



RÉPUBLIQUE ALGÉRIENNE  
DÉMOCRATIQUE ET POPULAIRE



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI de Tizi-Ouzou

Faculté de Génie Électrique et d'Informatique

Département d'Informatique

# Mémoire de Fin d'étude

En vue de l'obtention du diplôme de Master Académique en  
Informatique

**Option : System informatique**

## Thème :

Conception et réalisation d'une application  
Android pour le paiement électronique via le  
standard NFC.

**Dirigée par :**

**Mlle Ait Adda Samia**

**Réalisé par:**

**Mr. HADID Belkacem**

**Mr TIZA Mohamed Akli**

2016/2017



# *Remerciements*

*Au terme de la rédaction de ce mémoire, c'est un devoir agréable d'exprimer en quelques lignes la reconnaissance que nous devons à tous ceux qui ont contribué de loin ou de près à l'élaboration de ce travail, qu'ils trouvent ici nos vifs respects et notre profonde gratitude.*

*Tout d'abord, nous adressons toute notre gratitude à notre encadreur **Mlle Ait Adda Samia**, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter notre réflexion. Nous la remercions également de nous avoir fait confiance et encouragé tout le long de ce projet.*

*Puis à notre Co-encadreur **Mme Ramdani**, d'avoir pu nous donner la chance de réaliser notre stage pratique, de nous avoir pris sous sa tutelle et de tous ses précieux conseils, merci infiniment*

*Nous tenons à remercier également les membres du jury d'avoir accepté d'évaluer notre travail.*

*Nous voudrions exprimer notre reconnaissance envers les amis(es) et collègues, qui nous ont apportés leur support moral et intellectuel tout le long de notre démarche.*

# DÉDICACES

*À ma très chère famille*

*Je vous dois ce que je suis aujourd'hui grâce à votre amour, à votre patience et vos innombrables sacrifices. Que ce modeste travail, soit pour vous une petite compensation et reconnaissance de ce que vous avez fait d'incroyable pour moi. Quoi que je fasse ou que je dise, je ne saurais point de vous remercier comme il se doit. Que DIEU, le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.*

*À mes très chers amis(es)*

*En témoignage de l'amitié sincère qui nous a liés et des bons moments passés ensemble je dédie ce travail à tous mes amis(es) et camarades de la promotion, en vous souhaitant un avenir radieux et plein de bonnes promesses.*

*Mouhamed Akli*

# DÉDICACES

*À mes très chers parents*

*Je vous dois ce que je suis aujourd'hui grâce à votre amour, à votre patience et vos innombrables sacrifices. Que ce modeste travail, soit pour vous une petite compensation et reconnaissance de ce que vous avez fait d'incroyable pour moi. Quoi que je fasse ou que je dise, je ne saurais point de vous remercier comme il se doit. Que DIEU, le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.*

*À mon cher frère et ma chère sœur, d'avoir su m'encourager m'aider dans n'importe quelle situation.*

*À mes très chers amis(es)*

*En témoignage de l'amitié sincère qui nous a liés et des bons moments passés ensemble je dédie ce travail à Smail, Hocine, Yacine, marzouk, Lyes, et biens sûre Khali ali et à tous mes amis(es) et camarades de la promotion en vous souhaitant un avenir radieux et plein de bonnes promesses.*

*Belkacem*

# Table des matières

<b>Introduction générale</b> .....	1
<b>Chapitre I Généralités sur l'e-commerce</b> .....	4
I. Introduction.....	5
II. Définitions du e-commerce : .....	5
II.1. E-commerce .....	5
II.2. Le m-commerce .....	6
III. Les différents types d'échanges commerciaux .....	6
IV. Étapes d'une transaction e-commerce .....	8
V. Comparaison entre le commerce traditionnel et le e-commerce .....	9
VI. Les avantages du commerce électronique.....	10
VII. Les inconvénients et les contraintes du commerce électronique .....	10
VIII. L'évolution du commerce électronique en quelques chiffres .....	11
IX. Aspects juridiques.....	12
IX.1. Les problèmes causés par l'informatique.....	12
IX.2. La fraude informatique.....	13
IX.2.1. L'action frauduleuse sur les STAD .....	13
IX.2.2. L'atteinte informatique aux libertés individuelles.....	14
IX.2.3. Les délits généraux .....	14
IX.2.4. Les textes juridiques .....	14
X. E-Commerce Algérien .....	14
X.1. Présentation du commerce électronique en quelques chiffres .....	15
X.3. Paiement électronique .....	17
XI. Conclusion .....	17
<b>Chapitre II Le paiement électronique</b> .....	19
I. Introduction.....	20
II. Définitions .....	20

II.1.	E-paiement.....	20
II.2.	M-paiement.....	20
III.	Les modes du paiement.....	20
III.1.	Modes de paiement direct .....	20
III.1.1.	Cache .....	21
III.1.2.	Les chèques.....	21
III.1.3.	Les cartes bancaires .....	21
III.2.	Modes du paiement indirect.....	21
III.2.1.	Le Porte-monnaie électronique.....	22
III.2.2.	Le chèque électronique .....	22
III.2.3.	Le numéro à 16 chiffres de la carte bancaire .....	22
III.2.4.	E-paiement par téléphone portable .....	23
IV.	Les critères du paiement électronique .....	23
IV.1.	Identifier les parties concernées .....	23
IV.2.	Confidentialité de la transaction .....	24
IV.3.	Intégrité du procédé .....	24
IV.4.	Non-répudiation .....	24
IV.5.	Contrôle d'accès.....	24
V.	La monétique .....	24
V.1.	les acteurs .....	25
V.2.	Les relations entre les acteurs .....	25
V.3.	Les transactions bancaires .....	26
V.3.1.	Le processus général .....	26
V.3.2.	La transaction .....	27
V.3.3.	La télécollecte .....	28
V.3.4.	Télé-compensation .....	29
V.4.	La Sécurité dans des cartes bancaires .....	30

V.4.1.	Les menaces .....	30
V.4.2.	Sécurité interne de la carte bancaire.....	31
V.4.3.	Sécurité Fonctionnelle (externe à la carte bancaire) .....	31
V.4.4.	Réseau .....	31
VI.	Le m-paiement .....	32
VI.1.	Les différents modes de paiement mobile.....	32
VI.1.1.	Paiement à distance .....	32
VI.1.2.	Paiement de proximité .....	32
VI.1.3.	Paiement de mobile à mobile.....	32
VI.1.4.	Autre type de m-paiement .....	32
VI.2.	Les technologies utilisées dans le M-paiement.....	32
VI.2.1.	Le SMS (mode de paiement mobile à distance) .....	32
VI.2.2.	Square .....	33
VI.2.3.	Bluetooth .....	33
VI.2.4.	Code QR .....	34
VI.2.5.	Le NFC (Near Field Communications) .....	34
VII.	Les techniques de sécurités dans l'm-paiement .....	37
VII.1.	La cryptographie .....	37
VII.1.1.	Cryptage symétrique.....	37
VII.1.2.	Cryptage asymétrique .....	38
VII.2.	La signature électronique .....	39
VII.3.	Les certificats électroniques.....	40
VII.4.	L'identification .....	40
VII.5.	La datation .....	42
VII.6.	Le protocole SSL .....	42
VII.7.	Le protocole SET .....	43
VIII.	Conclusion .....	44



<b>Chapitre III : Présentation de l'organisme d'accueil .....</b>	<b>46</b>
I. Introduction.....	47
II. Définition de la banque .....	47
III. Historique de la Banque Nationale d'Algérie .....	47
IV. La mission de la BNA.....	48
V. Le réseau bancaire algérien .....	48
V.1. Les principales missions du SATIM .....	49
VI. Organisation de la BNA.....	49
VI.1 Description de l'organigramme :.....	51
VI.2 Organisation interne de la BNA .....	52
VI.2.1 La direction générale(DG) .....	52
VI.2.2 Les divisions .....	53
VI.2.3 Direction centrale (DC) .....	53
VI.2.4 Direction régionales (DRE) .....	53
VI.2.5 Agences.....	53
VII. Présentation du champ d'études.....	54
VII.1 Activités de la Cellule informatique .....	55
VII.2 Situations informatique de la banque.....	55
VIII. Conclusion .....	56
<b>Chapitre IV: Analyse &amp; conception .....</b>	<b>57</b>
I. Introduction.....	58
II. Problématique et objectifs attendus .....	58
III. Architecture de notre application :.....	58
III.1.1 Les interfaces : .....	60
III.1.2 Les modules : .....	60
IV. Analyse .....	61
IV.1 Spécification des besoins.....	61

IV.1.1	Spécification des besoins fonctionnels.....	61
IV.1.2	Spécification des besoins non fonctionnels.....	62
IV.2	Méthodologie et approche adoptée.....	63
IV.3	Identification des acteurs .....	63
IV.4	Les diagrammes de cas d'utilisation.....	65
IV.4.1	Diagrammes de cas d'utilisation .....	65
IV.4.2	Diagramme de cas d'utilisation pour le client.....	65
IV.4.3	Diagramme de cas d'utilisation pour le commerçant :.....	67
V.	Conception .....	70
V.1	Les diagrammes de séquence : .....	70
V.1.1.	Diagramme de séquence pour le cas d'utilisation inscrire client. ....	72
V.1.2.	Diagramme de séquence pour le cas d'utilisation payé le commerçant.....	73
V.2.	Diagramme de déploiement :.....	74
V.3.	Conception de la couche communication avec les modes NFC :.....	75
V.3.1.	Architecture du mode Emulation de carte « SmartPay » .....	75
V.3.2.	Architecture du mode lecteur « SmartTPE » : .....	81
V.3.3.	La Communication NFC entre le lecteur « SmartTPE » et le Mode Carte « SmartPay » .....	83
V.4	Niveau organisationnel des données.....	84
V.4.1	Le modèle entités associations : .....	84
V.4.2	Schéma relationnel : .....	85
VI.	Conclusion : .....	85
<b>Chapitre V Réalisation.....</b>		<b>87</b>
I.	Introduction :.....	88
II.	Les bases et le cadre du projet .....	88
II.1.	A propos d'Android.....	88
II.1.1.	Système d'exploitation .....	88

II.1.2.	Android API .....	88
II.1.3.	Développement d'application Android .....	88
II.2.	Les objectifs du projet .....	90
III.	La mise en œuvre du projet.....	91
III.1.	Android Studio.....	91
III.2.	L'API Android NFC .....	91
III.3.	Les APDU :.....	92
III.4.	Les smartphones.....	92
III.5.	Planification du projet.....	92
IV.	Réalisation .....	92
IV.1.	SmartPay .....	93
IV.2.	SmartTPE.....	98
IV.3.	Simulation d'un serveur de la banque.....	105
V.	Conclusion .....	107
	<b>Conclusion générale</b> .....	108
	<b>Bibliographie</b> .....	111
	<b>Webographie</b> .....	112
	<b>Annexe</b> .....	113

## Table des figures

Figure I.1 : Différents échanges de produits et de services .....	7
Figure I.2 : Les étapes d'une transaction e-commerce .....	8
Figure I.3 : Chiffre d'affaires de l'e-commerce mondial .....	12
Figure I.4 : Chiffres clés par âge de l'e-commerce en Algérie année 2015 .....	15
Figure I.5 : Répartition géographique de l'e-commerce en Algérie année 2015 .....	16
Figure II.1 : Schéma général d'une transaction bancaire .....	26
Figure II.2 : les étapes d'une e-transaction .....	28
Figure II.3 synthèse de la télécollecte .....	29
Figure II.4 : synthèse de la télé-compensation .....	30
Figure II.5 : photo d'un square avec une prise Jack .....	33
Figure II.6 : exemple de code QR .....	34
Figure II.7 : schéma illustrant le fonctionnement du chiffrement symétrique. ....	38
Figure II.8 : schéma illustrant le fonctionnement du chiffrement asymétrique .....	38
Figure II.9 : Fabrication du certificat. ....	40
Figure II.10 : schéma d'identification .....	41
Figure II.11 : schéma datation d'un document.....	42
Figure II.12 : L'identification dans le protocole SSL .....	43
Figure II.13 : Le schéma d'une transaction à l'aide du protocole SET .....	44
Figure III.1 : L'organigramme de la BNA .....	50
Figure III.2 : Organisation interne de la BNA.....	52
Figure III.3 : Organigramme de champ d'étude.....	54
Figure IV.1 Architecture globale de notre application.....	59
Figure IV.2 Diagramme de cas d'utilisation pour le client. ....	66
Figure IV.3 Diagramme de cas d'utilisation pour le commerçant .....	68
Figure IV.4 Diagramme de cas d'utilisation pour la banque. ....	69
Figure IV.5 Diagramme de séquence pour le cas d'utilisation inscrire client .....	72
Figure IV.6 Diagramme de séquence pour le cas d'utilisation payé le commerçant.....	73
Figure IV.7 Diagramme de déploiement.....	74
Figure IV.8 Schéma paiement NFC en mode HCE .....	76
Figure IV.9 : Les trames ISO 14443-4 transportent des APDUs (ISO 7816-4).....	78
Figure IV.10 : les étapes de la lecture de tags par le contrôleur NFC dans le système Android.....	82

Figure IV.11 Séquencement de la sélection du service HCE.....	84
Figure IV.12 Le modèle entités associations.....	85
Figure V.1: le cycle de vie d'une Activité.....	89
Figure V.2 : Interface principale de « SmartPay » .....	93
Figure V.3 : Les étapes de l'inscription .....	94
Figure V.4 :L'interface transaction du client .....	95
Figure V.5 :L'interface principale de SmartTPE .....	99
Figure V.6:L'activité Accueil de SmartTPE .....	99
Figure V.7 : Le déroulement de transaction .....	100
Figure V.8 : Historique et statistique des transactions .....	101
Figure V.9: le code java de la classe ServerS .....	106
Figure V.10 : le code java de serveur mail.....	107

## Table des tableaux

Tableau I.1 : E-commerce VS Commerce traditionnel .....	9
Tableau IV.1 formats des commandes APDU's. ....	80
Tableau IV.2 formats des réponses APDU's.....	80
Tableau IV.3 Format de l'AID.....	81

# *Introduction*

## *générale*

## Introduction générale

---

Les systèmes de paiement ne cessent d'évoluer au fil des années, du troc jusqu'aux pièces d'or puis par la suite les billets de banque et enfin les cartes bancaires, les êtres humains ne cessent de recréer les systèmes de paiement, à l'air de l'informatique la virtualisation de la monnaie devient indispensable.

En effet, les technologies de communication créent de nouvelles opportunités et des nouveaux domaines à explorer. Depuis quelques années, les Smartphones sont dotés d'une puissance de plus en plus importante. Les téléphones tendent à devenir des objets quasi indispensables dans notre vie quotidienne, et possèdent des fonctionnalités qu'aucune technologie ne pouvait espérer auparavant : connexion haut débit, localisation GPS (Global Positioning System), boussole, accéléromètre, écran tactile, puces sans contact à champs rapprocher NFC (Near Field Communication), lecteur d'empreintes digitales ... Autant de qualités permettant de créer des applications innovantes.

La révolution des Smartphones dans le e-paiement concurrence le système de la carte bancaire actuel, beaucoup de grandes entreprises se lancent dans cette nouvelle technologie et parmi elles, Apple avec son application « Apple Pay » qui utilise la puce sans contact NFC et une validation par l'empreinte digitale du possesseur de l'iPhone (TouchID). Samsung en Corée du Sud et Sony au Japon ont réussi à convertir des millions de consommateurs au paiement à courte distance, à côté de son accord avec Samsung, la société PayPal développe sa propre solution de paiement via mobile chez le commerçant (One Touch)<sup>1</sup>, pour l'instant testée en France à Nancy. Le géant Google n'est bien sûr pas absent de cette bataille : il a créé un concurrent direct de PayPal, Google Wallet, disponible aux États-Unis seulement, le moteur de recherche a développé aussi sa solution de paiement mobile également via le standard NFC.

L'Algérie se lance dans l'e-paiement à partir de 2017 selon les dires de madame la ministre de la poste et des technologies de l'information et de la communication, avec ce type d'application on pourra garantir aux algériens un moyen de paiement fiable sécurisé et simple à mettre en place de coût minime. Et promouvoir l'Algérie au niveau actuel des pays développés et sauter l'étape de la carte bancaire qui cède sa place de plus en plus aux nouvelles

---

<sup>1</sup> Conçu pour faciliter le paiement à l'intérieur des applications mobiles, le service PayPal One Touch fait ses débuts officiels en France. Expérimenté dans les commerces de proximité à travers le service Pay@Table, exploité dans le cadre d'une solution associant smartphone et lecteur de cartes bancaires, enrichi par des expérimentations autour de la technologie Beacon

# Introduction générale

---

technologies, ainsi économiser des milliers de dollars aux banques et à la poste algériennes (le maintien des distributeurs de billets et fabrication des cartes bancaires). Intégrer la carte bancaire et l'e-paiement au quotidien d'un algérien brusquement risque de lever une grande résistance au changement contrairement au smartphone qui est déjà intégré dans la vie d'un simple citoyen, et avec cette application les chances d'acceptation de ce type de paiement s'accroîtront et permettra ainsi à un grand nombre de citoyens de bénéficier de ses avantages.

C'est dans ce contexte que s'inscrit ce projet de fin d'études, qui consiste à créer une application Android de paiement en ligne, avec une seule application qui englobe toutes les cartes bancaires encombrantes actuelles, une application qui va jouer le rôle de la carte bancaire avec la puce NFC, mais aussi la possibilité de payer en ligne dans les sites de e-commerce. Cette application sera le couteau suisse du futur utilisateur, mais aussi pour les commerçants qui seront doté d'un terminale NFC ou bien d'un autre smartphone compatible NFC et ainsi résoudre beaucoup de problèmes : le manque de monnaie liquide, traçabilité des transactions, paiement des impôts, surveillance des achats par le client.

Notre mémoire s'articule sur c'est cinq chapitres :

- Le premier chapitre introduit les généralités sur l'e-commerce.
- Le second chapitre est dédié explicitement au e-paiement via le mobile paiement appelé aussi m-paiement.
- Le troisième chapitre est consacré à la présentation de l'organisme d'accueil.
- Le quatrième chapitre nous détaillerons l'analyse et la conception de notre système.
- Le dernier chapitre décrit les différents moyens et techniques utilisés pour sa réalisation.



# ***Chapitre I***

***Généralités sur l'e-commerce***

## I. Introduction

Depuis que les réseaux de communication existent, il y a eu toujours des entrepreneurs qui ont pleinement exploité les possibilités à des fins purement économiques. La récente percée des techniques modernes de télécommunication et de l'informatique a porté ces nouvelles technologies au cœur de l'infrastructure économique internationale, surtout le développement explosif du réseau Internet qui a accéléré la transformation du commerce national et international, permettant des contacts instantanés et peu onéreux entre vendeurs, acheteurs, investisseurs, publicitaires et financiers dans le monde entier.

Comme dans tout domaine en voie de développement, la notion du commerce électronique est encore mal cernée. Donc nous allons expliquer brièvement dans ce chapitre la notion de e-commerce, puis nous allons préciser ses avantages et ses contraintes sans oublier l'aspect juridique, et enfin nous allons indiquer les points essentiels dans le e-commerce algérien.

## II. Définitions du e-commerce :

Le commerce sur internet est divisé en deux parties la première c'est le E-Commerce et la seconde est le M-Commerce, dans ce qui va suivre nous allons définir ces deux concepts.

### II.1. E-commerce [1]

Le commerce électronique (ou commerce en ligne, vente en ligne ou à distance, parfois cybercommerce). On emploie également la dénomination anglaise e-commerce.

