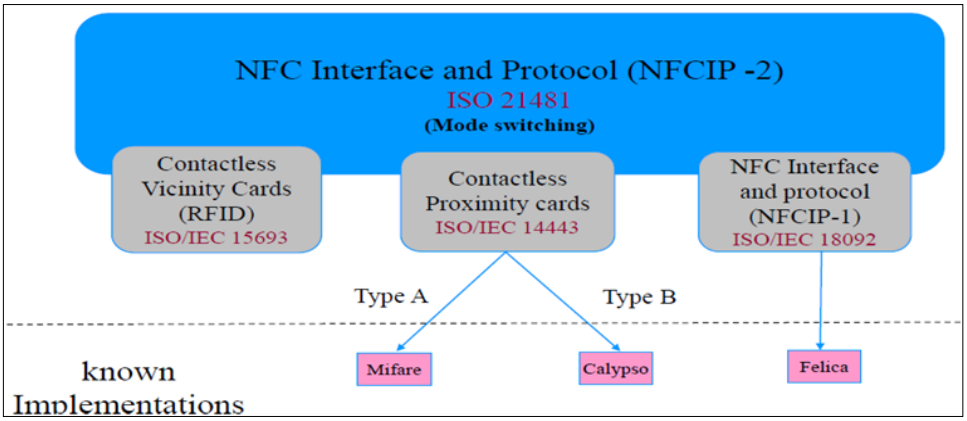


Figure II. 3 NFCIP-2

LES SPECIFICATIONS NFC FORUM

Le NFC Forum [6] est un consortium international crée en 2004 à l'initiative de Sony et de Philips (aujourd'hui NXP Semiconductors) avec pour mission de promouvoir la technologie NFC en élaborant des spécifications, en assurant l'interopérabilité entre les dispositifs (électronique grand public, les appareils mobiles et les PCs) et services, et de sensibiliser le marché sur la technologie.

Cet organisme, rejoint aujourd'hui par la plupart des acteurs du domaine (industriels, développeurs d'applications, prestataires de services, opérateurs), compte actuellement plus de 160 membres. Ces membres travaillent sur l'élaboration de spécifications(le Forum a publié à ce jour 16 spécifications) pour une architecture NFC modulaire, pour des protocoles d'échange de données interopérables et indépendants des dispositifs des différents constructeurs. Ces spécifications se basent sur les normes ISO et ECMA vues précédemment comme le montre la figure II.6

En Juin 2006, le NFC Forum a officiellement présenté l'architecture de la technologie NFC composée d'un ensemble de spécifications [7] comme le montre la figure II.8.Les explications concernant chacune de ces spécification sera donné après cette figure.