« Le commerce électronique est l'ensemble des échanges numérisés liés à des activités commerciales qui prendraient en considération <sup>2</sup> :

#### 1) Personnes et organismes :

Il s'agit aussi bien des relations inter-entreprises (business to business) que des relations entre entreprises et administrations ainsi que des échanges entre entreprises et consommateurs (business to consumer).

---

<sup>2</sup> Cette définition est donnée par **Francis Lorentz**, né en 1942 (à Mulhouse), un dirigeant français d'entreprises dans le domaine des technologies de l'information et de la communication

## 2) Produit :

Le commerce électronique couvre à la fois les échanges d'informations et les transactions concernant les produits, les équipements, les biens de consommation courants, les services d'informations...etc.

## 3) Mode de transmission utilisé :

Il concerne : les opérations effectuées via la télévision, les réseaux informatiques et Internet ; leur caractéristique commune est de traiter l'information incluant textes, données, sons et images. »

## II.2. Le m-commerce

Le m-commerce ou commerce mobile (mobile commerce en anglais) est une partie du e-commerce, correspond à l'utilisation des technologies sans fil, et plus particulièrement de la téléphonie mobile, afin d'effectuer des achats. Il regroupe l'ensemble des applications commerciales liées aux terminaux mobiles et effectuées le plus souvent en situation de mobilité<sup>3</sup>. Le commerce mobile ne se limite pas aux téléphones portables de type smartphones mais aussi aux tablettes tactiles et PDA (Personal Digital Assistant). [2]

## III. Les différents types d'échanges commerciaux

Internet propose des moyens de communication souples dont l'utilisation permet à l'entreprise, ou aux particuliers, de s'affranchir des contraintes temporelles et spatiales. On distingue plusieurs types d'échanges commerciaux comme il est représenté dans la figure I.1:

---

<sup>3</sup>Définition webmarketing. 2011 [consulté le 24 novembre 2011]. Disponible sur : <http://www.definitions-webmarketing.com/Definition-M-commerce>

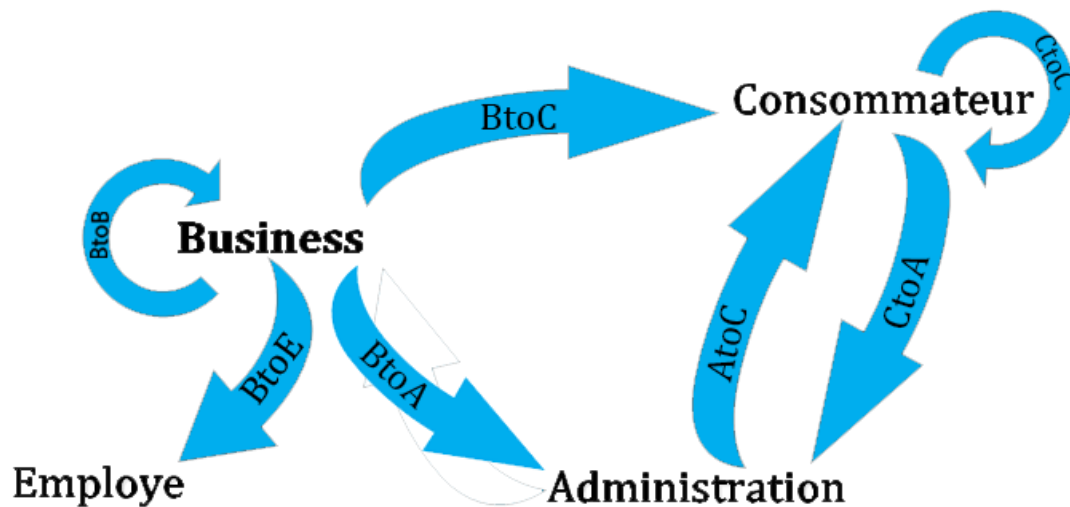


Figure I.1 : Différents échanges de produits et de services

**1) Commerce électronique d'entreprise à entreprise (Business to Business, BtoB) :**

Le commerce électronique d'entreprise à entreprise concerne les transactions électroniques entre deux ou plusieurs entreprises, c'est-à-dire l'achat auprès des vendeurs de biens et de services.

**2) Commerce électronique d'entreprise à consommateur (Business to Consumer, BtoC) :**

Le business to consumer est constitué de différentes transactions électroniques entre une entreprise et un consommateur. Ce type d'échanges est sans doute l'aspect le plus viable du commerce électronique, car il permet au consommateur d'acheter directement sur Internet des biens et des services pour son usage personnel.

**3) Commerce électronique intra-entreprise (within-business) :**

Un intranet est un réseau hermétique connecté à Internet mais protégé par un pare-feu. L'entreprise qui dispose d'un intranet met à la disposition de son personnel toutes formes d'informations pertinentes accessibles de manière instantanée.

**4) Commerce électronique d'entreprise à administration (Business to Administration B to A):**

Le business to administration (B to A) concerne les transactions entre une entreprise et une administration, par exemple, la transmission d'une déclaration de revenus vers un ministre.

**5) Commerce électronique de consommateur à administration (Consumer to administration, C to A) :**

Ce type d'échange concerne les transactions entre un citoyen et une administration (déclaration d'impôt, demande de passeport...).

### 6) Commerce électronique de consommateur à consommateur (Consumer to Consumer, C to C) :

Cette forme d'échange concerne les transactions électroniques entre deux ou plusieurs consommateurs comme par exemple la vente aux enchères et la bourse d'échange.

## IV. Étapes d'une transaction e-commerce [3]

Le e-commerce est divisé en plusieurs étapes que le client et le commerçant doivent suivre pour réaliser une transaction commerciale, comme le montre la figure I.2 :

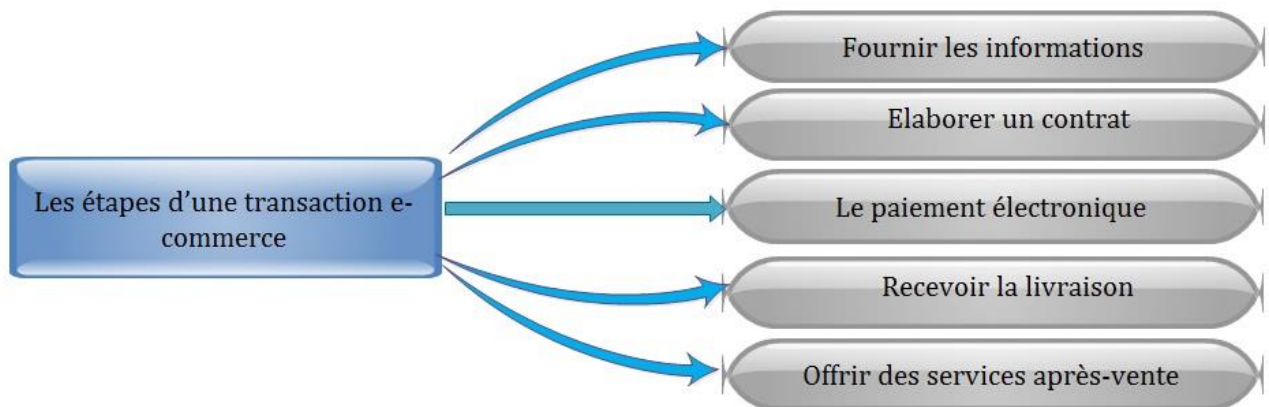


Figure I.2 : Les étapes d'une transaction e-commerce

### 1) Fournir les informations :

Il s'agit de donner toutes les informations nécessaires sur les produits ou services au client : catalogue, liste des prix, caractéristiques des produits, les offres de l'entreprise...

### 2) Elaborer un contrat :

Mentionner les conditions de vente, ceci contient le prix, les rabais, méthode de paiement et méthode de livraison. Cette phase doit aboutir à un contrat très bien compris par les deux côtés de la transaction.

### 3) Le paiement électronique :

Le client doit payer le produit tout en respectant la méthode choisie dans le contrat, celle qui convient au commerçant et au client, cette méthode doit être un transfert d'argent en ligne. Le paiement électronique représente notre domaine d'étude il sera développé dans le chapitre II.

**4) Recevoir la livraison :**

Le client doit être satisfait après la livraison comme il était convenu dans les conditions du contrat, que ce soit sur la qualité des marchandises ou le délai de livraison.

**5) Offrir des services après-vente :**

Satisfaire le minimum de service après-vente : support technique, information sur les nouveaux produits, réparation et remboursement en cas de panne...

**V. Comparaison entre le commerce traditionnel et le e-commerce [3]**

Une comparaison entre le commerce traditionnel et le commerce électronique est schématisée dans le tableau synoptique suivant :

<b>Etapes</b>	<b>Le commerce traditionnel</b>	<b>Le commerce électronique</b>
Recherche d'un vendeur	Aller dans un magasin.  Lire la presse.  Recevoir un représentant.	Utiliser un moteur de recherche.  Visiter les portails et lire les publicités web.  Recevoir des mails.
Vérification du produit et délai de livraison	Visiter le magasin.  Recevoir un représentant.	Consulter le catalogue électronique.  Recevoir un mail
Acheter	Aller à la caisse.  Faire une demande par lettre.	Envoyer un mail.  Compléter un formulaire web.
Facturation	Imprimer et poster.  Imprimer et envoyer avec le produit ou par un agent.	Expédier par mail.  Imprimer directement après la validation d'achat.
Suivi de livraison	Se renseigner par téléphone.	Consulter le portail de livreur.
Paielement	Paielement liquide uniquement.	Choisir entre le paielement liquide ou paielement électronique.

*Tableau I.1 : E-commerce VS Commerce traditionnel*

## VI. Les avantages du commerce électronique

La liste des avantages que nous dressons ici n'a pas pour vocation d'être complète mais plutôt d'identifier ceux qui ont le plus d'importance dans le cadre du commerce électronique.

### Pour l'entreprise :

- Une entreprise peut atteindre des clients potentiels un peu partout dans le monde.
- Réduction du coût de stockage et des délais de vente grâce à l'utilisation d'outils numériques.
- Certaines procédures ou modes de stockage seront omis, dont les taxes qui viennent avec.
- Avec le e-commerce les PME<sup>4</sup> peuvent concurrencer les grandes entreprises et se faire une place dans le marché mondial.
- Faciliter l'innovation en ouvrant les portes du commerce à tout le monde et accélérer les procédures de vente.
- Les services et les produits seront offerts dès leur disponibilité.
- Le service de vente est ouvert 24/24 pendant toute l'année.

### Pour le consommateur :

- Le client peut choisir à son goût et prendre son temps à faire son choix.
- Une sélection plus variée et une comparaison des différents prix et des différentes marques.
- Les produits numériques peuvent être téléchargés immédiatement.
- Trouver un produit qui satisfera le client plus aisément.
- Commander chez soi.

## VII. Les inconvénients et les contraintes du commerce électronique

On ce qui concerne les contraintes et les limitations du E-commerce nous citons ci-dessous quelques exemples qui font l'inconvénient majeur de ce type de commerce.

---

<sup>4</sup> Petite et Moyenne Entreprise

### Pour L'entreprise :

- Il est difficile d'oser mettre son investissement dans la toile « internet ».
- Perdre la confiance des consommateurs à cause du manque de sécurité.
- La résistance des intermédiaires (grossistes, livreurs) qui craignent une perte du chiffre d'affaire.
- Les traitements des commandes de BtoC à grande échelle demandent des entrepôts de données et des serveurs web ce qui ajoute d'avantage de dépenses.
- Il est difficile d'intégrer internet et la solution e-commerce avec certaines applications ou bases de données.

### Pour le client :

- La plupart des gens aiment toucher et sentir la marchandise.
- La fraude en ligne qui s'accroît.
- Les gens ne font pas encore confiance aux transactions numériques et les vendeurs sont souvent inconnus.
- Si le produit arrive dans un mauvais état, il peut être difficile à remplacer ou se faire rembourser

## VIII. L'évolution du commerce électronique en quelques chiffres

Selon une étude française faite par la Fevad<sup>5</sup>, le commerce en ligne continue son ascension en France en grappillant toujours plus de chiffre d'affaire d'année en année, pour preuve en 10 ans le marché est passé d'un revenu de 8 milliards d'euros à plus de 70 milliards aujourd'hui. Les habitudes de consommation des Français place la France au 5eme rang mondial des achats en ligne, derrière notamment la Chine, les Etats-Unis et le Royaume-Unis. Retenons également que le phénomène du « cross-border », à savoir l'achat/vente à l'étranger sur internet, va s'accroître dans les prochaines années, notamment dans l'Union Européenne où les règles tendent à s'harmoniser. Par exemple, le seuil de 50% de cybermarchands français ayant déjà reçu des commandes de l'étranger a été dépassé en 2015.[4]

---

<sup>5</sup>Fédération e-commerce et vente à distance créée en 1957 par **Marcel Delcourt**, elle regroupe plus de 500 entreprises et membres du Mouvement des entreprises de France (MEDEF).



Dans la figure I.3 l'e-commerce BtoC mondiale s'est élevé à 1 671 milliards de dollars en 2015, en hausse de 25% par rapport à 2014, d'après eMarketer<sup>6</sup>. Il pèse donc 7,4% du total des ventes de détail dans le monde. L'institut prévoit pour 2016 que l'e-commerce BtoC mondial dépassera 3 500 milliards en 2019. Il représentera alors 12,8% du total des ventes de détail sur la planète. [5]



Figure I.3 : Chiffre d'affaires de l'e-commerce mondial

## IX. Aspects juridiques

La société humaine est entrée depuis près d'un quart de siècle, dans une ère de communication et de développement technologique. En plus, des espaces juridiques classiques (terrestre, maritime et aérien), un nouvel espace est apparu, à savoir l'espace virtuel. Dans ce qui va suivre nous allons citer les problèmes causés par l'informatique et les fraudes commises contre l'e-commerce.

### IX.1. Les problèmes causés par l'informatique

L'informatique en général et internet en particulier remettent en cause toute notre vision et toute l'architecture du droit national, communautaire et international. De ce fait, l'informatique pose de nombreux problèmes :

- ✓ dans la structuration du droit : le droit est territorial et national.
- ✓ dans le respect des libertés publiques : respect de la vie privée.
- ✓ dans le respect de l'ordre public : lutte contre le terrorisme, racisme, antisémitisme.

<sup>6</sup>eMarketer : est une société de recherche de marché filiale à 93%, fondée en 1996

- ✓ dans la conclusion des contrats : le droit des contrats est fondé sur un écrit et une signature manuelle entre deux personnes soumises au même droit.
- ✓ des règles en matière de responsabilité : responsabilité civile, pénale, responsabilité des hébergeurs, des prestataires.
- ✓ dans le droit du travail : surveillance des salariés, chartes informatiques, tracts par internet, contrôle des e-mails, utilisation de l'outil informatique par les salariés.
- ✓ dans les pratiques commerciales : délai de livraison, fraude, abus de position dominante, contrefaçon, recel, escroquerie.

## IX.2. La fraude informatique

Lorsque l'on évoque la fraude informatique, nous distinguons trois types d'infractions pénales, à savoir les actions frauduleuses sur les STAD<sup>7</sup>, L'atteinte informatique aux libertés individuelles et les délits généraux (la falsification de documents informatisés, la contrefaçon,...). Ces fraudes touchent de près ou de loin le commerce électronique.

### IX.2.1. L'action frauduleuse sur les STAD

L'intrusion a un système informatisé et puni de plusieurs manières selon la gravité du délit effectué on distingue :

#### 1) L'intrusion frauduleuse dans le système

Exemple : modification du système de vérification des comptes bancaires, modification du système de paiement dans les sites e-commerce, accéder à l'historique des ventes sur un site de e-commerce.

#### 2) La manipulation des STAD

- ✓ la perturbation des données : Exemple virus, logiciels piégés, détournements du code secret et de l'argent.
- ✓ l'altération des données : Exemple : les cookies, les numéros des cartes bancaires.
- ✓ importation, détention, offre, mise à disposition d'outils pour commettre l'infraction Ex : auteurs de virus, vers, cheval de Troie, spywares...

---

<sup>7</sup>STAD : système de traitements automatisé de données « tous ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité »

## IX.2.2. L'atteinte informatique aux libertés individuelles

Exemple : divulgation d'informations nominatives, collecte frauduleuse des données, espionnage des comptes bancaires, intercepter les transactions du paiement.

## IX.2.3. Les délits généraux

### 1) la falsification des documents informatisés :

Comme le certificat électronique, ou chèque électronique ou un virement bancaire....

### 2) la contrefaçon

Lorsque un bien informationnel (logiciel, base de données, pages web, produits multimédias...) fait l'objet d'un acte qui n'est pas autorisé par son auteur (reproduction, adaptation, utilisation sans droit...).

### 3) Les atteintes aux intérêts des banques

Par exemple : contourner l'argent des clients, dévaliser une banque, avoir les codes secrets des comptes des clients ...

## IX.2.4. Les textes juridiques

On entend par le cadre juridique formel du commerce électronique, l'ensemble des textes juridiques qui ont été élaborés et adoptés par des institutions étatiques qui sont destinées à être appliquées que ce soit au niveau national ou international. Il existe plusieurs références mondiales mais on constate un manque de lois en Algérie pour l'e-commerce et l'e-paiement, on peut se référer à des références à l'échelle mondiale européenne et enfin magrébine<sup>8</sup>.

## X. E-Commerce Algérien

Avec la libération progressive du marché algérien, le pays commence à s'élargir à d'autres domaines que les hydrocarbures tels que le tourisme, l'industrie et les télécommunications. À propos ce dernier point, les télécommunications ou les TIC<sup>9</sup> ce secteur connaît une nette amélioration, avec la création de l'ARPT (autorité de régulation de la poste et des télécommunications) et la mise en place du registre de commerce électronique en 2014, puis le lancement de l'E-paiement en octobre 2016. Ce qui induit au développement explosif de ce type de commerce. Dans cette partie nous allons présenter le commerce électronique algérien

---

<sup>8</sup> Voir l'annexe 1 : Aspect juridique

<sup>9</sup> Technologies de l'information et de la communication

par quelques chiffres et une explication de l'état actuel du cybercommerce puis on va finir par introduire le paiement électronique qui est notre domaine d'étude.

### X.1. Présentation du commerce électronique en quelques chiffres [6]

L'Algérie est loin d'être prête pour le commerce électronique, selon un nouveau rapport des Nations Unies publié le 22 avril 2015. Faisant son entrée au 95e rang de l'édition 2016 du classement "BtoC E-Commerce Index" après avoir été absent des rapports précédents, le pays accuse un important retard, notamment comparé à d'autres pays africains.

Loin derrière l'Afrique du Sud (61), la Tunisie (73) et le Maroc (79), et bien qu'ayant la quatrième plus grande économie du continent, l'Algérie apparaît au 8e rang africain sur ce rapport de l'e-commerce établi par la CNUCED (Conférence des Nations Unies sur le Commerce Et le Développement).

Les facteurs pris en considération par ce classement, qui s'appuie sur la performance de l'Algérie en matière de commerce en ligne, sont le taux de pénétration de l'utilisation d'internet. Le taux de pénétration des cartes de crédit, le nombre de serveurs sécurisés et la fiabilité de la poste et des services de livraison. Seulement 28% des Algériens ont accès à internet en 2015, le nombre de personnes âgées de plus 15 ans et possédant une carte de crédit ne dépasse pas les 6% comme il est indiqué dans la figure I.4.

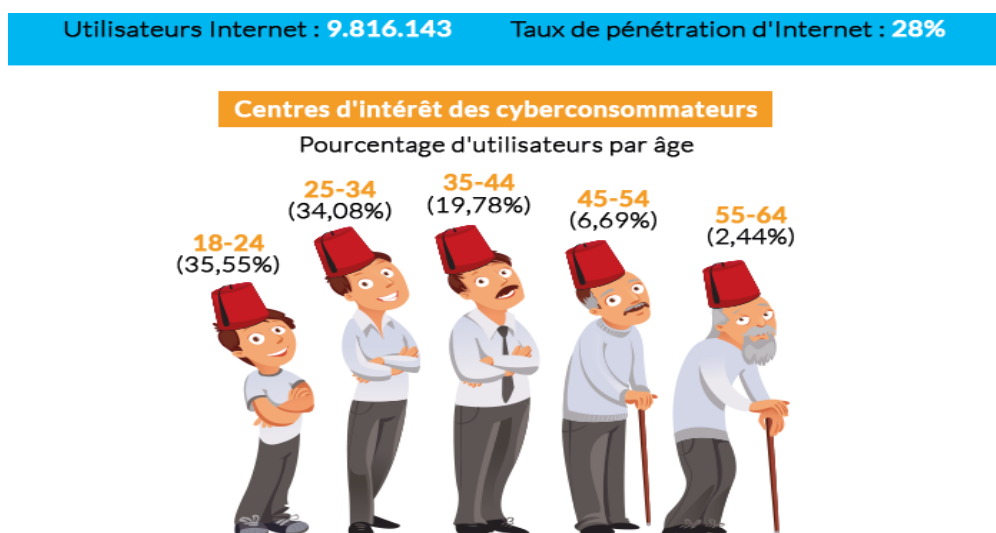


Figure I.4 : Chiffres clés par âge de l'e-commerce en Algérie année 2015

En matière de serveurs sécurisés, un autre maillon essentiel de la chaîne BtoC du commerce électronique, l'Algérie ne dispose que de 37 serveurs pour un million de personnes. Le seul indicateur positif pour l'Algérie est celui de l'efficacité de la poste. Elle obtient 68 points selon

le score de la CNUCED<sup>10</sup>, elle est dépassée légèrement par la Tunisie (69) et devance ainsi le Maroc (60) et l'Afrique du Sud (61).

À la fin de 2016, le nombre d'opérateurs inscrits au registre de commerce s'élevait à 1.890.257 opérateurs dont 1.717.382 personnes physiques (90,9%) et 172.875 personnes morales (9,1%). Le centre national du registre de commerce (CNRC), a certes mis en place une application pour la production de toutes les informations sur le registre de commerce, mais l'étape finale de la certification et le paiement électronique bute sur des problèmes techniques. La figure I.5 représente la répartition géographique publiée par la Marketplace Jumia Algérie sur l'utilisation de l'e-commerce.

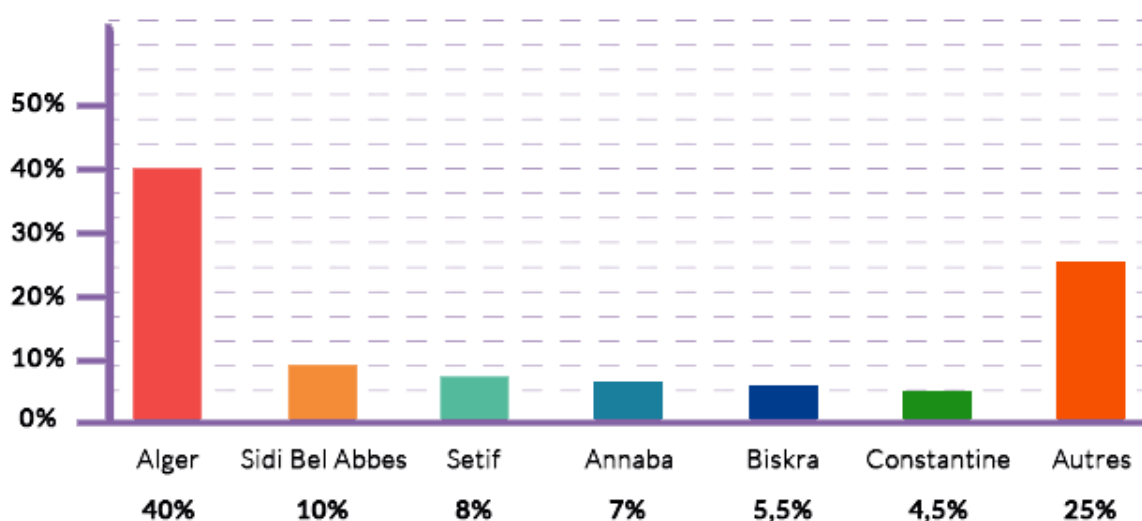


Figure I.5 : Répartition géographique de l'e-commerce en Algérie année 2015

## X.2. L'état du e-commerce algérien [7]

Malgré l'absence du paiement en ligne, les sites d'e-commerce se multiplient en Algérie. Les premiers sites du e-commerce algériens sont apparus à partir de 2012. eChrily.com fait partie des sites pionniers dans le secteur de vente en ligne. Spécialisé dans l'alimentation, eChrily.com, propose notamment des conserves, fruits et légumes, boissons, épicerie, crèmerie, etc. "Pour financer les achats sur le site il faut disposer de deux comptes utilisateurs. L'un sur le site epay.dz partenaire de eChrily qui fournit le côté e-paiement à travers des cartes de recharges de 1000 et de 2000 DA, et un autre compte sur le site du commerce électronique à partir duquel les articles sont commandés ".

<sup>10</sup>Conférence des Nations unies sur le commerce et le développement

Six mois plus tard, en janvier 2013, la toile algérienne accueillait deux nouveaux sites algériens de l'e-commerce : Tbeznyss.com, lancé le 12 janvier, spécialisé dans la vente de produits électroniques, comme eChrily.com, Tbeznyss.com utilise le paiement en ligne par compte virtuel prépayé epay.dz pour l'achat des marchandises. Un service de livraison à domicile a aussi été mis en place pour la wilaya d'Alger et sa périphérie.

Et Nechrifenet.com, créé le 16 janvier 2013, proposant des produits d'équipement maison, électroménager, puériculture, etc. En l'absence de cartes de crédit, Nechrifenet.com propose un paiement par virement ou par chèque. La livraison s'effectue à travers un réseau de points relais.

Sans oublier Ouedkniss.com le site des annonces classé à la 84<sup>ème</sup> place parmi les sites les plus visités en Algérie. Il enregistre entre 500 et 700 annonces par jour dans l'immobilier, les automobiles, l'informatique, les vêtements, les offre d'emploi...

### **X.3. Paiement électronique [8]**

Le paiement électronique (e-paiement) a été officiellement lancé en Algérie le mardi 4 octobre 2016. Il s'agit cependant que d'une première phase, puisque seuls quelques services seront à la disposition d'un nombre limité de personnes.

Les personnes possédant une carte de paiement électronique et muni de son mot de passe à quatre chiffres pourront utiliser le service d'e-paiement. Environ 1.3 million de détenteurs de cartes répartis dans onze banques (dont six banques publiques la BADR, CPA, BDL, BNA, BEA, CNEP, et cinq autres privées, Trust Bank Algérie, Natixis Algérie, Société Générale Algérie, Gulf Bank Algérie et Al Baraka.) .

Aujourd'hui, seuls les services de base proposés par les grandes entreprises sont disponibles pour les utilisateurs d'e-paiement. Le paiement électronique permet donc à l'heure actuelle de régler ses factures d'eau (SEAAL), de téléphone mobile (Ooredoo, Djezzy, Mobilis) et fixe (Algérie Télécom) ou encore acheter son billet d'avion sur Internet (Air Algérie), voire souscrire à une assurance en ligne (Amana Assurances). Un deuxième lot d'entreprises devrait cependant suivre ces grands facturiers.

## **XI. Conclusion**

Durant ce chapitre nous avons donné une vue générale sur le e-commerce mondiale et nationale, et nous avons aussi constaté le retard accumulé par l'Algérie dans ce type de commerce et les problèmes rencontrer , comme payer directement ses factures par une carte de

crédit ou tout simplement transférer de l'argent par un moyen électronique entre un client et un commerçant sur internet ou sur un espace commercial chez le commerçant.

L'Algérie en étant un pays émergent cherche à convoiter de plus en plus près le train de l'évolution (économique, technologique), est parmi eux le ministère du commerce, le ministère du TIC et la banque d'Algérie qui ont lancé ce nouveau type de paiement en 2016. Le second chapitre sera dédié à l'e-paiement.

# ***Chapitre II***

## ***Le paiement électronique***



## **I. Introduction**

Durant les dernières années la popularisation des cartes bancaires et de l'internet a favorisé l'explosion du e-commerce qui a permis au paiement électronique de gagner d'avantage la vie quotidienne. De la simple carte magnétique développée dans les années 70 à l'ère des smartphones et des objets connectés, les hommes ne cessent de créer et de se développer, la nécessité de gagner du temps et de sécuriser des transactions pousse les ingénieurs à développer toujours de nouveaux moyens de paiement plus sûr et plus performant.

Dans ce chapitre nous allons parcourir les différents moyens du paiement électronique matériels et logiciels et nous détaillerons notre domaine d'étude qui est le m-paiement.

## **II. Définitions**

Nous allons présenter dans ce qui suit deux définitions qui nous semblent importantes pour bien comprendre la suite du chapitre.

### **II.1. E-paiement**

Appelé aussi Paiement en ligne est l'utilisation d'un système électronique pour un échange d'argent. Il s'agit des paiements que l'on réalise sur Internet ou via des réseaux de télécommunications, générés à partir soit d'un ordinateur, soit d'un téléphone mobile. [9]

### **II.2. M-paiement**

Le paiement mobile ou Mobile paiement fait partie du e-paiement, il permet aux consommateurs de régler des achats depuis un téléphone mobile. Cette transaction sera alors débitée soit sur le compte lié à la carte bancaire, soit sur la facture opérateur ou soit sur un porte-monnaie électronique. [10]

## **III. Les modes du paiement**

On peut répertorier les moyens de paiements en deux catégories, les moyens de paiement direct et des moyens de paiement indirect (en ligne).

### **III.1. Modes de paiement direct [11]**

Les moyens de paiement dit direct du point de vue client , c'est lorsqu'il paie directement chez le commerçant en utilisant des moyens traditionnels comme le cash et le

chèque, mais aussi des moyens de paiement récent comme les cartes bancaires et le paiement mobile.

### **III.1.1. Cache**

Ce mode de paiement classique est le plus simple et le plus sûr et il ne contient aucune charge à payer contre le transfert d'argent. Néanmoins cette méthode n'est pas gratuite ; 10 milliards de billets sont détruits et remplacés, avec le coût de la production d'un billet et l'assurance contre les incendies, sécuriser leur transport, coutent des milliards de dollars chaque année pour l'état.

### **III.1.2. Les chèques**

Le chèque est un moyen de paiement scriptural utilisant le circuit bancaire. Il est généralement utilisé pour faire transiter de la monnaie d'un compte bancaire à un autre, cette méthode a fait ses preuves depuis déjà deux siècles, elle est très répandue aux pays occidentaux et au Japon, mais elle implique beaucoup d'infrastructures et de moyens pour le traitement et la compensation des chèques.

### **III.1.3. Les cartes bancaires**

Les cartes de crédit se présentent aujourd'hui comme le moyen le plus privilégié sur Internet pour tous les commerces à distance mais aussi dans le commerce direct chez le commerçant, il suffit de passer sa carte de crédit dans le terminal (TPE<sup>11</sup>) et de valider son code PIN pour que la transaction soit faite. Il faut noter quand même que les cartes de crédit ne deviendront pourtant jamais un moyen de paiement universel. Les prélèvements qu'elles imposent entre 2 et 5% de la transaction ne sont endurés qu'en l'absence alternative plus économique. C'est d'ailleurs pour cette raison que les trois quarts des transactions existants sur le Web sont payées par chèque.

## **III.2. Modes du paiement indirect**

Le paiement indirect est le paiement sur internet, plusieurs moyens ont vu le jour mais on peut retenir que les plus réussis et surtout les plus utilisés, dans ce qui suit nous allons présenter les moyens de paiement les plus répandus sur internet :

---

<sup>11</sup>Le **Terminal de Paiement Électronique** est un équipement électronique utilisé par les commerçants/ prestataires du service et qui assure, à travers la lecture des cartes interbancaires de paiement, l'encaissement du montant des ventes ou prestations du service offert aux clients détenteurs de cartes interbancaires de paiement.

### **III.2.1. Le Porte-monnaie électronique**

On peut distinguer deux types de porte-monnaie électronique le porte-monnaie matériel et le porte monnaie logiciel :

- 1) **Le porte-monnaie électronique matériel** : le porteur du porte-monnaie électronique est muni d'une carte à puce dont il peut charger en monnaie électronique. La puce stock l'identifiant du titulaire ainsi que le montant chargé. Comme la carte bancaire classique, le porte-monnaie électronique doit être introduit dans un lecteur de carte. Toutefois, le porteur n'aura pas à saisir un code personnel, exemple: Veritas, Skrill et Moneo.
- 2) **Le porte-monnaie électronique virtuel** : est un dispositif sécurisé installé sur des appareils électroniques portables (téléphones mobiles principalement) permettant d'initier un virement de son compte vers celui d'un fournisseur, via un terminal de paiement installé dans le magasin. Dans ce cas il s'agit d'un substitut à la carte bancaire traditionnelle, l'appareil ne contenant pas de monnaie mais permettant simplement d'accéder à son compte bancaire de façon sûre, exemple : Google Wallet et Paypal.

### **III.2.2. Le chèque électronique**

Les chèques électroniques (e-chèques) sont destinés aux échanges entre entreprises et aux échanges dans lesquels le client veut profiter des délais de paiement traditionnel plutôt que d'effectuer un paiement immédiat. En utilisant les e-chèques, les entreprises peuvent non seulement effectuer les paiements mais également joindre des détails concernant le versement par l'intermédiaire d'un ensemble de transactions EDI<sup>12</sup>. A l'instar du porte-monnaie électronique, l'acheteur doit s'inscrire auprès d'une institution financière pour utiliser les e-chèques. La banque peut exiger une carte de crédit ou un compte bancaire pour approvisionner les e-chèques. Une fois le compte créé, l'acheteur peut envoyer un e-chèque au vendeur par e-mail.

### **III.2.3. Le numéro à 16 chiffres de la carte bancaire**

L'image de la carte de paiement peut être utilisée pour régler des achats grâce au numéro apparent de la carte bancaire mais également par le biais d'une carte virtuelle qui génère un numéro de carte à 16 chiffres.

---

<sup>12</sup>L'**Échange de Données Informatisées (EDI)**, ou en version originale *Electronic Data Interchange*, est le terme générique définissant un échange d'informations automatique entre deux entités à l'aide des messages standardisés, de machine à machine

- 1) **L'utilisation du numéro apparent** : cette solution est prédominante en matière de paiement sur les réseaux. L'utilisateur communique au vendeur le nom du porteur de la carte, son numéro de carte à 16 chiffres ainsi que sa date de validité et le cryptogramme visuel<sup>13</sup> (ces informations sont visibles sur la carte bancaire). Le système informatique du commerçant répercute ces informations à la banque émettrice. Puis l'établissement émetteur crédite le compte du vendeur et débite le compte du porteur.
- 2) **La carte virtuelle dynamique** : le système de sécurisation des paiements basé sur l'utilisation de la carte virtuelle dynamique, remplace la saisie du numéro à seize chiffres de la carte physique par saisie d'un numéro apparent dynamique de même longueur en temps réel par le serveur de la banque, ce type de carte s'utilise de la même manière que la carte bancaire classique.

#### **III.2.4. E-paiement par téléphone portable**

Appelé aussi m-paiement à susciter l'intérêt des développeurs dès la fin des années 90 vue l'importance du téléphone portable, alors que les technologies étaient primitives les ingénieurs tentaient de développer ce type de paiement mais ça restait dans le cadre des laboratoires. Jusqu'à l'arrivée des Smartphones qui ont permis à ce type de paiement à être la technologie du futur et être un concurrent réel pour la carte bancaire (le m-paiement est détaillé dans la suite du chapitre voire le M-paiement).

### **IV. Les critères du paiement électronique [11]**

Lors du paiement sur le réseau le client comme le commerçant ont la même peur. Le client a peur de payer et de rien recevoir, le commerçant à peur de livrer et de ne pas être payé. Donc, une méthode de qualité pour le paiement électronique doit apporter la confiance et doit sécuriser les deux parties tout en gardant le maximum de souplesse et de confort dans l'utilisation, on a donné dans ce qui suit quelques critères de base :

#### **IV.1. Identifier les parties concernées**

Le vendeur doit s'assurer de l'identité de l'acquéreur et sa solvabilité et l'acheteur doit pouvoir identifier le vendeur auprès d'un organisme digne de foi, qui se porte garant vis-à-vis de l'acheteur. Le seul souci légitime du commerçant est d'être payé. Le système doit donc être

---

<sup>13</sup> Il s'agit d'une combinaison de trois chiffres inscrit sur le panneau au verso de la carte bancaire portant par exemple le nom de CVV2 pour le réseau Visa, de CVC2 pour le réseau MasterCard et de CVN 2 pour les cartes nationales (en France).

en mesure de fournir cette garantie tout en masquant la situation du compte de l'acheteur et l'acheteur lui aussi ne souhaite pas que son identité bancaire soit révélée au commerçant.

#### **IV.2. Confidentialité de la transaction**

La substance de la transaction ne doit être connue que par l'acheteur et le commerçant. Mais, il est impératif que l'acheteur soit en mesure de conserver un document valable juridiquement certifiant de façon définitive toutes les caractéristiques de la transaction. Dans l'e-paiement un document numérique certifié peut faire office d'un document juridique (Cf. VII.2 et VII.3).

#### **IV.3. Intégrité du procédé**

L'intégrité assure qu'aucune modification n'est apportée aux données et surtout à la trace de la commande pendant le transfert, jusqu'à la validation de la transaction financière. Le mot modification englobe en fait, la duplication, l'insertion, l'effacement d'une partie de l'information et le changement dans l'ordonnancement des informations.

#### **IV.4. Non-répudiation**

Elle permet d'éviter à ce que l'une des deux parties nie la transmission ou la réception de l'information lors du procédé de commande d'échange des données ou du paiement électronique sur le Web.

#### **IV.5. Contrôle d'accès**

Assure que seulement des personnes autorisées peuvent obtenir accès lors du paiement. L'objectif de ce critère est de protéger les informations.





### **V. La monétique [12]**

La monétique est l'ensemble des traitements électroniques, informatiques et télématiques nécessaires à la gestion des cartes bancaires ainsi que des transactions associées.

Notre travail consiste à créer une application mobile dédiée au paiement électronique en utilisant la technologie NFC (il sera développé dans le titre VI.2.5), cette dernière doit fournir à l'utilisateur la possibilité de payer dans des TPE, or pour bien comprendre son fonctionnement, on va présenter dans ce qui suit les différentes étapes du paiement par carte bancaire dit aussi monétique, qui a les mêmes étapes que le m-paiement.

### V.1. les acteurs

Lorsque nous parlons de monétique, il y a quatre acteurs principaux :

-  **Le porteur** est une personne physique qui porte la carte de paiement. Dans une transaction bancaire, il s'agit du client.
-  **L'émetteur** est un organisme financier ou assimilé qui émet la carte de paiement. Dans une transaction bancaire, l'émetteur est la banque du client.
-  **L'accepteur** est une personne physique ou morale qui accepte le moyen de paiement grâce à un système accepteur. Dans une transaction bancaire, l'accepteur est assimilé au commerçant équipé d'un terminal de paiement électronique (TPE).
-  **L'acquéreur** est l'organisme financier ou assimilé qui va acquérir les données de la transaction. Dans une transaction bancaire, il s'agit de la banque du commerçant.