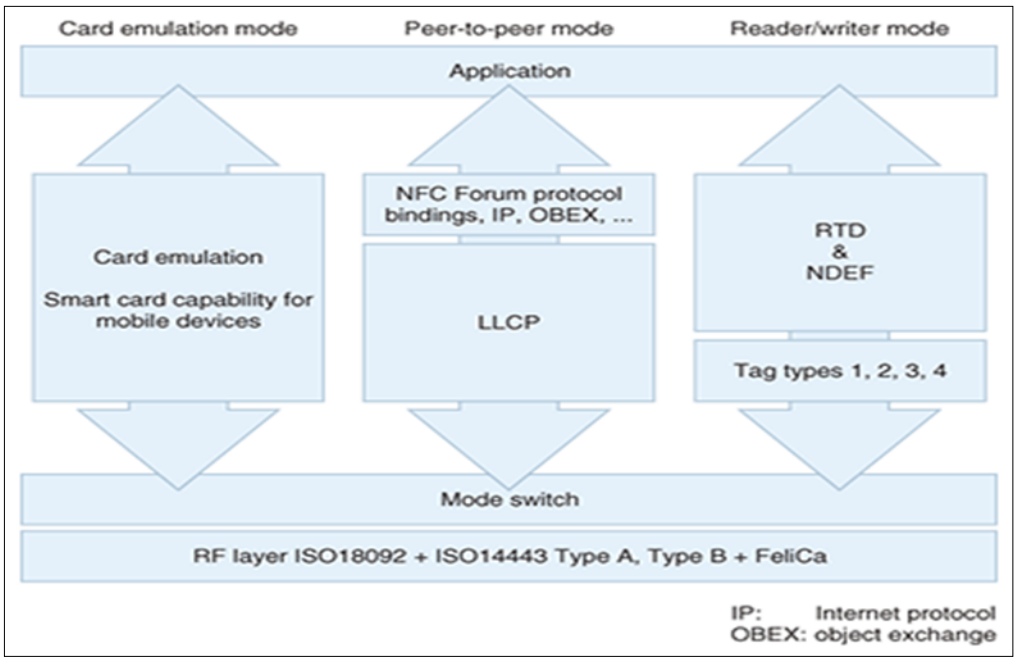


Figure II. 4 Architecture des standards NFC Forum

2. CAS SIM CENTRIC

La carte SIM a énormément évolué ces dernières années. Certes, elle répond toujours à sa fonction première d'identification de l'abonné sur le réseau (et donc de facturation), mais elle s'est enrichie de nombreuses autres fonctionnalités, engendrant une augmentation significative de sa capacité de stockage, qui double quasiment chaque année.

La SIM du téléphone a un rôle très important dans l'architecture d'un système basé sur la technologie NFC puisque l'élément de sécurité NFC peut être déployé sur les cartes SIM pour l'utilisation par les opérateurs du monde entier. Et cette technique est utilisé dans le mode de fonctionnement « émulation de carte ».

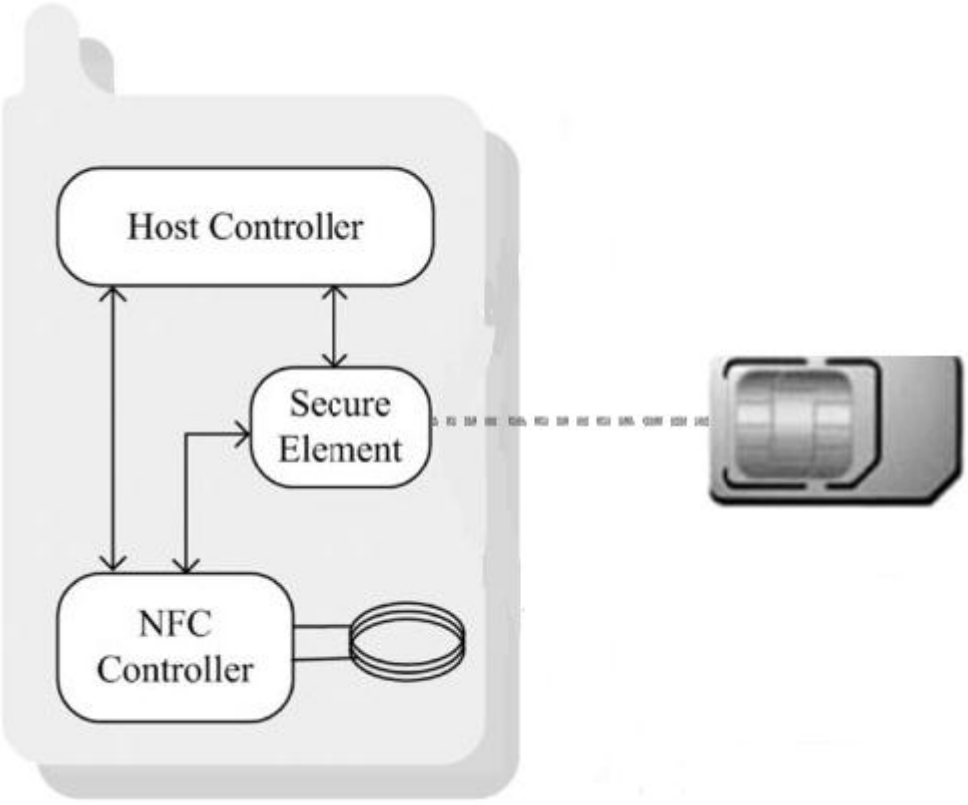
2.1. DEFINITIONS

NFC permet l'utilisation d'un téléphone mobile pour effectuer des transactions de paiement sans contact. Pour cela, le téléphone mobile doit contenir des éléments spécifiques:

- Contrôleur NFC pour l'administration de l'élément de sécurité : lire et écrire sur des étiquettes et des cartes, communiquer avec des téléphones (pour le traitement des paiements), et agir comme un tag NFC.