### V.2. Les relations entre les acteurs

- **Le contrat porteur** est le contrat liant l'émetteur et le porteur. L'émetteur fournit un moyen de paiement sûr et facile à utiliser. Le porteur en utilisant ce moyen de paiement est solvable des montants des transactions réalisées. L'émetteur quant à lui assure la sécurité du système bancaire et fournit une assurance en cas d'utilisation frauduleuse du moyen de paiement. Dans ce type de situation, l'émetteur va rembourser le porteur du montant des transactions frauduleuses.
- **Le contrat commerçant** lie l'acquéreur et l'accepteur du moyen de paiement. L'acquéreur fournit à l'accepteur un système accepteur contre un pourcentage fixe du montant des transactions effectuées. Le système accepteur va permettre d'effectuer la transaction : lecture de la carte, saisie du code pin, sauvegarde de la transaction... Typiquement le système accepteur utilisé fournit un terminal de paiement électronique (TPE). Par ailleurs, l'accepteur choisit le système accepteur proposé par l'acquéreur.

### V.3. Les transactions bancaires

En apparence la transaction bancaire est très simple, il suffit juste de passer la carte dans le terminal de paiement pour générer la transaction (débité le compte du client et accréditer le compte du commerçant). Mais en réalité c'est plus compliqué que ça, le processus de paiement passe par plusieurs étapes, donc nous allons présenter les différentes étapes dans ce qui suit :

#### V.3.1. Le processus général

Une transaction bancaire est définie par les étapes suivantes comme il est représenté dans la figure II.1 :

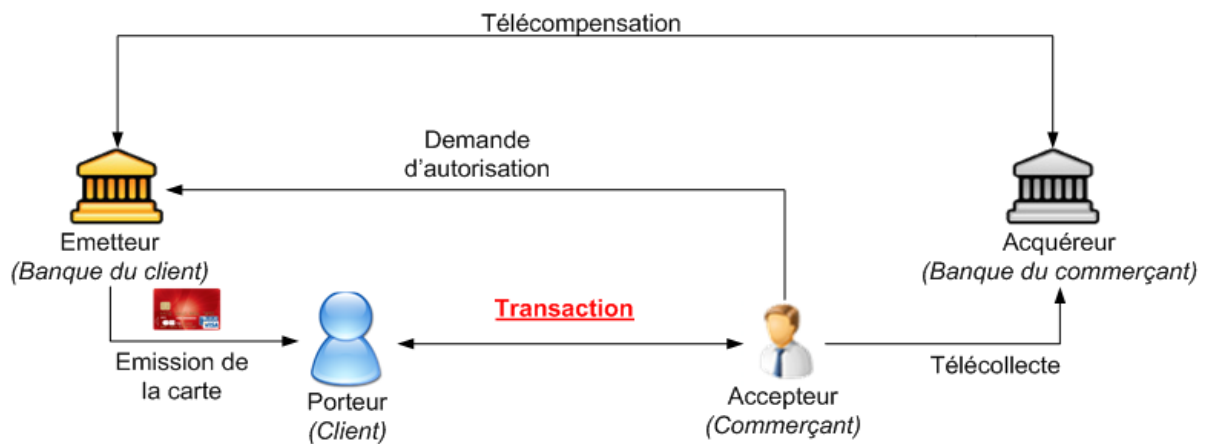


Figure II.1 : Schéma général d'une transaction bancaire

1. Le client crée un compte bancaire chez une banque, la Banque envoie la carte de paiement associée au compte avec le code PIN.
2. Le client va chez le commerçant, choisit un article et le paye. C'est la **transaction**. Parfois il peut y avoir des demandes d'autorisation pour vérifier la solvabilité du compte et si la carte est valide.
3. Après la transaction c'est le lecteur de carte qui va transmettre les données de plusieurs transactions. C'est la **télécollecte**.
4. Enfin, une fois la télécollecte effectuée. Les deux banques communiquent entre elles pour effectuer la **télé-compensation**. C'est-à-dire qu'un compte va être débité et l'autre crédité.

**V.3.2. La transaction**

Globalement quand on achète un bien ou un service, la transaction se déroule en plusieurs étapes. Chez le commerçant, nous allons à la caisse où nous tendons notre carte de paiement (voir la figure II.2).

1. Le commerçant la prend, saisi sur le terminal de paiement électronique (TPE) le montant de la transaction et insert la carte.
2. Le TPE fait des vérifications sur la carte. Il lit principalement le PAN (Permanent Account Number). En cas d'impossibilité de lecture, la carte est dite muette par le terminal de paiement.
3. Le porteur saisit son code PIN. En cas de trois essais, sa carte peut être confisquée et bloquée. Le commerçant peut toutefois forcer la transaction mais, il n'est pas garanti sur la transaction.
4. À cette étape, il peut y avoir une demande d'autorisation.
5. Lorsque la demande d'autorisation est acceptée, le TPE enregistre la transaction dans un fichier.
6. On imprime les deux tickets clients et commerçants.
7. La transaction est terminée.



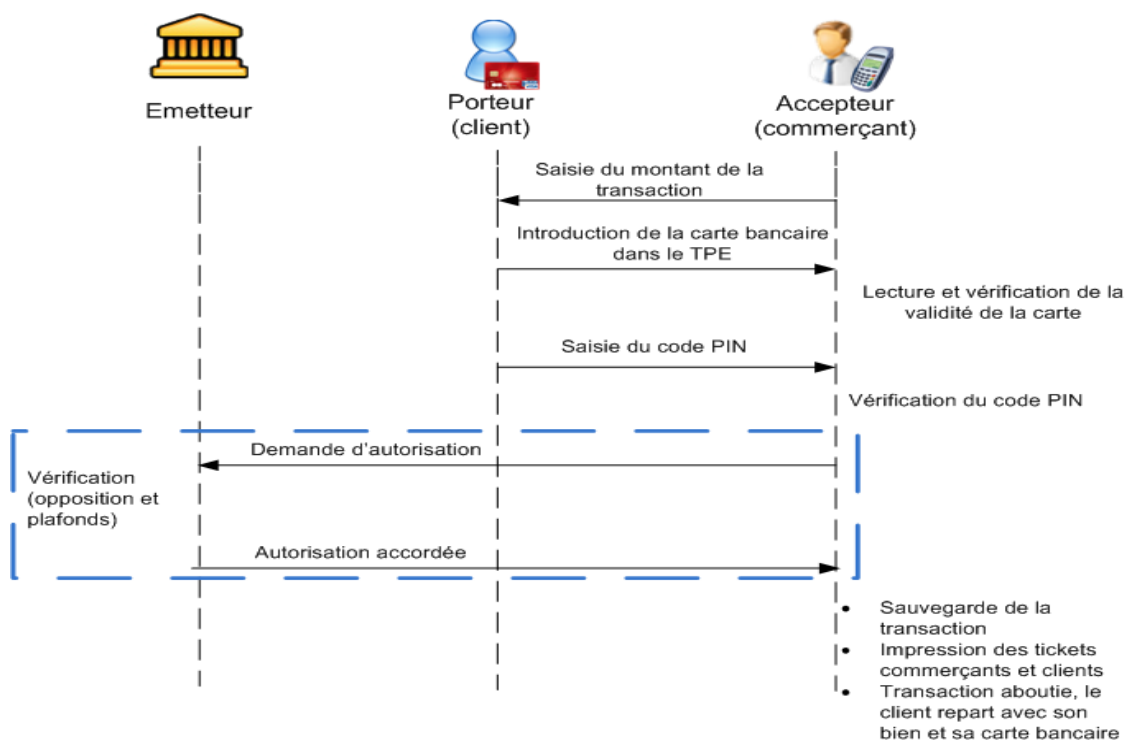


Figure II.2 : les étapes d'une e-transaction

### V.3.3. La télécollecte

Après la transaction, il y a le processus de la télécollecte. Ce processus consiste à transmettre les fichiers enregistrés sur le terminal de paiement à la banque acquéreur (la banque du commerçant).

Cela est effectué dans un intervalle de temps régulier à un moment où la transmission de ces informations ne gêne pas les autres opérations bancaires. Généralement, ces traitements sont effectués pendant la nuit. Cela dépend du contrat commerçant. Une fois téléchargés, les fichiers sont supprimés du TPE (voir la figure II.3).

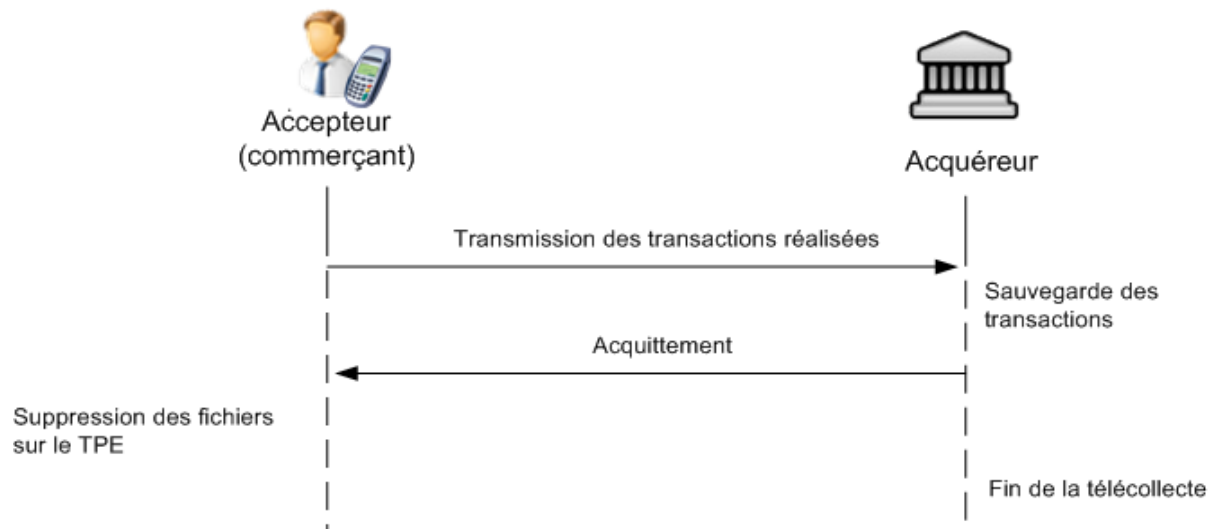


Figure II.3 synthèse de la télécollecte

#### V.3.4. Télé-compensation

Après la télécollecte, il va y avoir la compensation des deux comptes bancaires mis en jeu dans la transaction. Le compte porteur va être débité du montant de la transaction et le compte commerçant sera crédité du même montant. Cette étape est la télé-compensation.

L'acquéreur va transmettre à une plateforme de compensation les données de la transaction. Cette dernière sauvegarde l'information.

À une heure fixée, elle s'occupe alors de transmettre l'opération de débit du compte porteur au serveur émetteur et l'opération de crédit du compte accepteur sur le serveur acquéreur. Elle attend un acquittement de leurs parts (voire la figure II.4).

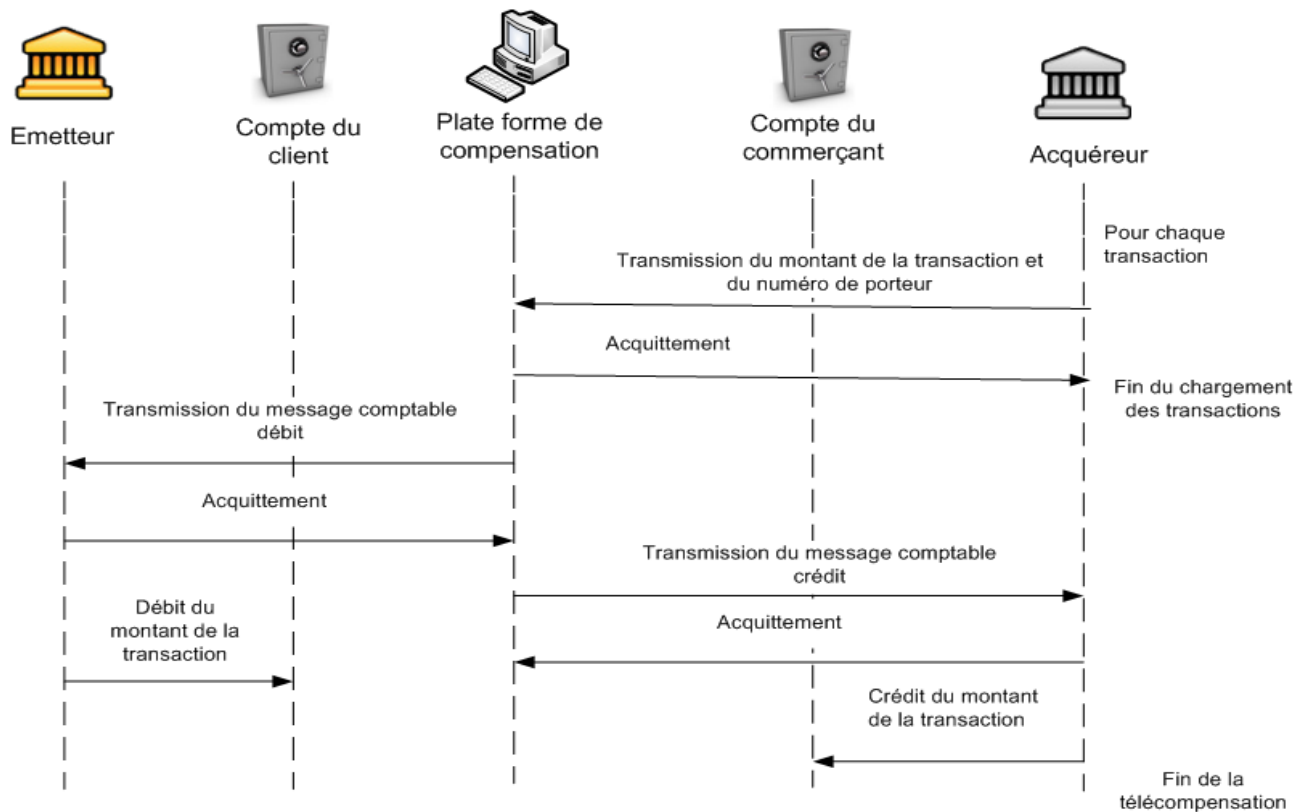


Figure II.4 : synthèse de la télé-compensation

## V.4. La Sécurité dans des cartes bancaires

Le système bancaire dont les cartes bancaires sont sécurisées par différents moyens, afin de se protéger de plusieurs types de menaces, dans ce qui va suivre nous allons aborder certaines menaces puis on va donner quelques méthodes de sécurité.

### V.4.1. Les menaces

On constate les types de menace suivants :

- Le fishing, on envoie un mail en se faisant passer pour la banque du client et on récupère les codes d'accès.
- Le skimming consiste à modifier un appareil. On va mettre une micro caméra de surveillance ou un boîtier qui va lire la carte et sauvegarder les données.
- Bien entendu, le vol de la CB (carte bancaire). Ensuite, le voleur peut la copier s'il possède les compétences adéquates.

- La contrefaçon de CB étrangère généralement –car sans puce. Pour contrer les contrefaçons, des algorithmes de DDA<sup>14</sup> sont utilisés. Cela permet une identification dynamique.
- Par rapport aux transactions sur le net, il y a de nombreux générateurs de numéro de CB et on peut aussi récupérer les tickets de caisse chez le commerçant pour connaître toutes les informations liées à la carte.

### V.4.2. Sécurité interne de la carte bancaire

On distingue un dispositif physique sur la carte avec la carte à puce (SE<sup>15</sup>). Brouillage et chiffrement du bus et des données, impossibilité d'attaquer et d'interroger directement la carte pour obtenir le code PIN ou d'autres informations. La carte en elle-même peut être verrouillée après trois échecs de la saisie du code PIN.

### V.4.3. Sécurité Fonctionnelle (externe à la carte bancaire)

Au niveau fonctionnel, les banques possèdent une liste des cartes stockées dans des fichiers dans leurs systèmes informatiques. Cette liste est présente sur les serveurs émetteurs des banques. Elle est consultée par le système à chaque demande d'autorisation.

En outre, les tickets clients<sup>16</sup> ont été améliorés en retirant le code complet de la carte. Auparavant, tout était en clair et quiconque pouvait récupérer les numéros des cartes de paiement et les utiliser pour payer sur Internet.

### V.4.4. Réseau

Au niveau des communications réseaux, le x25<sup>17</sup> garantie l'intégrité des données et chiffre la communication. La communication est faite en point à point. Il n'y a pas de possibilité d'avoir un cas de sniffing<sup>18</sup> du réseau.

---

<sup>14</sup>Dynamic Data Authentication (DDA) : authentification dynamique des données, est un protocole de chiffrement d'un nombre de 32 bits avec la clé privée de la carte

<sup>15</sup>Un élément sécurisé (SE) est une puce séparée qui contient un processeur sécurisé, un stockage inviolable et la mémoire d'exécution. Ce processeur est différent du processeur hôte ou du processeur de l'ordinateur. Son seul but est de permettre des transactions sécurisées. Cet élément sécurisé contient donc des applications qui s'appuient sur des clés sécurisées fonctionnant à l'intérieur de ce processeur sécurisé

<sup>16</sup> Les tickets clients dis aussi les tickets de caisse, au paravent, lors du paiement par carte bancaire le terminale imprime un petit ticket qui est garder par le client, ce ticket contient les informations sur la transaction dont le numéro à 16 chiffre de la carte.

<sup>17</sup>X.25 est un protocole de communication normalisé par commutation de paquets en mode point à point offrant de nombreux services

<sup>18</sup> Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisée par les pirates pour espionner le trafic sur le réseau ;

## **VI. Le m-paiement**

**VI.1. Les différents modes de paiement mobile :** À l'heure actuelle, il existe trois grandes catégories de paiement mobile :

### **VI.1.1. Paiement à distance**

Proche de l'e-commerce, c'est le mode de paiement le plus répandu. Il suffit au consommateur de se connecter à Internet depuis son mobile et de régler ses achats directement sur Internet à travers une application dédiée ou un navigateur permettant le paiement en ligne (comme s'il effectuait un paiement via son ordinateur).

### **VI.1.2. Paiement de proximité**

Encore peu utilisé, ce mode de paiement est en cours de développement. Paiement qui repose majoritairement sur deux technologies : le QR code et la Near Field Communication (NFC). Pour réaliser son paiement, l'utilisateur doit passer son téléphone mobile sur une borne de paiement puis valider son règlement par un code. Pour que l'opération soit valide, il faut que le mobile soit doté d'un système de puce et que le commerçant ait préalablement installé une borne de paiement.

### **VI.1.3. Paiement de mobile à mobile**

Le transfert d'argent de mobile à mobile est particulièrement développé dans les pays en voie de développement, où de nombreuses personnes n'ont pas de compte bancaire (Express Union), en France elle se développe depuis peu (Kwixo, S-Money5, LemonWay ou Paypal).

### **VI.1.4. Autre type de m-paiement**

On pourrait également ajouter un autre type de paiement mobile qui existe via les applications de gestion des comptes bancaires des banques. En effet, il est possible d'effectuer rapidement un virement bancaire vers un compte tiers via son mobile.

## **VI.2. Les technologies utilisées dans le M-paiement**

Selon les services que le consommateur utilise pour réaliser les paiements sur son mobile, différentes technologies ont été mises en place. Les technologies suivantes sont par exemple utilisées pour le paiement mobile :

### **VI.2.1. Le SMS (mode de paiement mobile à distance)**

Disponible sur tous les téléphones, simple d'utilisation et ne nécessitant pas d'investissement de la part du commerçant, c'est un moyen pratique pour les consommateurs et commerçants. En échange d'un SMS, l'utilisateur reçoit sur son téléphone l'application ou le service qu'il a acheté. Il paye donc via sa facture mobile. L'opérateur reverse ensuite un certain quota au fournisseur d'origine.