- Antenne NFC : La technologie NFC nécessite la présence d'une antenne dans le mobile. Car cette antenne est spécialement conçue pour répondre sans contrainte à toute demande d'intégration et quel que soit l'environnement et gérer les communications entre l'appareil et les dispositifs externes ou des systèmes qui suivent la norme ISO 14443. Elle peut être intégrée n'importe où dans le mobile (sur l'écran, sur la batterie, sur la carte électronique, etc.) quels que soient le facteur de forme ou le silicium NFC utilisé toujours en garantissant de très bonnes performances radio en conformité avec la norme ISO14443.

- L'élément de sécurité : Dans le cas de SIM CENTRIC l'élément de sécurité est dans la carte SIM.

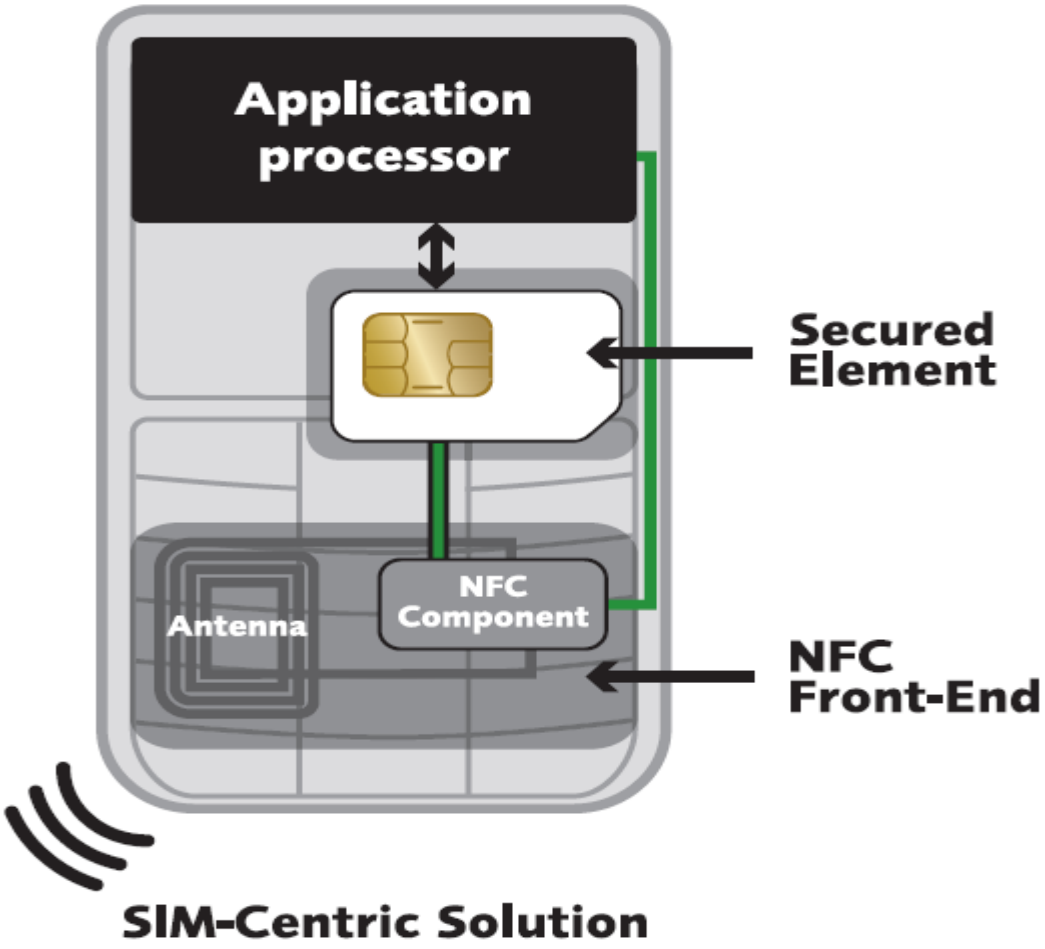


Les services (applications et données dédiées à l'application d'interface de l'utilisateur) sont stockés et hébergés dans un élément de sécurité (La carte Sim dans ce cas) qui est le cœur de la technologie NFC et qui est connecté au contrôleur NFC pour effectuer des transactions sécurisées à proximité des périphériques NFC externes. L'élément de sécurité offre un

environnement dynamique et sécurisé pour les programmes et les données. Il permet aussi un stockage sécurisé des données privées tel que l'utilisation des informations de carte de crédit.

Le contrôleur hôte est le cœur de n'importe quel téléphone mobile. L'interface 261/921 de la norme ISO / CEI 7816 prend en charge la liaison de L'élément de sécurité au contrôleur hôte. L'interface de contrôleur hôte crée un pont entre Le contrôleur hôte et le contrôleur NFC, définit le mode de fonctionnement de ce dernier, traite les données envoyées et reçues et établit une connexion entre le contrôleur NFC et l'élément de sécurité.
En outre, il maintient l'interface de communication, les périphériques, et l'interface d'utilisateur.

L'ARCHITECTURE SIM CENTRIC



La puce NFC n'est pas sur la carte SIM, mais les applications NFC sont sur la carte, comme l'application qui permet par exemple de valider des titres de transport. Le fait de placer les applications sur la carte SIM

permet d'assurer une qualité de service importante pour l'utilisateur final. S'il perd le téléphone et la carte SIM par exemple, il est possible pour l'opérateur de désactiver le tout à distance, ce qui réduit les risques.

2.2. AVANTAGES ET INCONVENIENTS

La SIM CENTRIC fournit à la fois une sécurité logique (le cryptage) et une sécurité physique (l'anti-falsification et la protection contre les copies). Elle a d'ailleurs été définie par les opérateurs mobiles comme étant l'élément de sécurité dans un système NFC, grâce aux avantages unique qu'elle offre sur le marché :

- **Universalité :** La carte SIM a un grand taux de déploiement, avec plus de trois milliards d'utilisateurs à travers le monde.

- **Portabilité :** Elle est portable, les utilisateurs peuvent donc facilement transférer leurs applications d'un téléphone NFC à un autre.

- **Gestion dynamique à distance :** Les opérateurs mobiles peuvent déjà gérer les cartes SIM à distance, ils pourront sans aucun problème le faire pour les services NFC. Ainsi, Les services chargés dans la carte peuvent immédiatement être bloqués, activés ou suspendus à distance par l'opérateur en cas de perte ou de vol.

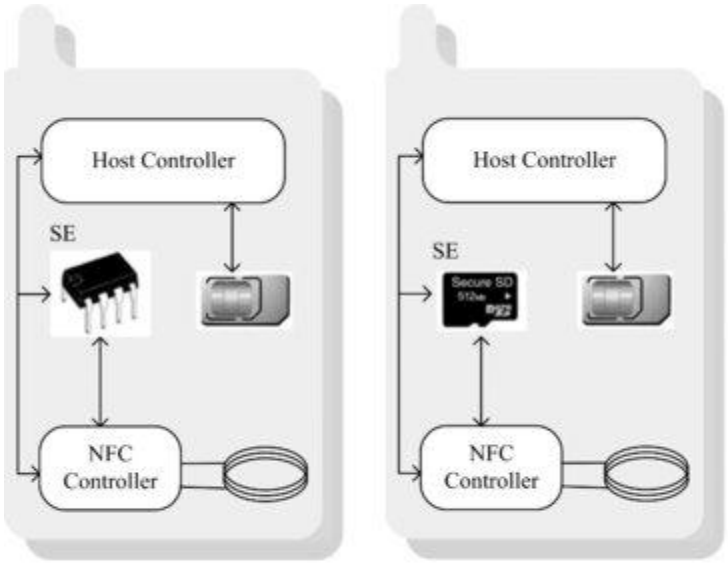
- **Standardisation :** La sécurité de la carte SIM est basée sur des standards globaux déjà bien établis couvrant le stockage des applications, les communications, la protection de la vie privée et la gestion du cycle de vie.

- **Long cycle de vie :** La carte SIM a un plus long cycle de vie qu'un téléphone, elle est donc appropriée pour héberger les applications NFC qu'un appareil mobile.