**Exemple** : les publicités télévisées proposant des sonneries de téléphone et des jeux.

### **VI.2.2. Square<sup>19</sup>(mode de paiement mobile de proximité)**

Gratuite et ne nécessitant aucun téléchargement de la part du consommateur, cette technologie permet aux commerçants qui ne disposent pas de terminal de carte bancaire de pouvoir cependant accepter le paiement par carte bancaire en utilisant un téléphone (iPhone, iPad ou terminal Android) comme lecteur de carte. Il suffit de brancher sur la prise jack du téléphone un petit boîtier qui permettra de lire la carte bancaire du consommateur, comme s'il s'agissait d'un lecteur de carte normal.



*Figure II.5 : photo d'un square avec une prise Jack*

### **VI.2.3. Bluetooth**

La technologie Bluetooth utilise une technique radio à courte distance destinée à simplifier les connexions entre les appareils électroniques. Le BLE et le NFC offrent des débits et une consommation électrique similaires, mais les portées sont très différentes (le Bluetooth peut atteindre 50 m, le NFC 4cms).

La technologie BLE permet l'arrivée de plusieurs nouveautés dans le domaine de la vente comme le fait de détecter la présence des clients, de les identifier, de leurs proposer des

---

<sup>19</sup>Square est une entreprise américaine spécialisée dans le paiement mobile et le paiement électronique. Elle est basée à San Francisco. Elle est fondée en 2009 par Jack Dorsey et Jim McKelvey.

offres personnalisées ou encore de les guider en intérieur (en fonction de la balise qu'ils captent le mieux et de l'intensité du signal).

#### **VI.2.4. Code QR**

Ce mode s'utilise à proximité et à distance. Il s'agit d'un code-barres en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le code.

QR (Quick Response) signifie que le contenu du code peut être décodé rapidement après avoir été lu par un lecteur de code-barres, un téléphone mobile ou un Smartphone. Son avantage est de pouvoir stocker plus d'informations qu'un code-barres et surtout des données directement reconnues par des applications, permettant ainsi de déclencher facilement des actions dont le paiement mobile.

Le principe est simple : il faut télécharger une application qui permet de scanner avec son téléphone, ouvrir un compte sur cette dernière (exemple Flashiz) et l'alimenter en le liant à une carte de crédit (possibilité de rechargement automatique), scanner le QR code présenté par le commerçant et valider pour que la transaction soit réalisée.



*Figure II.6 : exemple de code QR*

#### **VI.2.5. Le NFC (Near Field Communications)**

Le NFC est une technologie de communication sans fil par radiofréquence qui permet l'échange de données entre un lecteur et une cible NFC ou un terminal sur une distance de quelques centimètres grâce à des puces spécifiques insérées côté émetteurs. [13]

La technologie NFC a eu un grand succès au grand public, dès la popularisation des smartphones qui ont des puces embarquées NFC, avec l'apparition de Apple-Pay l'application de paiement d'Apple, qui a connu un grand succès dans les Etas Unis plusieurs fabricants dont Google se lance dans ce type de paiement en lançant Google Wallet. Le NFC apporte plusieurs avantages comme la rapidité et la fluidité lors des passages en caisse mais aussi de la sécurité on utilisant l'authentification biométrique (reconnaissance faciale et vocale et l'identification

par l'empreinte digitale). Ce qui nous a poussés à choisir de développer notre application en se basant sur cette technologie.

Le NFC fonctionne selon 3 modes :

- un mode émulation de carte (le terminal mobile émule le fonctionnement d'une carte bancaire) ;
- un mode lecteur (le terminal devient un lecteur de carte sans contact) ;
- enfin un mode peer-to-peer (les données s'échangent entre 2 terminaux mobiles).

Le NFC a une portée délibérément courte (quelques centimètres), ce qui permet de cibler précisément un terminal de paiement, une balise ou un appareil et d'éviter de capter tous ceux aux alentours (comme ceux par exemple des autres clients). L'utilisateur fait donc survoler son mobile à quelques centimètres de la zone à détecter.

- **Pour les paiements des petites sommes :** le commerçant saisit le montant sur le terminal et le consommateur présente son mobile à moins de 4 cm du lecteur de carte. Un bip et une lumière verte signalent alors que la transaction est effectuée. Le consommateur n'a donc même pas à déverrouiller ou à manipuler l'interface de son téléphone.
- **Pour les paiements de grandes sommes :** Après avoir présenté son mobile devant le terminal, le consommateur doit saisir son code confidentiel sur son téléphone mobile puis le présenter de nouveau devant le lecteur carte pour conclure le paiement.

La technologie NFC se développe avec l'augmentation du nombre de terminaux de paiement sans contact chez les commerçants (348.000 terminaux de paiement sont dotés de NFC en 2016, soit 29% de 1,2 million de machines en France) et l'augmentation du nombre de téléphones équipés avec cette technologie.

### VI.2.6. Les avantages du paiement par puces NFC

Nous avons donné dans ce qui suit quelques avantages du paiement avec la technologie NFC :

- 1) **Les commerçants/distributeurs :** Souhaitent ramener le consommateur dans les magasins, recréer un contact, de la proximité physique, lui offrir des services, des informations, des promotions, qu'on ne peut trouver nul part ailleurs et garder une relation forte avec son consommateur.



2) **Les banques** : à travers le paiement mobile sans contact les banques ont pour objectif de répondre aux nouveaux besoins de leurs clients et de profiter des avantages liés à la dématérialisation comme :

- Les paiements mobiles permettent de réduire les coûts pour les banques liés à l'utilisation des espèces ou des chèques tout en accroissant les revenus tirés des commissions (notamment en augmentant le nombre de transactions).
- La satisfaction du client peut être améliorée en offrant de nouveaux services aux clients.
- Ces nouveaux services à valeur ajoutée permettent de créer une barrière à l'entrée face à la compétition et même de gagner des parts du marché.
- Les banques installent l'infrastructure de terminaux de paiement sans contact chez les commerçants. Cette infrastructure fonctionne aussi bien pour des cartes de paiement standard, des cartes sans contact et des mobiles NFC. Elles distribuent donc également des cartes de paiement sans contact.

3) **Les entreprises** : les entreprises du monde entier avaient recueilli près de 633 milliards de dollars en 2014, selon la société de technologie mobile des données de recherche Portio ce chiffre a été multiplié par 7 en 2015. Les entreprises qui profitent d'options de paiement mobiles et NFC bénéficient d'une clientèle variée qui contribue à l'augmentation du chiffre d'affaires.

4) **Les opérateurs télécom** : associés aux banques ont pour « *business model* » le partage des commissions bancaires à chaque transaction de proximité sur le mobile. Leur arme fatale est la présence du « *Secure Element* », l'endroit où sont gérées la sécurité des données et des transactions sur la SIM du mobile (en accord avec presque toutes les banques) pour assurer la sécurité des transactions. Ils poussent donc également le déploiement des mobiles NFC.

5) **Pour le client** : cette technologie offre plusieurs avantages, comme :

- Gain de temps lors du paiement ;
- Possibilité de gérer ces achats et les suivre en temps réel ;
- En cas de vol ou de perte du terminal on peut bloquer le compte du client par un simple appel, et aussi le géo-localiser ;
- Éviter de transporter plusieurs cartes bancaires ou de l'argent liquide sur soi.

- Accroître la sécurité du paiement en ajoutant des modules d'authentification biométrique, déjà existant dans l'appareil comme la reconnaissance faciale et l'authentification par empreintes digitales.

## **VII. Les techniques de sécurités dans l'm-paiement [11]**

Cette partie va concerner l'usage des protocoles de sécurité dans le milieu bancaire, où la sécurité des échanges est cruciale. Parmi les moyens utilisés nous avons des protocoles cryptographiques, la datation, l'identification et le protocole SET et SSL... dans ce qui suit nous allons présenter ces différentes techniques.

### **VII.1.La cryptographie**

La cryptographie c'est la science de préserver la confidentialité des messages alors que la cryptanalyse est l'art de décrypter des messages chiffrés.

Il existe 2 grandes familles de méthodes de cryptage : le cryptage symétrique et le cryptage asymétrique.

#### **VII.1.1. Cryptage symétrique**

Le cryptage symétrique, aussi appelé cryptage à clé secrète ou privée, est la plus ancienne forme de chiffrement. La caractéristique de ce chiffrement est l'usage de la même clé pour le chiffrement et pour le déchiffrement (type Chiffre de César, Vigenère ...).

Pour crypter un message, on applique une opération (algorithme) à l'aide de la clé. Ce type de cryptage est très sûr en théorie (l'utilisation d'une clé d'une longueur au moins égale à celle du message, assure en effet l'inviolabilité du message).

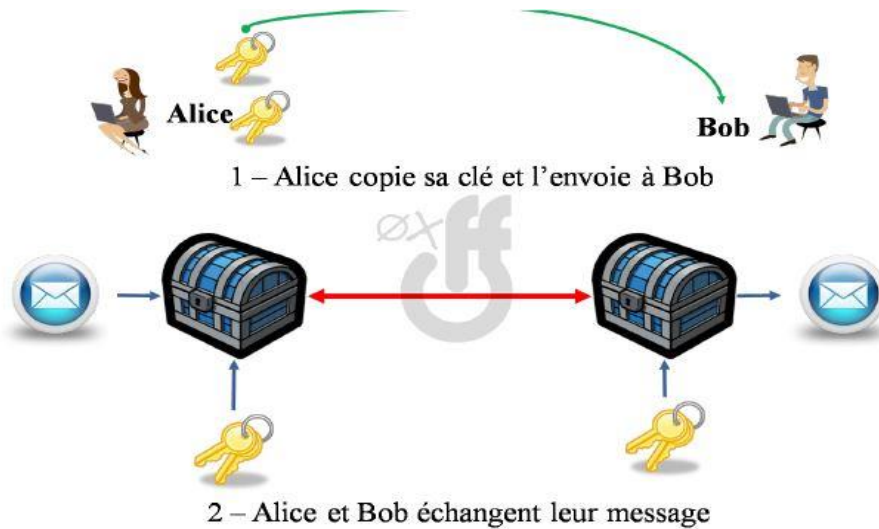


Figure II.7 : schéma illustrant le fonctionnement du chiffrement symétrique.

Cependant, en pratique, il se pose un problème majeur : comment échanger de manière sûre les clés ? C'est le principal défaut de ce système.

### VII.1.2. Cryptage asymétrique

Un cryptage asymétrique est un algorithme pour lequel, le cryptage et le décryptage sont des fonctions différentes et qui fait intervenir deux clefs différentes. En fait, les procédés du type DES sont également appelés procéder « à clef privée » car la confidentialité des informations est conditionnée au secret qui entoure la clef de cryptage.

On peut comparer ce système de chiffrement au fonctionnement d'un cadenas.

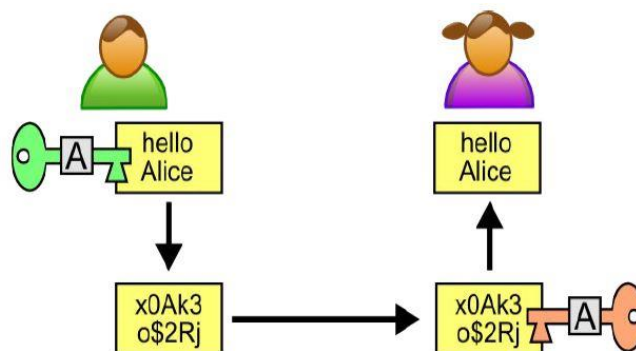


Figure II.8 : schéma illustrant le fonctionnement du chiffrement asymétrique

Alice dispose de 2 clés : une clé publique (verte ici, c'est elle qui fait office du « cadenas ») et une clé privée (rouge ici, la clé du « cadenas »). Ainsi, Bob peut chiffrer un message à

l'aide de la clé publique et seule Alice pourra le déchiffrer avec sa clé secrète (elle est la seule à la posséder).

L'inverse, Alice peut coder un message à l'aide de sa clé privée et Bob peut le déchiffrer à l'aide de la clé publique : ce mécanisme est utilisé par la signature numérique pour authentifier l'auteur d'un message. Ce type de cryptographie est basé sur l'existence de fonctions à sens unique : ce sont des fonctions faciles à appliquer dans un sens (chiffrement), mais très difficiles « d'inverser » (déchiffrement). L'exemple le plus utilisé dans les cartes bancaires est l'algorithme RSA<sup>20</sup>.

## **VII.2. La signature électronique**

Le concept de la signature électronique a été introduit par Diffie et Hellman en 1992. Si le détenteur des clefs asymétriques publie une de ces clefs asymétriques et s'engage à garder l'autre secrète, le cryptage d'un document électronique réalisé par cette clef asymétrique privée constitue une signature juridiquement acceptable de ce document. On authentifie le document en le décryptant par la clef asymétrique publique. La probabilité d'erreur est minime surtout avec des clefs sur 768 bits.

La signature électronique d'un document n'est généralement pas le cryptage de tout le document mais d'une forme abrégée du message, de taille fixe, appelée : ***L'empreinte électronique*** « Digest en Anglais ». Cette empreinte est réalisée par une fonction de *hachage* à sens unique.

Plusieurs fonctions de hachage sont couramment employées mais le MD5<sup>21</sup> et SHA-1<sup>22</sup> sont les deux fonctions de hachage les plus populaires.

---

<sup>20</sup> Un des algorithmes asymétriques les plus utilisés est l'algorithme RSA, du nom de ses créateurs Ronald Rivest, Adi Shamir et Leonard Adleman, en 1977). Il est basé sur une propriété simple des nombres premiers.

<sup>21</sup> **L'algorithme MD5**, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message). Il a été inventé par Ronald Rivest en 1991. (Voici l'empreinte (MD5("Wikipedia, l'encyclopedie libre et gratuite")) = d6aa97d33d459ea3670056e737c99a3d En modifiant un caractère, cette empreinte change radicalement : MD5("Wikipedia, l'encyclopedie libre et gratuit**E**") = 5da8aa7126701c9840f99f8e9fa54976 ).

<sup>22</sup> **SHA-1** (Secure Hash Algorithm) est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (Federal Information Processing Standard du National Institute of Standards and Technology (NIST)). Elle produit un résultat (appelé « hash » ou condensat) de 160 bits.

### VII.3. Les certificats électroniques

Le certificat est un document d'identité électronique attestant du lien entre une identité et une clef publique. Un certificat mentionne au minimum l'identité en question et la clef publique qui lui est associée. Il peut également mentionner une date d'expiration et un numéro de série. Le certificat est signé électroniquement par l'autorité émettrice, qu'on appelle aussi « autorité certifiante », en anglais « Certifying Authority / CA ». Cette autorité est un organisme ayant intérêt quelconque à se porter garant de certaines identités. Parmi les autorités certifiant, on trouve VeriSign, Thawte, Entrust, Baltimore, Gemplus et Matra...

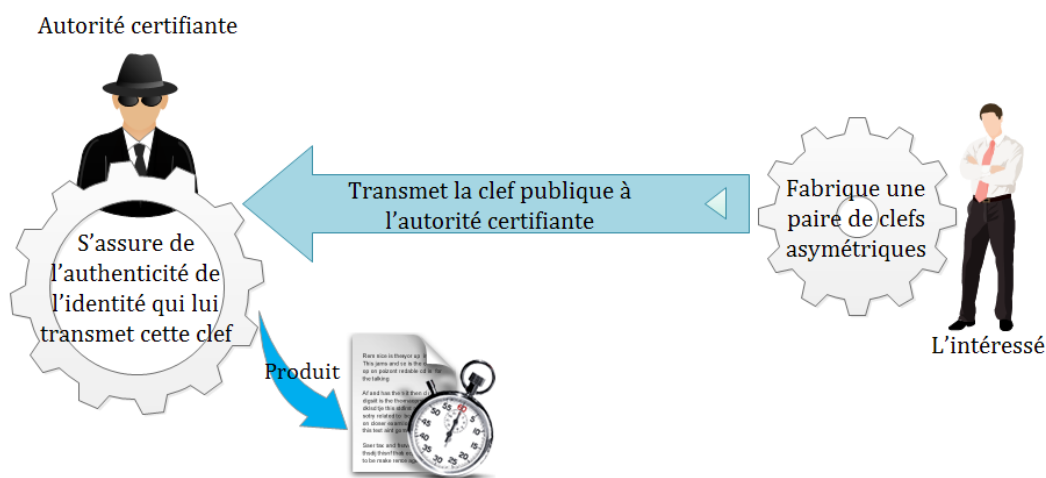


Figure II.9 : Fabrication du certificat.

Pour vérifier la clef d'un interlocuteur, on va consulter son certificat, puis vérifier la signature du certificat. Vérifier cette signature c'est faire usage de la clef publique de l'autorité émettrice du certificat. Comme tout document d'identité, les certificats n'ont ni plus ni moins de crédibilité que l'autorité émettrice. Cette crédibilité tient en particulier aux méthodes qu'emploie l'autorité pour s'assurer de l'identité du producteur de la clef et des protections dont elle entoure sa propre signature (sa clef secrète). La règle veut qu'une autorité certifiant digne de foi publie ses procédures d'identification.

### VII.4. L'identification

Avant d'entamer un échange sécurisé sur un réseau, on va s'assurer une bonne fois de l'identité de son correspondant et partager ensuite avec lui une clef symétrique (privée) qui permettra de crypter par blocs la suite des échanges. Les deux se font dans la même phase, dite d'identification (*Authentication*).

On décrit ci-dessous un schéma d'identification de base. Tous les schémas employés sont des variantes de celui-ci. Partant de deux interlocuteurs Alice et Bob qui ont chacun un couple de clefs asymétriques, attestés par des certificats qu'ils se sont échangés :

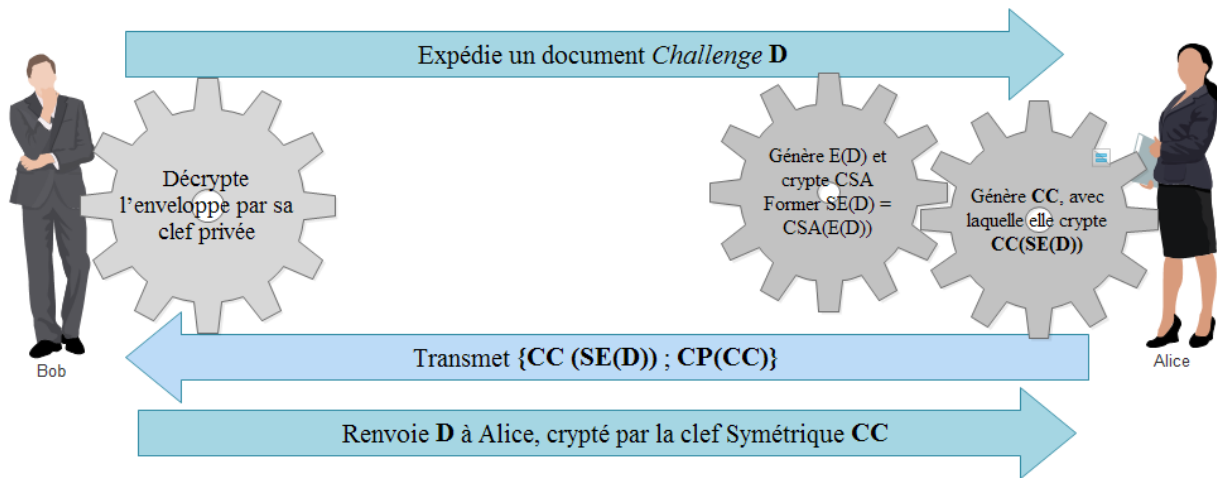


Figure II.10 : schéma d'identification

1. . Bob (par exemple) expédie à Alice un document qu'il crée pour l'occasion et qu'on appelle un défi (*Challenge* en anglais). Soit  $D$  ce défi ;
2. . Alice va signer  $D$  par sa clef secrète. C'est à dire qu'elle génère une empreinte  $E(D)$ , qu'elle crypte avec sa clef secrète  $CSA$  pour former la signature électronique  $SE(D) = CSA(E(D))$  ;
3. . Alice génère une clef symétrique  $CC$ , avec laquelle elle crypte la signature de  $D$ , soit  $CC(SE(D))$ ;
4. . Elle transmet à Bob, le cryptage précédent accompagné de la clé symétrique  $CC$ , crypté par la clef publique de bob  $CP$ . Soit dans l'ensemble  $\{CC(SE(D)) ; CP(CC)\}$ . La portion  $CP(CC)$  est appelée l'enveloppe électronique du message ;
5. . Bob décrypte l'enveloppe par sa clef privée et y trouve la clef  $CC$  avec laquelle il est en mesure de décrypter le document signé. Il peut vérifier l'identité de son interlocuteur en employant la clef publique d'Alice pour décrypter la signature et vérifier qu'il obtient bien l'empreint de défi ;
6. Bob renvoie  $D$  à Alice, crypté par la clef Symétrique  $CC$  démontrant ainsi qu'il est celui qu'il prétend.