Toutefois, cette solution présente l'inconvénient de « lier » les applications à l'opérateur mobile. Le passage d'un opérateur mobile à un autre nécessitera le rechargement des applications. De même, pour un voyageur se déplaçant dans plusieurs pays et changeant par conséquent fréquemment de réseau mobile, il semble plus approprié que les applications soient hébergées sur le téléphone plutôt que sur la carte SIM.

3. CAS SIM NON-CENTRIC

3.1. DEFINITION



NFC Mobile with Embedded Hardware

NFC Mobile with SMC

Au niveau matériel l'élément de sécurité (*Secure Element, SE*) peut être implémenté sous la forme d'une puce embarqué (*embedded SE, eSE*) ou un support amovible sécurisé de type carte mémoire (*Secure Memory Card, SMC*).

Les SE basées sur des puces embarquées sont des puces soudées au téléphone mobile de manière définitive. Ainsi, le niveau de sécurité fourni par le SE est important car supporté par la puce. Cette puce est intégrée au téléphone mobile durant la phase de production et doivent être personnalisées après que l'appareil ait été délivré à l'utilisateur final.

Soudé au téléphone, la puce SE ne peut évidemment pas être transférée d'un mobile à un autre. Elle doit être adaptée à chaque nouvel utilisateur. Bien que conforme avec les différents standards des smart cards, la communication avec le téléphone n'est pas encore standardisée.

Une carte SMC amovible est constituée de mémoire et d'un circuit intégré, en d'autres termes c'est la combinaison d'une carte mémoire ainsi que d'une carte à puce. La SMC offre ainsi un niveau de sécurité aussi élevé que celui des cartes à puces et est en conforme avec la plupart des standards, interfaces et environnements (comme EMV, GlobalPlatform, ISO/IEC 7816, JavaCard).

3.2. AVANTAGES ET INCONVENIENTS

Du fait qu'elle soit amovible et qu'elle offre une grande capacité de mémoire, l'architecture basée sur la SMC en tant qu'élément de sécurité peut donc accueillir un grand nombre d'applications et n'a pas besoin d'être réadapter quand le client acquière un nouveau téléphone car la SMC peut être facilement insérée dans le nouveau dispositif.

Mais à cause de cette même raison, on peut imaginer que quelqu'un puisse par la suite d'un vol utiliser le support à de mauvaises fins. Contrairement à une architecture SIM-Centric l'opérateur ne peut pas désactiver directement le dispositif.

4. GLOBALPLATFORM

4.1. DEFINITION

GlobalPlatform est un consortium créé en 1999 par les grandes entreprises des secteurs du paiement, des télécommunications, et gouvernemental; et fut le premier à promouvoir une infrastructure globale pour l'implémentation des cartes à puce commune à tous les secteurs industriels.

Les spécifications GlobalPlatform (anciennement Visa Open Platform) visent à gérer les cartes de façon indépendante du matériel, des vendeurs et des applications. Elles répondent efficacement aux problématiques de la gestion du multi-applicatif : chargement sécurisé des applications, gestion du contenu, cycle de vie. Les spécifications GlobalPlatform sont divisées en trois thèmes : cartes, terminaux et systèmes.

4.2. LES MECANISMES DE SECURITE

Les mécanismes de sécurité qu'offre GlobalPlatform spécifient des méthodes pour :

- sécuriser les communications ;
- s'assurer que les applications chargées sont officiellement signées
- authentifier le porteur.

LA SECURITE DES COMMUNICATIONS

Pour sécuriser les échanges entre la carte et une entité extérieure, GlobalPlatform spécifie deux mécanismes : l'authentification mutuelle, le canal sécurisé.

L'authentification mutuelle est la phase d'initiation d'un canal sécurisé pendant laquelle la carte et l'entité extérieure se donnent réciproquement l'assurance qu'elles communiquent avec une entité authentifiée i.e. qu'elles partagent le même secret.

Quatre algorithmes et protocoles sont supportés : Secure Channel Protocol (SCP) 01 (déprécié) et 02 basés sur DES, SCP 03 basé sur AES et SCP 10 basé sur RSA.

Après que l'authentification mutuelle ait réussie, le canal sécurisé est initié.