Après cet échange, Bob et Alice peuvent communiquer secrètement par des messages cryptés selon  $CC$ .

## VII.5. La datation

Pour dater un document, on utilise le principe de la signature en aveugle (*Blind signature*). Une signature en aveugle est une signature pratiquée sur un document par une identité qui n'a pas accès au contenu de ce document.

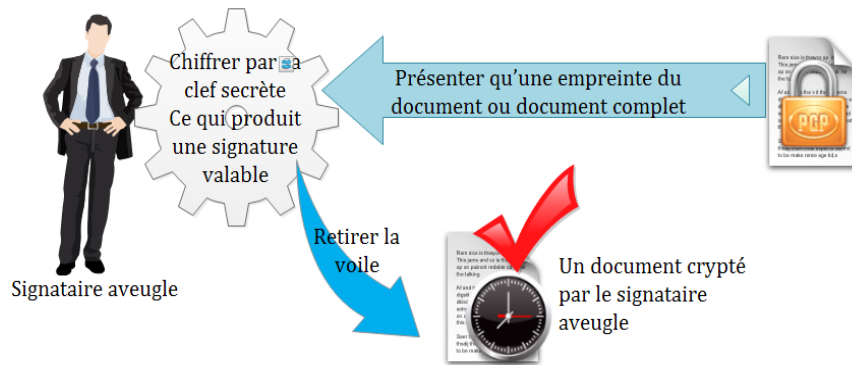


Figure II.11 : schéma datation d'un document

Le cryptage asymétrique de ce service change à chaque instant et de façon aléatoire. Toutes les clefs publiques correspondant à chaque époque sont notoires et sont archivées. Pour vérifier la datation d'un document, il suffit de retrouver quelle clef publique était en vigueur à la date supposée. Le site de la compagnie *Surety Technologies* propose des systèmes de datation.

## VII.6. Le protocole SSL

Le protocole SSL (Secure Sockets Layer) a été développé par Netscape pour offrir sécurité et confidentialité sur Internet. Ce protocole permet d'identifier clients et serveurs dans une connexion de type socket. En fait, le mot Socket peut être défini comme la combinaison d'une adresse IP avec un numéro de port. Le protocole SSL s'applique au niveau de la couche TCP/IP et il chiffre les communications entre le navigateur et les serveurs.

SSL s'inscrit comme une couche intermédiaire du protocole de communication (niveau session). Elle n'est pas liée à une application en particulier. Elle permet donc de sécuriser tout protocole existant d'application Internet, que ce soit HTTP, SMTP, Telnet, FTP ou NNTP et cela, sans modifier les logiciels (exemple le protocole HTTP donne le HTTPS).

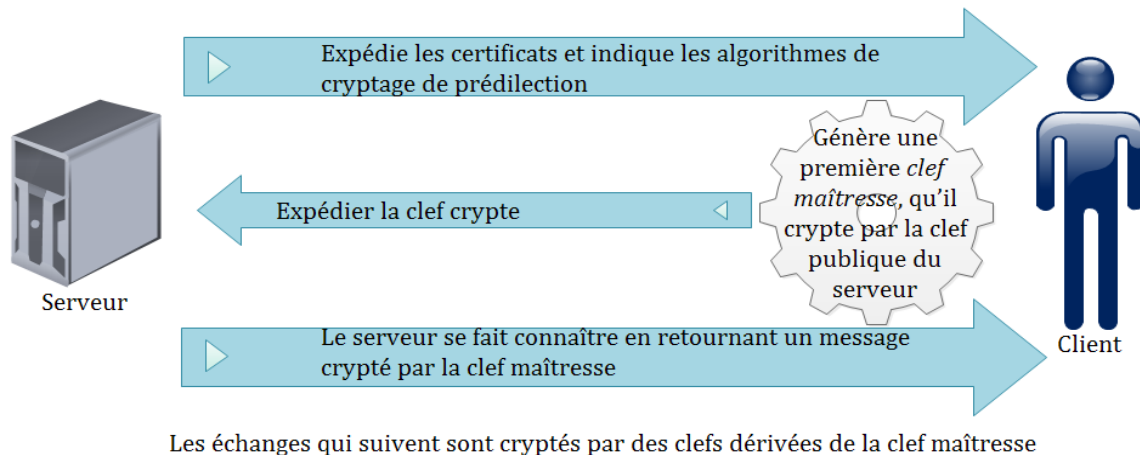


Figure II.12 : L'identification dans le protocole SSL

Au démarrage de la session, le protocole SSL identifie le client et le serveur, puis négocie les paramètres de cryptage. Durant la session SSL assure la confidentialité et la fiabilité des échanges, par des techniques de cryptage et d'identification des messages

L'identification du client est facultative. Le serveur expédie au client un message quelconque et le client s'identifie en retournant sa signature électronique sur ce message, accompagnée de ses certificats. SSL ne gère de signature que sur les messages prévus dans la phase d'identification.

## VII.7. Le protocole SET

Le protocole SET a été développé conjointement par Visa, MasterCard, Microsoft, IBM et Netscape. En effet, le protocole SET est une spécification technique qui vise à sécuriser au moindre coût les transactions par carte bancaire sur les réseaux ouverts tel Internet.

SET est indépendant du transport. Il peut par exemple fonctionner sur le Web en interactif. Pour se faire, les messages de SET sont définis en tant que type MIME (Multipurpose Internet Mail Extension). Les transactions peuvent être très longues. Elles sont identifiées par un numéro unique repris dans tous les messages. Pour éviter des allers retours complexes, une manœuvre élégante a été créée qui exploite les propriétés des *empreintes électroniques*.

Les deux messages (**O** = offre et **I** = instructions) sont réduits en deux empreintes électroniques **E(O)** et **E(I)**. Les empreintes sont *concaténées* puis réduites en signature **SC** (**{E(O), E(I)}**) par la clef publique de l'acheteur **C**. C'est la signature duale.



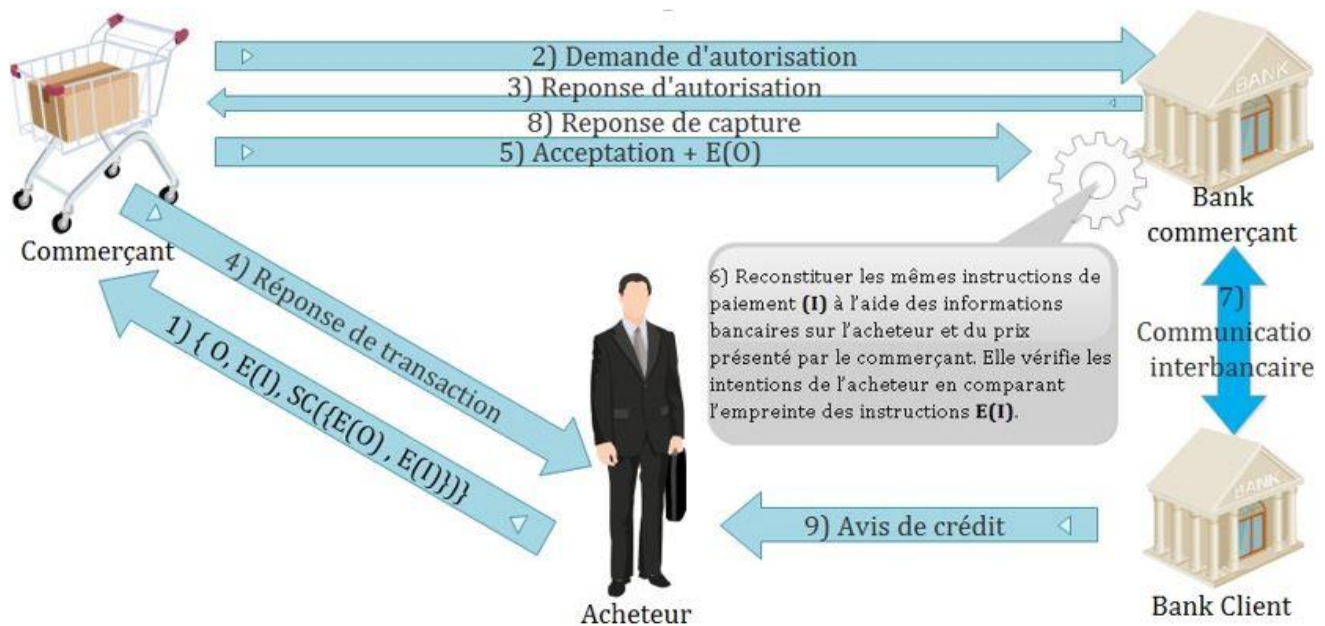


Figure II.13 : Le schéma d'une transaction à l'aide du protocole SET

SET entérine les normes de fait et effectue des choix définitifs. DES<sup>23</sup> est employé pour le cryptage des messages. Les enveloppes électroniques forment une variante du format « PKCS#7<sup>24</sup> » de RSA. SET compte imposer ce format comme nouveau standard. Les signatures suivent les standards de RSA. Les empreintes sont réalisées par l'algorithme SHA-1 et les certificats sont à la norme X.509<sup>25</sup>. La faiblesse de SET est qu'il s'agit d'un système à usage unique (paiement par carte). Le système ne permet pas de modifier le scénario ni d'y introduire de nouveaux intervenants.

## VIII. Conclusion

Durant ce chapitre on a pu voir le e-paiement sous différents angles, de la transaction jusqu'à la sécurité et on a détaillé le paiement par carte bancaire qui constitue une référence pour notre domaine d'étude et enfin on a exposé le m-paiement qui est le cœur même de notre travail.

<sup>23</sup>Le **Data Encryption Standard (DES)** est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits

<sup>24</sup>Les **PKCS (Public-Key Cryptography Standards)**, ou *standards de cryptographie à clé publique*, sont un ensemble de spécifications conçues par les laboratoires RSA en Californie. La société RSA Security est spécialisée dans les solutions de sécurité cryptographiques.

<sup>25</sup>**X.509** est une norme spécifiant les formats pour les certificats à clé publique, les listes de révocation de certificat, les attributs de certificat, et un algorithme de validation du chemin de certification, définie par l'Union internationale des télécommunications (UIT)

Vu que nous avons comme objectif la réalisation d'une application Android pour le paiement électronique en utilisant la technologie NFC, notre application doit communiquer avec d'autres TPE et d'autres applications du système bancaire national. Pour réaliser notre système on a eu besoin d'un organisme d'accueil afin de recueillir des informations pertinentes, et on a opté pour la Banque Nationale Algérienne « BNA ».

Le troisième chapitre sera dédié à la présentation du système bancaire algérien en général et plus précisément celui de la BNA.

# ***Chapitre III :***

***Présentation de l'organisme  
d'accueil***

### **I. Introduction**

Après avoir vu l'e-paiement sous ses différents angles, puis le m-paiement qui est le type de paiement de notre application, nous avons dédié ce présent chapitre à la présentation de notre organisme d'accueil.

à travers le temps, la banque a gagné le quotidien des êtres humains, maintenant à l'ère des technologies son pouvoir est de plus en plus étendu, elle permet de donner du crédit au simple citoyens mais aussi, de participer à des projets à l'échelle national ou même prêter de l'argent pour tout un pays. Dans notre cas nous allons prendre exemple sur la BNA qui est notre organisme d'accueil. On va donner un aperçu sur son historique, son architecture interne et externe et surtout sur les services qui ont pu nous aider à concevoir et réaliser notre projet.

### **II. Définition de la banque [14]**

La banque est un établissement privé ou public qui facilite les paiements des particuliers et des entreprises, elle avance et reçoit des fonds et gère des moyens de paiement ; le siège local de cette entreprise est appelé Succursale d'une banque.

D'une vue informatique la Banque est un ensemble de données relatives au domaine financier, organisées par traitement informatique, accessibles en ligne et à distance.

### **III. Historique de la Banque Nationale d'Algérie [15]**

La Banque Nationale d'Algérie est la première banque commerciale algérienne, elle a été créée le 13 juin 1966. En septembre 1995, la BNA a été la première banque algérienne à obtenir son agrément conformément aux dispositions de la loi 90-10 relative à la Monnaie et au Crédit.

Au mois de juin 2009, le capital de la BNA a été augmenté. Il a été porté de 14 600 milliards de dinars à 41 600 milliards de dinars par l'émission de 27 000 nouvelles actions de 1 million de dinars chacune, souscrites et détenues par le Trésor Public.

Au 1 mars 2011, la BNA se voit confier la gestion de dix fonds d'investissement de wilayas dans le cadre de la loi de finances complémentaire de 2009. En 2013, la BNA annonce un résultat net bénéficiaire de 30,2 milliards de dinars algériens. Le magazine Jeune Afrique la classe alors 13<sup>ème</sup> banque du continent africain. La banque annonce en janvier 2013 un partenariat avec la Compagnie d'Assurances des Hydrocarbures (filiale de Sonatrach) pour le développement d'une offre d'assurance de personnes. En octobre 2013, le conseil des participations de l'Etat a donné son accord pour l'introduction à la bourse d'Alger de la BNA.

En janvier 2014, la BNA dégage un crédit à Air Algérie pour l'achat de 9 avions d'ici à 2017. En décembre 2015 elle affirme avoir 211 agences réparties sur tout le territoire algérien, 17 directions de réseau d'exploitation, 138 distributeurs automatiques de billets (DAB) 90 guichets automatiques de banque (GAB), plus de 5.000 collaborateurs, plusieurs centaines d'entreprises abonnées au service EDI (échange de données informatisées), 165.160 cartes inter bancaires et 2.513 197 comptes clientèles.

En mars 2017, la direction de la Banque nationale d'Algérie annonce qu'elle vient de signer un partenariat avec le groupe Sonelgaz pour permettre aux abonnés de Sonelgaz le paiement électronique des factures.

### **IV. La mission de la BNA**

La BNA exerce toutes les activités d'une banque de dépôt (le secteur bancaire le plus connu).

Elle traite toutes les opérations de banque, de change et de crédit dans le cadre de la législation et de la réglementation des banques et peut notamment :

- Servir d'intermédiaire pour l'achat, la souscription ou la vente de toutes actions, obligation, valeurs mobilières ;
- Consentir sous toutes formes de crédit et de prêts, ou avances avec garanties ;
- Effectuer et recevoir tout paiement en espèce ou par chèque, virement, les opérations d'échanges de monnaie et le tout en conformité avec la réglementation en la matière ;
- Effectue toutes les acquisitions, ventes, locations, ou autre opération mobilières ou immobilières nécessitées par l'activité de la banque ou les mesures sociales en faveur de son personnel...

### **V. Le réseau bancaire algérien [16]**

Le réseau bancaire algérien est géré par la SATIM, Société d'Automatisation des Transactions Interbancaires et de Monétique, qui est :

- Une filiale de 08 Banques Algériennes : (BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, ALBARAKA), créée en 1995 à l'initiative de la communauté bancaire.
- L'opérateur monétique interbancaire en Algérie, pour les cartes domestiques et dans un futur proche, internationales.

- L'un des instruments techniques d'accompagnement du programme de développement et de modernisation des banques et particulièrement les moyens de paiement par carte.
- SATIM réuni 17 adhérents dans son réseau monétique interbancaire : 16 Banques dont 07 banques publiques et 09 banques privées ainsi que l'Algérie Poste.

### **V.1. Les principales missions du SATIM**

- Œuvre au développement et à l'utilisation des moyens de paiement électronique.
- Met en place et gère la plate-forme technique et organisationnelle assurant une interopérabilité totale entre tous les acteurs du Réseau Monétique en Algérie.
- Participe à la mise en place des règles interbancaires de gestion des produits monétiques interbancaires en étant une force de proposition.
- Accompagne la banque dans la mise en place et le développement des produits monétiques.
- Personnalise les chèques et les cartes de paiement et de retrait d'espèces.
- Met en œuvre l'ensemble des actions qui régissent le fonctionnement du système monétique dans ses diverses composantes :
  - maîtrise des technologies,
  - automatisation des procédures,
  - rapidité des transactions,
  - économie des flux financiers, etc...

## **VI. Organisation de la BNA**

La Figure III.1 représente l'organisation générale de la BNA :

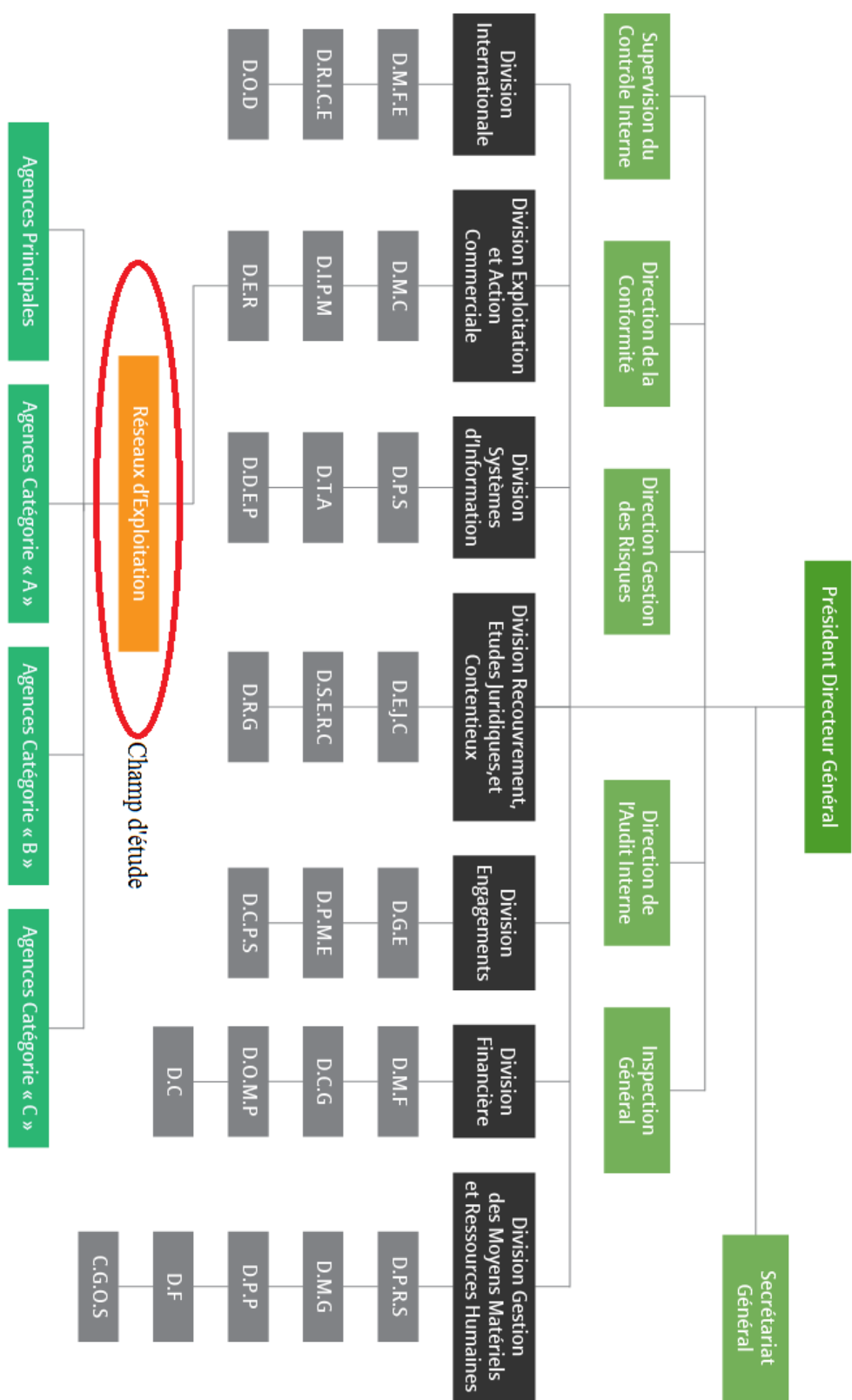


Figure III.1 : L'organigramme de la BNA

### **VI.1 Description de l'organigramme : [15]**

#### **Structures rattachées à la Division Internationale :**

DMFE : Direction des Mouvements Financiers avec l'Etranger.