Durant la phase d'authentification mutuelle, le niveau de sécurité à appliquer à tous les messages suivant a été négocié. GlobalPlatform propose trois niveaux de sécurité :

- le niveau *authentification* correspond à un canal dans lequel les entités se sont authentifiées selon le mécanisme décrit précédemment ;
- le niveau *authentification et intégrité* assure que les messages reçus par une entité proviennent bien de l'autre entité, et que ni l'ordre des messages, ni leur contenu n'aient été altérés ;
- le niveau *authentification, intégrité et confidentialité* assure que les messages transmis entre les deux entités authentifiées ne sont pas visibles par une entité non authentifiée.

LA SIGNATURE DES APPLICATIONS

Un fournisseur d'applications peut exiger de vérifier l'intégrité et l'authentification des applications qu'il charge sur la carte. GlobalPlatform propose un mécanisme répondant à ce besoin : le DAP (Data Authentication Pattern). Pour chaque morceau de code envoyé à la carte, une empreinte est calculée. Cette empreinte est ensuite signée et rajoutée à la structure du bloc envoyé. L'APSD dans lequel l'application est chargée doit posséder le privilège de vérification des DAP afin de fournir ce service au nom du fournisseur d'applications.

LA VERIFICATION DU PORTEUR

GlobalPlatform, via le service global Cardholder Verification Method (CVM), fournit un mécanisme de vérification du porteur accessible à toutes les applications. Dans la version actuelle des spécifications, 5, seule la vérification du code PIN est supportée.

5. CAS D'ETUDES

5.1. ACCES A UNE CHAMBRE HOTEL

Prenons le cas d'un premier utilisateur de téléphone mobile. Il a l'habitude de voyager et de s'installer dans un hôtel pour ses voyages. Cette personne a une carte SIM dans laquelle est installée une application NFC. Son opérateur mobile, en France métropolitaine, lui a indiqué qu'il pouvait avoir accès à des dispositifs NFC grâce à sa carte SIM car elle détient une technologie SIM-Centric.

Notre utilisateur se déplace donc pour affaires dans différentes régions de France. Les hôtels dans lesquels il s'installe lui demandent de passer son portable devant une borne afin d'obtenir une clé numérique. Ainsi son portable pourra être utilisé comme clé.

Par la suite, notre utilisateur va à une conférence en Allemagne et souhaite aussi s'installer dans une chambre d'hôtel. Au moment de l'enregistrement, le lecteur accepte sa carte SIM mais lui signale que son opérateur lui imputera des frais dues à ce service hors de la France métropolitaine.

De retour de sa conférence, l'utilisateur demande à son opérateur de changer de forfait pour ne pas avoir à payer de frais à l'avenir et l'opérateur lui dit que cela est impossible car pour l'instant le service entraîne des frais à l'opérateur.

Dans un autre cas notre utilisateur pourrait réserver sa chambre d'hôtel en ligne. Il recevrait ensuite sur son téléphone mobile une clé électronique qui serait valable durant toute la durée du séjour et qui, utilisée avec la puce NFC et l'application adéquate, lui permettrait d'accéder à sa chambre en présentant le mobile devant la porte équipée d'un lecteur NFC.

L'Hôtel Clarion de Stockholm, en remplaçant en 2011 les clés de chambre par des clés numériques envoyées aux clients déjà équipés de portables NFC, leur a permis de se rendre directement à leur chambre en évitant les files d'attente. Même approche pour le check-out, réalisé d'un simple contact entre leurs téléphones et le lecteur du hall. 60% des utilisateurs ont déclaré avoir économisé plus de dix minutes et 80% utiliseraient à nouveau le système s'ils en avaient l'occasion tandis que l'hôtel a pu réaffecter le personnel dédié au check-in tout en supprimant les problèmes liés au remplacement des clés.

Les experts du secteur prédisent que le NFC va révolutionner nos vies dans les années à venir. Notre check-list quotidienne -« clés, portefeuille, téléphone »- est sur le point de se raccourcir. Il ne faudra pas longtemps avant de voir la fonctionnalité de ces trois objets intégrée dans un combiné compatible NFC.

Les utilisateurs du transport utilisent déjà leurs téléphones comme carte d'embarquement et au Japon, les systèmes de paiement NFC sont installés dans les restaurants, les taxis ou les distributeurs. Sur les campus universitaires, les étudiants peuvent utiliser leurs portables pour entrer dans les bâtiments, faire des achats, utiliser les transports et s'identifier lors des examens. Les téléphones NFC pourraient même être utilisés pour fournir aux médecins l'accès à votre historique médical. [8]

5.2. AUTRES CAS D'APPLICATIONS

Le champ d'application du NFC est très vaste. :

- Présentation d'une carte de fidélité auprès d'une caisse.
- Contrôle d'accès et ouverture de portes.
- Téléchargement d'application, ouverture d'un lien vers une page Web ou une vidéo Youtube, etc. suite à un tag présent sur une affiche, à la manière d'un QR Code (type d'un code barre).
- Inscription à un événement sur Google+, Facebook, etc.
- Paiement mobile à l'aide de son Smartphone.
- Accès sécurisé à un bâtiment ou un réseau.
- Carte de visite « dynamique » – Exemple NET-7
- L'approche d'une photo taguée du lecteur RFID lance l'application Skype et appelle la personne.

Carte de visite NET-7 et son tag NFC

Appel automatique Skype par sa photo étiquetée

Cette technologie permet le paiement mobile et le transfert de fichiers. Des périphériques NFC commencent également à apparaître, comme, par exemple, un clavier de poche sur lequel on pose simplement notre terminal préféré. Si l'ajout du NFC dans ce type d'appareil permet une utilisation assez poussée et ouverte, il est également utilisé dans des situations plus transparentes pour l'utilisateur final, par exemple, des cartes prépayées permettant alors de payer rapidement sans contact un ticket de bus ou un journal.

5.3. BUSINESS MODEL

On peut citer deux grands business model *ad hoc*.

BUSINESS MODEL SIM-CENTRIC

L'Opérateur de réseau mobile est l'émetteur de l'élément de sécurité et c'est ce dernier qui en charge de sa gestion ainsi que de son contrôle. Plusieurs fournisseurs de services peuvent ainsi télécharger leurs applications mobiles directement dans la carte SIM via un TSM (fournisseur de services de confiance).

Un TSM (Trusted Service Manager, fournisseur de services de confiance) assure l'efficacité et la sécurité de l'ensemble de la procédure de téléchargement des comptes de paiement dans les téléphones. Le commerce et le paiement mobiles nécessitent un niveau de coopération sans précédent entre opérateurs mobiles et établissements financiers. Le TSM connaît les mécanismes de sécurité des banques comme des téléphones mobiles, faisant le lien entre de multiples établissements financiers et opérateurs tout en garantissant la sécurité complète des informations de carte de crédit des consommateurs. La chaîne du commerce mobile comprend différents intervenants. Elle demande par exemple des téléphones compatibles, des cartes SIM, des TSM ainsi qu'une intégration avec les systèmes d'émission des établissements financiers et la signature de nouveaux partenariats commerciaux.

L'utilisation d'un TSM est souhaitable même s'il elle est optionnelle pour les raisons suivantes :

On s'attend à ce que plusieurs opérateurs téléphoniques et fournisseurs d'applications de paiement sans contacts travaillent ensemble en formant un écosystème. Pour faire face à une complexité supplémentaire, il est souhaitable qu'une entité indépendante et centrale fournisse les applications de paiement sans contact.

Le TSM peut aussi contrôler les contrats commerciaux : le fournisseur d'application de paiement n'a donc qu'à négocier avec Le TCM pour avoir accès aux UICC de tous les OTM (MNO).