DRICE : Direction des Relations Internationales et du Commerce Extérieur.

DOD : Direction des Opérations Documentaires.

#### **Structures rattachées à la Division Exploitation et Action Commerciale :**

DER : Direction Encadrement du Réseau.

DMC : Direction Marketing et Communication.

DIPM : Direction des Instruments de Paiement et de la Monétique.

#### **Structures rattachées à la Division des Systèmes d'Information :**

DDEP : Direction du Développement Etudes et Projets

DTA : Direction des Technologies et de l'Architecture

DPS : Direction de la Production et des Services

#### **Structures rattachées à la Division du Recouvrement des Etudes Juridiques et du Contentieux :**

DSERC : Direction du Suivi des Engagements et du Recouvrement de Créances.

DEJ : Direction des Etudes Juridiques et du Contentieux

DRG : Direction des Réalisations des Garanties

#### **Structures rattachées à la Division Engagements :**

DGE : Direction des Grandes Entreprises.

DPME : Direction des Petites et Moyennes Entreprises.

DCPS : Direction de Crédit aux Particuliers et Spécifiques.

#### **Structures rattachées à la Division Financière :**

DC : Direction de la Comptabilité

DOMP : Direction de l'Organisation des Méthodes et Procédures

DCG : Direction du Control de Gestion

DMF : Direction de Marches Financières

#### **Structures rattachées à la Division Gestion des Moyens Matériels et des Ressources Humaines :**

DPRS : Direction du Personnel et des Relations Sociales.

DMG : Direction des Moyens Généraux.

DPP : Direction de la Préservation du Patrimoine.

DF : Direction de la Formation.



CGOS : Centre de Gestion des Œuvres Sociales

### Réseau d'Exploitation :

Le réseau d'exploitation de la BNA compte 17 Directions Régionales d'Exploitation qui supervisent 211 agences de différentes catégories implantées sur tout le territoire national.

## VI.2 Organisation interne de la BNA

La figure III.2 représente l'organisation interne de la BNA

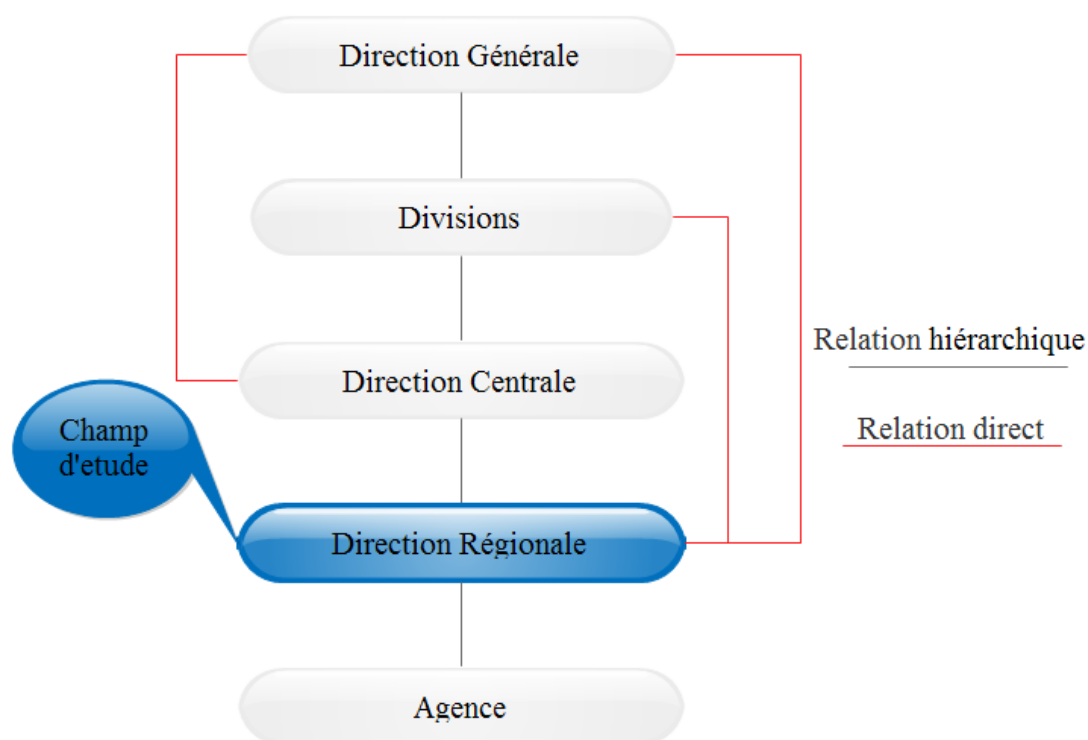


Figure III.2 : Organisation interne de la BNA

### VI.2.1 La direction générale(DG)

La direction générale est composée de :

- **Secrétaire Générale** : il est à la disposition du conseil d'administration.
- **Inspection Générale** : il intervient pour une meilleure gestion, c'est le contrôle du 1<sup>er</sup> degré.
- **Direction de l'Audit interne** : il est à la disposition du commissaire au compte. (Contrôle la situation de la banque).

- *Direction de la Gestion des Risques*
- *Superviseur du Contrôle Interne*

### **VI.2.2 Les divisions**

La BNA est composée des divisions suivantes :

- *Division internationale*
- *Division d'engagement*
- *Division d'exploitation et d'action commerciale*
- *Division de gestion des moyens matériels et ressources humaines*
- *Division d'organisation et système d'information*
- *Division recouvrement des études juridiques et contentieuses*
- *Division financière*

### **VI.2.3 Direction centrale (DC)**

C'est l'ensemble des directions suivantes :

- *Direction de personnel*
- *Direction de formation*
- *Direction des engagements*
- *Direction des moyens généraux*

### **VI.2.4 Direction régionales (DRE)**

En général la BNA dispose de 17 directions régionales d'exploitation (parmi ces DRE nous trouvons la DRE de Tizi-Ouzou N° 183 où nous avons effectué notre stage de formation), et chaque direction est décomposée de quatre départements qui sont :

- *Département crédit ;*
- *Département commercial ;*
- *Département control ;*
- *Département administration ;*
- *Cellule informatique.*

### **VI.2.5 Agences**

Une agence est une cellule de base de l'institution, c'est au niveau de cette dernière que l'ensemble des opérations bancaires sont traitées avec la clientèle.

L'agence est classée en fonction du niveau d'activité déployé, celle-ci peut relever des catégories suivantes :

- Agence principale
- Agence de 1<sup>ère</sup> catégorie (A)
- Agence de 2<sup>ème</sup> catégorie (B)
- Agence de 3<sup>ème</sup> catégorie (C)

L'agence principale est dirigée par un directeur et deux directeurs adjoints selon son importance et le nombre de comptes clientèles gérés.

### VII. Présentation du champ d'études

Notre champ d'étude est la cellule informatique au niveau de la DRE de Tizi-Ouzou comme le montre la figure III.3, où nous avons eu une vue sur les transactions bancaires, les déferents comptes qui existent, la monétique et les protocoles de sécurité. Notre objectif c'est de créer une application de paiement sans contact en utilisant la technologie NFC, cette application sera développée sur les smartphones équipés de ce type de technologie, cette application permet de cibler un appareil (TPE ou téléphone) équipé aussi d'une puce NFC, ce dernier (téléphone ou TPE) est connecté au réseau et il permet de générer la transaction.

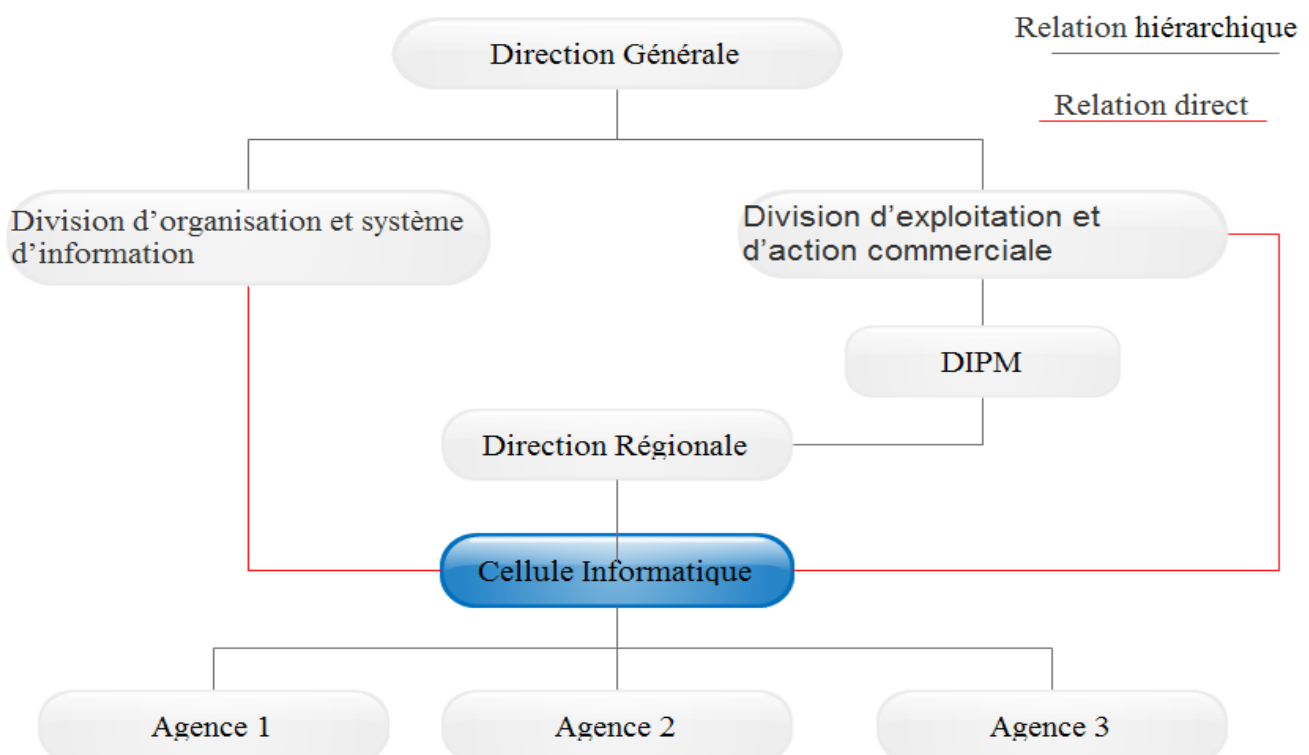


Figure III.3 : Organigramme de champ d'étude

### **VII.1 Activités de la Cellule informatique**

La Cellule Informatique est dirigée par un chef de cellule informatique, un ingénieur informatique et un ingénieur électronique, ces trois personnes s'occupent de l'infrastructure informatique. Ils assurent le bon fonctionnement des postes de travail, la maintenance, les applications et la configuration des équipements réseau.

Tout ça en collaborant avec les autres directions comme la DDEP, DPS, DIPM...

### **VII.2 Situations informatique de la banque**

Pour la situation informatique au niveau de la banque, on a pu constater que les informations sont toutes centralisées au niveau d'Alger, chaque agence et DRE communique en temps réel avec le serveur de la BNA en utilisant un réseau RMS<sup>26</sup>, puisque la banque ne possède pas un serveur d'authentification, elle a besoin de passer par la SATIM pour chaque transaction afin de vérifier la validité des cartes et l'existence du montant signalé.

En fin de journée, le serveur de la SATIM doit accumuler toutes les transactions générées durant la journée par les TPEs qui stockent les transactions accumulées pour générer des fichiers de transaction, ces derniers doivent être envoyés pour chaque banque. Après la réception des fichiers, ils seront traités par le serveur central au niveau d'Alger pour :

- faire la télécollecte ;
- la télé-compensation pour les transactions avec les autres banques ;
- La comptabilité ;
- Le calcul de fin de journée.

On plus la DRE possède :

- le DAB (c'est un distributeur automatique de billets) qui permet le retrait seulement,
- le GAB représente un guichet automatique, il réalise les mêmes opérations que les guichets d'une agence.
- Un serveur de test qui fonctionne en interne, il permet la vérification du fonctionnement des TPE lors de l'installation chez les commerçants, tester les installations réseaux des autres agences en cas de pannes, de modifications ou d'installation d'un nouveau réseau.

---

<sup>26</sup> RMS : réseau multi-services, est un réseau informatique multi services de nouvelles générations NGN (Next Generation Network) de Type IP/MPLS ( Multi-Protocol Label Switching ) et d'envergure nationale.

- Un routeur installé au niveau de la cellule informatique, il est utilisé pour relier les agences au serveur central
- Une installation réseau complète dont une armoire (pare-feu, un switch, et deux modems fournis par Algérie TELECOM un est filaire et un autre sans files), un ensemble d'ordinateurs de bureau distribués dans les différents guichets et sur les bureaux.

### **VIII. Conclusion**

Dans ce chapitre nous avons donné une vue générale sur l'organisation de la BNA et ses différents services, nous avons aussi précisé notre champ d'étude, la cellule informatique qui se trouve au niveau de la DRE de Tizi-Ouzou n° 18. Durant les séances de stages nous avons récolté un ensemble d'informations qui ont pu nous donner une idée générale sur le système bancaire algérien, son fonctionnement et les différentes étapes du e-paiement et les acteurs qui entrent en jeu.

Dans le chapitre suivant nous allons utiliser ces informations recueillies pour analyser les besoins de notre application puis entamer sa conception.

# **Chapitre *IV*:**

**Analyse & conception**

## **I. Introduction**

L'objectif de notre travail est de concevoir et de réaliser une application Android dédiée au paiement par Smartphone en utilisant la technologie de paiement par champs rapproché nommé aussi NFC (Near Field Communication).

Après avoir étudié dans les précédents chapitres le système de paiement électronique en général et plus précisément le m-paiement et présenter une vue globale sur notre organisme d'accueil, ce chapitre sera consacré à l'analyse et la conception de notre système de paiement.

- La première partie de ce chapitre portera sur la description générale de notre application et son architecture.
- La seconde partie est dédiée à sa conception détaillée.

## **II. Problématique et objectifs attendus**

En 2016 l'Algérie s'est lancée dans le monde du paiement électronique après plusieurs années de retard, les Algériens se retrouvent confronter à un mode de paiement très avancé par rapport à leur culture et leur mode de vie, la résistance au paiement par carte se ressent très vite, selon les dires des responsables des banques. Le manque de monnaies liquides et l'absence de traçabilité des transactions et l'inégalité dans le paiement des impôts, ne fait qu'accroître le problème.

Pour remédier à ces problèmes nous avons pris comme objectif la réalisation d'une application Android dédiée au paiement sans contact en utilisant la technologie NFC.

## **III. Architecture de notre application :**

La figure suivante montre l'architecture globale de notre application, dévisée en trois parties, dans la suite du chapitre nous détaillerons les différentes parties.

1-22: Inscription  
1-25: transaction NFC

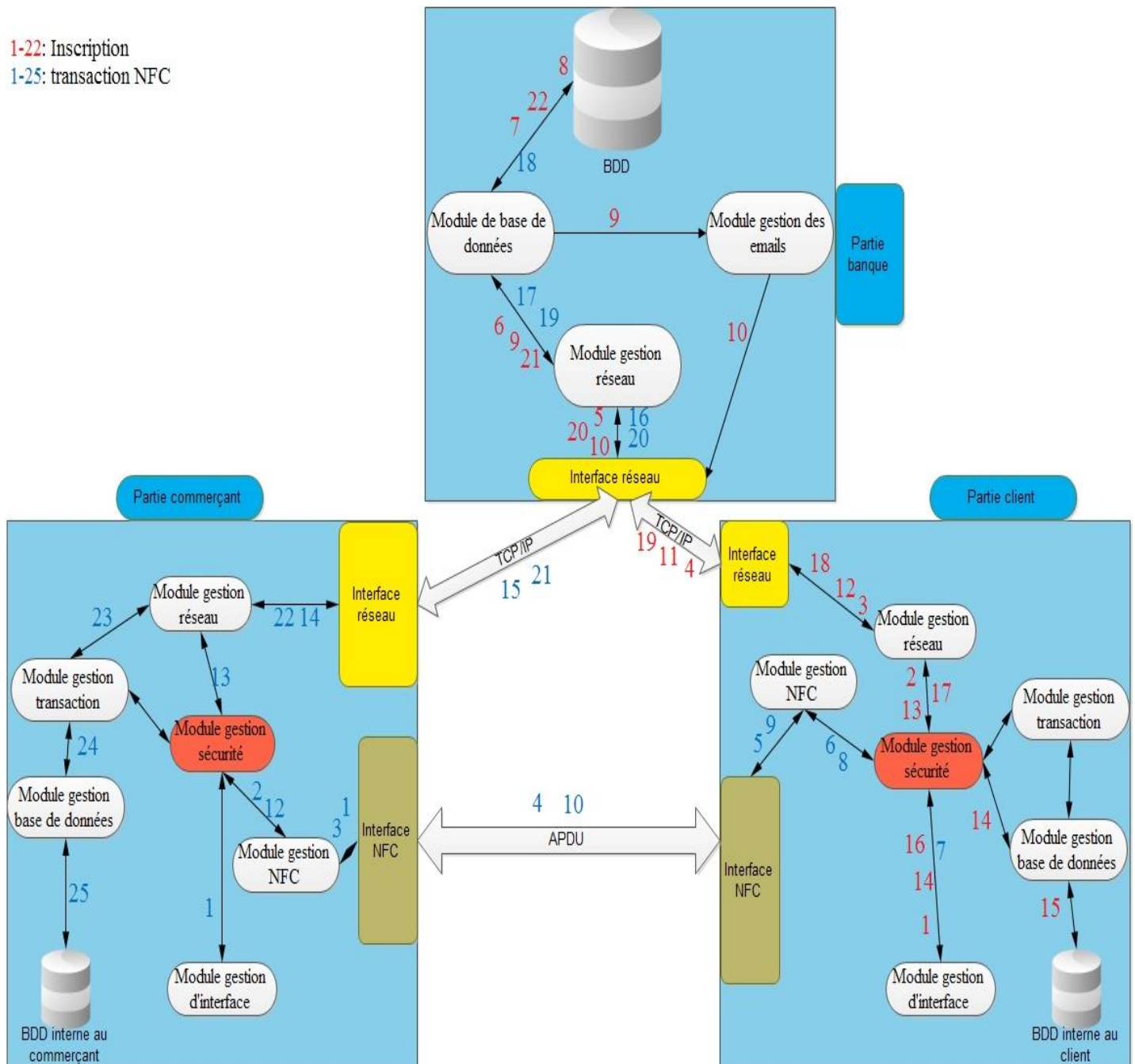


Figure IV.1 Architecture globale de notre application.