	Opérateur de réseau mobile	**Fournisseur application de paiement**	**TSM**
Valeur directe	**Revenus TSM :** Location de l'espace de stockage contenu dans la SIM et éventuellement des frais de gestion de la durée de vie **Revenus utilisateur :** Frais pour l'utilisation de services NFC	**Revenus utilisateur :** Frais de services	**Revenus fournisseur d'applications :** Services Over The Air (OTA) **Revenu Operateur de réseau mobile :** Accueil pour des services OTA tiers

Valeur indirecte	Reduction du taux d'attrition	Satisfaction client et retention Reduction du cash handling	Service à forte valeur ajoutée

BUSINESS MODEL SIM NON-CENTRIC

1. Puce embarquée

Dans ce scenario, l'élément de sécurité est une puce embarquée et l'émetteur est le constructeur de téléphone. Il est important de noter que dans certains cas le constructeur n'est pas le fournisseur du système d'exploitation, mais les téléphones sont conçus selon les exigences de l'OS. Dans ce cas, c'est l'OS qui contrôle l'élément de sécurité. Par conséquent, le constructeur et le fournisseur de l'OS du téléphone deviennent maintenant les principaux acteurs qui contrôlent les clés de l'élément de sécurité pour le téléchargement sécurisé des applications d'achats sans contact.

Dans ce cas de figure le modèle est de type bilatéral.

Le constructeur et le fournisseur de l'OS doivent faire partie de l'écosystème de paiement NFC; pour se faire, des relations ou des arrangements doivent s'établir avec les acteurs suivants :

Le fournisseur de l'application de paiement (soit directement ou bien par le biais d'un TSM)

Les opérateurs avec les utilisateurs et même d'autres operateurs

	Opérateur de réseau mobile	**Fournisseur application de paiement**
Valeur directe	Revenus TSM : Location de l'espace de stockage contenu dans la SIM et éventuellement des frais de gestion de la durée de vie	Revenus utilisateur : Frais de services
Valeur indirecte	Satisfaction client	Satisfaction client et retention Reduction du cash handling

2. Carte mémoire :

Dans ce cas, le fournisseur de l'application de paiement doit jouer différents rôles mais néanmoins compatible dans l'écosystème de paiement. Du fait de son positionnement, le fournisseur de l'application est forcé de supporter l'écosystème NFC de paiement à lui tout seul et d'accepter de grands risques. Néanmoins, cet acteur peut réussir cette entreprise tout en étant indépendant d'autres acteurs mais doit être d'une taille considérable et posséder une marque reconnue.

Valeur direct	Revenus utilisateur : Frais de services Revenus tiers : Location de l'espace disponible sur la microSD et services OTA
Valeur indirect	Satisfaction client et retention Réduction du cash handling Opportunités liées à la carte mémoire : marketing, publicité…

6. CONCLUSION

Les technologies de l'information et de la communication continuent d'intégrer notre mode de vie dans la société et dans nos activités professionnelles.

A travers ce rapport, nous avons vu l'origine de la technologie NFC, ses différentes normes internationales ainsi que ses domaines d'application.

Ainsi, nous avons pu constater que l'usage de cette technologie ouvre beaucoup de perspectives dans plusieurs domaines, allant du m-Commerce au domaine médical en passant par le domaine du réseau social.

La NFC SIM-Centric fournit des avantages commerciaux et techniques, et offre une architecture capable de réussir dans l'écosystème NFC. Cependant, avant de pouvoir être certifié afin d'héberger des applications de paiement, le réelle «standard» SIM-Centric doit évoluer afin de répondre aux exigences du secteur bancaire. Ces améliorations de sécurité sont en cours d'élaboration et pourrait ouvrir la voie au déploiement du NFC en masse à l'avenir.

REFERENCES BIBLIOGRAPHIQUES

[1] L. Frédéric, « Etat de l'art et applications des RFID », Mémoire présenté devant le jury, Le 9 Juin 2008, Grenoble.

[2] ISO-14443(1…4): « Identification Cards –Contactless integrated circuit cards –Proximity cards»

[3] ISO-18092: Information technology, « Telecommunications and information exchange between systems-Near Field Communication –Interface and Protocol», Technical Report, ISO/IEC, 2004

[4] ECMA International: Standard ECMA-340, « Near Field Communication Interface and Protocol -1 (NFCIP-1) », 3 rd Edition, February 2008

[5] ECMA International: Standard ECMA-352, « Near Field Communication Interface and Protocol -2 (NFCIP-2) », 2 nd Edition, 2010

[6] http://www.nfc-forum.org

[7] http://www.nfc-forum.org/specs

[8]http://www.infodsi.com/articles/134717/benefices-technologie-mobile-nfc-sonnera-glas-cle-traditionnelle.html