Notre application se compose de trois parties distinctes partie client, partie commerçant et partie banque.

Chaque partie est composée de modules et d'interfaces, Le module représente une entité logique « Software » (programme ou ensemble de classes), chaque module est indépendant des autres modules, quant à une interface c'est une entité physique « Hardware ».

Nous avons recensé les interfaces et les modules suivants :



**III.1.1 Les interfaces :**

➤ **Interface réseaux** : on retrouve cette interface dans les trois parties citées ci-dessus, cette interface s'occupe des échanges de données selon le protocole TCP/IP en utilisant différents moyens sans fil dans le cas des mobiles ou filaire dans le cas de la banque.

➤ **Interface NFC** : Composée d'une puce et d'une antenne NFC, cette interface permet des échanges de données selon plusieurs types de protocoles (CF. Annexe II ), on retrouve cette interface dans la partie client et la partie commerçant.

**III.1.2 Les modules :**

- **Module de gestion des interfaces graphiques** : ce module s'occupe de l'affichage des données graphiquement sur les deux Smartphones du commerçant et de son client ( Cf. Chapitre V ). Ce module communique avec le module de gestion de la sécurité.
- **Module de gestion de la sécurité** : c'est un ensemble de classes qui se charge de sécuriser les communications sur plusieurs niveaux :
  1. Authentifier l'utilisateur via un Login et un mot de passe, ou via des moyens biométriques (empreintes digital, reconnaissance faciale ou vocal).
  2. Générer la transaction en utilisant un code PIN ;
  3. Utiliser des algorithmes de cryptage, afin de chiffrer les données échangées.

On retrouve ce module dans les deux parties commerçant et client.

- **Module de gestion NFC** : ce module est constitué d'un contrôleur NFC intégré dans le système d'exploitation et un ensemble de programmes que nous devons créer pour permettre le paiement sécurisé via le standard NFC, ce module est situé sur les deux parties client (CF. V.4) et commerçant (CF. V.5).
- **Module de gestion des transactions** : ce module s'occupe de générer, vérifier et valider une transaction.
- **Module de gestion de Base de données** : ce module permet de créer une connexion, de modifier, d'insérer ou de supprimer des données. Il est intégré dans les trois parties :
  - Cas de la banque il permet de se connecter au serveur de base de données de la banque afin d'inscrire les commerçants et les clients, vérifier, valider et enregistrer les transactions.

- Cas du commerçant ou du client il permet d'enregistrer les traces des transactions et des bons, dans une base de données interne au Smartphone.
- **Module de gestion des interfaces réseaux** : il permet de créer des communications et d'échanger les données entre les différentes parties selon le protocole TCP/IP :
  - Entre le client et la banque, pour l'inscription et la consultation du crédit dans le compte.
  - Entre le commerçant et la banque, pour la vérification de la validité des coordonnées reçues du client lors du paiement, générer la transaction, et la consultation du crédit dans son compte.
- **Module de gestion des mails** : Ce module permet à la banque d'envoyer un e-mail contenant un numéro d'activation du compte et un code PIN après chaque l'inscription d'un client.

## **IV. Analyse**

Une étape essentielle de tout cycle de développement logiciel ou conceptuel consiste à effectuer une étude préalable. Le but de cette phase est de comprendre le contexte du système. Il s'agit d'éclaircir au mieux les besoins fonctionnels et non fonctionnels, faire apparaître les acteurs et identifier les cas d'utilisation.

### **IV.1 Spécification des besoins**

La spécification des besoins constitue la phase de départ de toute application à développer dans laquelle nous allons identifier les besoins de notre application. Nous distinguons des besoins fonctionnels qui présentent les fonctionnalités attendues de notre application et les besoins non fonctionnels, pour éviter le développement d'une application non satisfaisante ainsi de trouver un accord commun entre fonctionnement et convivialité et de permettre son utilisation par le grand public.

#### **IV.1.1 Spécification des besoins fonctionnels**

Après une étude détaillée nous avons pu cerner différents besoins fonctionnels pour les futurs utilisateurs de notre application à savoir le commerçant, son client et la banque. Cette partie est réservée à la description des exigences fonctionnelles à savoir :

- Payer ses achats chez le commerçant ;
- Permettre aux utilisateurs de voir le crédit compte en temps réel ;
- Accéder à l'historique des transactions effectuées par les différents utilisateurs ;
- Inscription des utilisateurs ;
- Statistiques d'achats ;
- Générer les bons de caisse ;
- Accéder à l'historique des bons de caisse ;
- accéder aux statistiques de vente ;
- Inscire les commerçants et les clients dans la banque ;
- Vérifier le compte du client pour debiter ;
- Débiter et accréditer les comptes ;
- Activer l'application pour les utilisateurs ;
- Valider la transaction pour le commerçant.

#### **IV.1.2 Spécification des besoins non fonctionnels**

Les besoins non fonctionnels décrivent toutes les contraintes techniques, ergonomiques et esthétiques auxquelles est soumis le système pour sa réalisation et pour son bon fonctionnement. Vu que notre application est dédiée au grand public elle doit répondre à des besoins fonctionnels spécifiques à l'application mais aussi à des besoins non fonctionnels. Et en ce qui concerne notre application, nous avons dégagé les besoins suivants :

- La disponibilité : l'application doit être disponible pour être utilisée par n'importe quel utilisateur dans n'importe quel lieu et à n'importe quel moment.
- La sécurité de l'accès aux informations critiques : nous devons prendre en considération la confidentialité des données du client surtout au niveau de l'authentification.
- La fiabilité : les données fournies par l'application doivent être fiables.
- La convivialité de l'interface graphique : l'application doit fournir une interface conviviale et simple pour tout type d'utilisateur car elle présente le premier contact de l'utilisateur avec l'application et par le biais de celle-ci il découvrira ses fonctionnalités.
- Une solution ouverte et évoluée : l'application peut être améliorée par l'ajout d'autres modules pour garantir la souplesse, l'évolutivité et l'ouverture de la solution.

**IV.2 Méthodologie et approche adoptée**

Avant de programmer l'application et se lancer dans l'écriture du code il faut tout d'abord organiser les idées, les documenter, puis organiser la réalisation en définissant les modules et les étapes de la réalisation. Cette démarche antérieure à l'écriture du code que l'on appelle modélisation ; son produit est un module.

La modélisation consiste à créer une représentation virtuelle d'une réalité de telle façon à faire ressortir les points auxquels on s'intéresse. Dans le cadre de notre projet on a utilisé la méthodologie UML pour la modélisation des différents diagrammes.

**➤ Présentation d'UML**

En regardant les objectifs fixés pour la réalisation du projet, nous remarquons que nous sommes face à une application modulaire et qui devra rester ouverte pour les améliorations futures. De ce fait, il est très important d'utiliser un langage universel pour la modélisation afin de clarifier la conception et de faciliter les échanges. Notre choix est porté sur le langage UML puisqu'il convient pour toutes les méthodes objet et se prête bien à la représentation de l'architecture du système.

**IV.3 Identification des acteurs**

Dans ce qui suit on va donner la définition d'un acteur et les différents acteurs de notre système suivis de leur rôle.

- 1) **Définition d'un acteur** : Un acteur est toute entité externe (utilisateur, dispositif matériel ou autre système) qui interagit directement avec le système étudié, il peut consulter et/ou modifier directement l'état du système, en émettant et/ou recevant des messages susceptibles d'être porteur de données, autrement dit un objet actif qui utilise les fonctions du système.
- 2) **Extraction des acteurs et leurs tâches**

Après l'étude de l'existant, on a pu identifier (extraire) les acteurs qui seront les futurs utilisateurs de notre application. Dans notre cas, nous recensons les acteurs suivant :

- **le client** : c'est l'utilisateur principale de notre application il représente le grand public (toutes les personnes ayant un compte courant dans la banque), notre application lui permettra de :
  - S'inscrire.
  - S'authentifier.
  - Accéder à son compte utilisateur.
  - Payer le commerçant.
  - Consulter le compte bancaire.
  - Accéder à l'historique des transactions.
  - Accéder aux bons de caisse.
  - Accéder aux statistiques des achats.
  
- **Le commerçant** : est le second acteur de notre système , il représente les commerçants ayant un compte commerçant chez la banque, notre application va lui permettre de :
  - Activer l'application.
  - S'authentifier
  - Accéder à son compte utilisateur.
  - Générer le bon de caisse.
  - Générer la transaction (encaisser chez le client).
  - Transmettre les données de la transaction pour la vérification à la banque.
  - Envoyer le bon de caisse au client.
  - Valider la transaction pour le client.
  - Consulter le compte bancaire.
  - Accéder à l'historique des bons de caisse.
  - accéder aux statistiques de vente.
  
- **La banque** : c'est l'acteur intermédiaire entre le commerçant et le client il est doté d'un serveur d'application et d'un serveur de base de données , son rôle est :
  - Inscrire les clients (acheteurs).
  - Activer l'application au commerçant.
  - Vérifier la validité des transactions.
  - Vérifier le compte du client pour débiter.

- Débitier le compte du client.
- Acréditer le compte du commerçant.
- Valider la transaction pour le commerçant.

## **IV.4 Les diagrammes de cas d'utilisation**

Les cas d'utilisation décrivent le comportement du système du point de vue de l'utilisateur. Ils permettent de définir les limites du système et les relations entre le système et son environnement. Un cas d'utilisation est une manière spécifique d'utiliser le système. C'est l'image d'une fonctionnalité en réponse à la stimulation d'un acteur externe.

### **IV.4.1 Diagrammes de cas d'utilisation**

Pour bien comprendre notre système, nous allons présenter trois diagrammes globaux pour les différentes parties de notre application :

- Diagramme de cas d'utilisation pour le client ;
- Diagramme de cas d'utilisation pour le commerçant ;
- Diagramme de cas d'utilisation pour la partie banque.

Chaque cas d'utilisation sera décrit textuellement, et enfin en vas mettre en évidence les différents scénarios nominaux et alternatifs.

### **IV.4.2 Diagramme de cas d'utilisation pour le client**

Dans ce qui suit nous allons donner le diagramme de cas d'utilisation globale pour la partie client du système que nous avons nommé « *SmartPay* » (voire la figure IV.2).

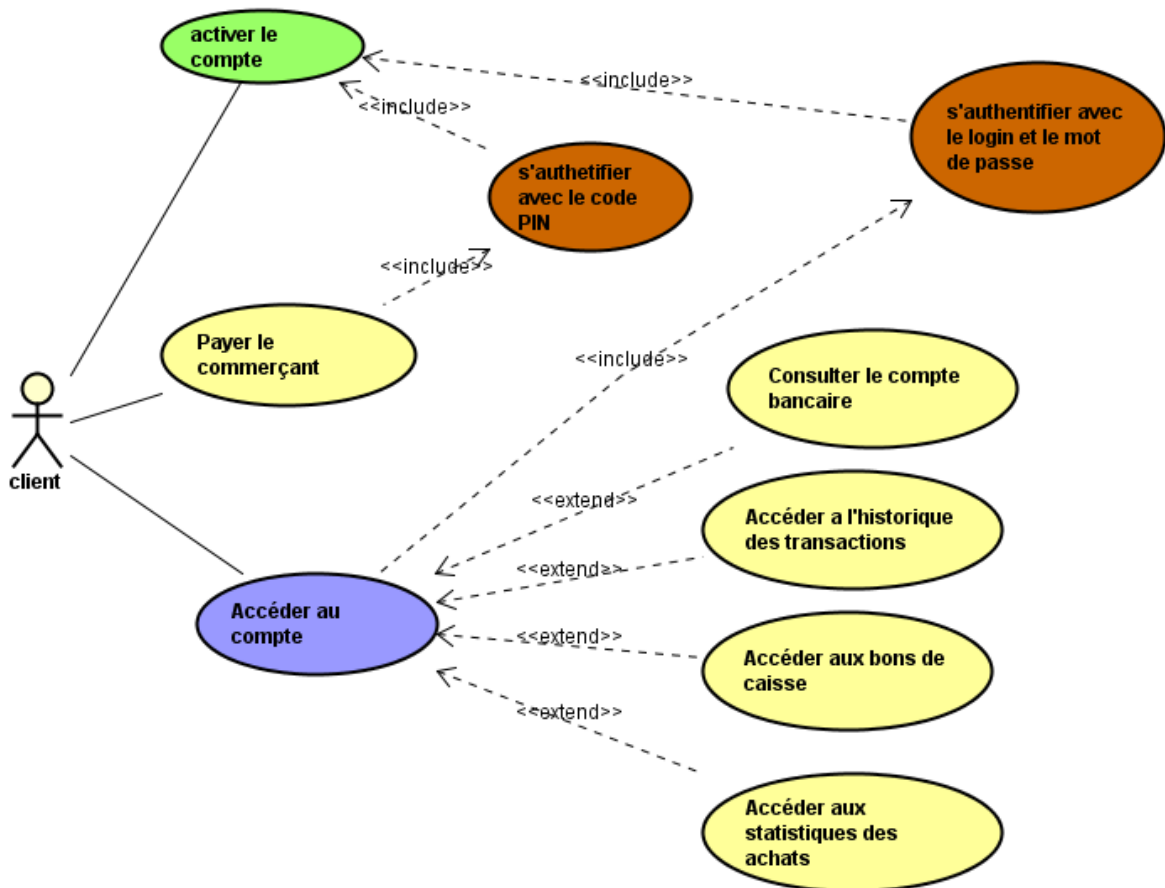


Figure IV.2 Diagramme de cas d'utilisation pour le client.

La figure ci-dessus représente le diagramme de cas d'utilisation globale pour le l'acteur « client », après l'installation de l'application, le client doit s'y inscrire pour accéder aux différentes fonctionnalités de l'application à savoir :

1) L'inscription qui comporte 4 étapes fondamentales :

- Saisir son numéro de compte dans l'interface inscription, et envoie les données au serveur.
- Le serveur retourne les identifiants du client (nom, prénom, Date et lieu de naissance...), le client confirme l'inscription en saisissant le Login et son mot de passe et son e-mail.
- Le serveur lui envoie le code Pin et un code d'activation dans un e-mail.
- Le client doit saisir son code d'activation pour activer l'application.

2) Après une authentification, le client peut accéder au compte utilisateur sur l'application, à partir de cette interface graphique l'utilisateur peut atteindre les fonctionnalités suivantes :

- Il peut consulter son compte bancaire en temps réel.

- Il peut aussi accéder à l'historique des transactions faites depuis le lancement de l'application.
  - Il peut voir les bons de caisse générés par le commerçant.
  - le client peut voir ses statistiques d'achats faites durant la journée, le mois, ou l'année.
- 3) Le client peut payer le commerçant en approchant son smart phone sur le terminal de paiement sans contact doté de la puce NFC.

### IV.4.3 Diagramme de cas d'utilisation pour le commerçant :

les terminaux de paiement doté de puce NFC appelés aussi des TPE sans contact, sont pas encore utilisés en Algérie, par conséquent, nous sommes obligés de développer une application mobile pour jouer le rôle d'un TPE sans contact, ainsi notre application sera une application de paiement mobile à mobile.

Ce choix est mûrement réfléchi car les Smartphones actuels sont plus que capable d'endosser ce rôle, du fait qu'ils sont technologiquement performants (connexion haut débit, puce NFC, sécurité biométrique par empreintes digital...) mais aussi par leur disponibilité et leur prix abordable.

Dans ce qui suit nous allons donner le diagramme de cas d'utilisation général pour la partie commerçant de notre application que nous avons nommé « *SmartTPE* » (voire la figure VI.3).



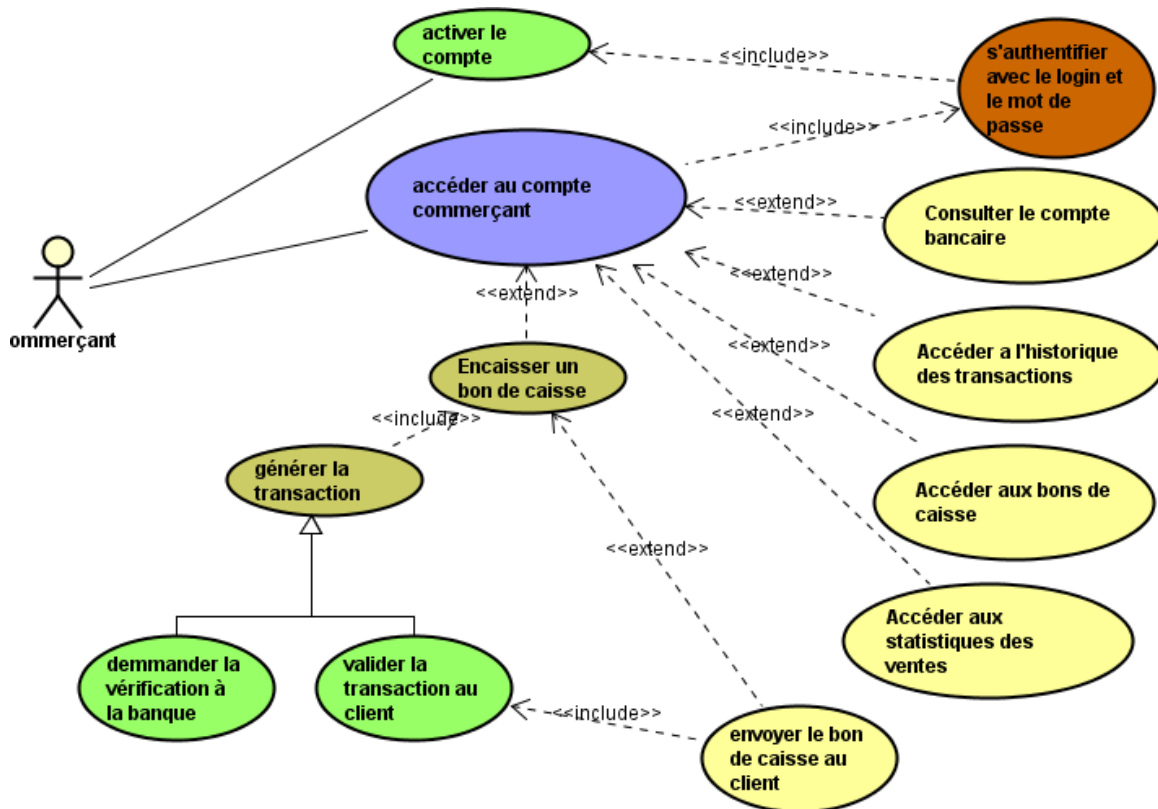


Figure IV.3 Diagramme de cas d'utilisation pour le commerçant

La figure ci-dessus représente le diagramme de cas d'utilisation globale pour le l'acteur « commerçant », après l'installation et l'activation de l'application chez la banque. Après une authentification, le commerçant peut accéder au compte utilisateur sur l'application, à partir de cette interface graphique l'utilisateur peut atteindre les fonctionnalités suivantes :

- 1) Accéder à l'interface de paiement.
- 2) Il peut consulter son compte bancaire en temps réel.
- 3) Il peut aussi accéder à l'historique des transactions faites depuis le lancement de l'application.
- 4) Il peut voir les bons de caisse générés par le commerçant.
- 5) Il peut voir ses statistiques de vente faites durant la journée, le mois, ou l'année.

## IV.4.4 Diagramme de cas d'utilisation pour la banque

Chaque banque possède son propre système d'information et son propre serveur, pour permettre l'intégration de notre système de paiement nous sommes obligés de créer une extension pour le serveur de la BNA. Dans ce qui va suivre nous allons donner le diagramme cas d'utilisation simplifié de cette partie.

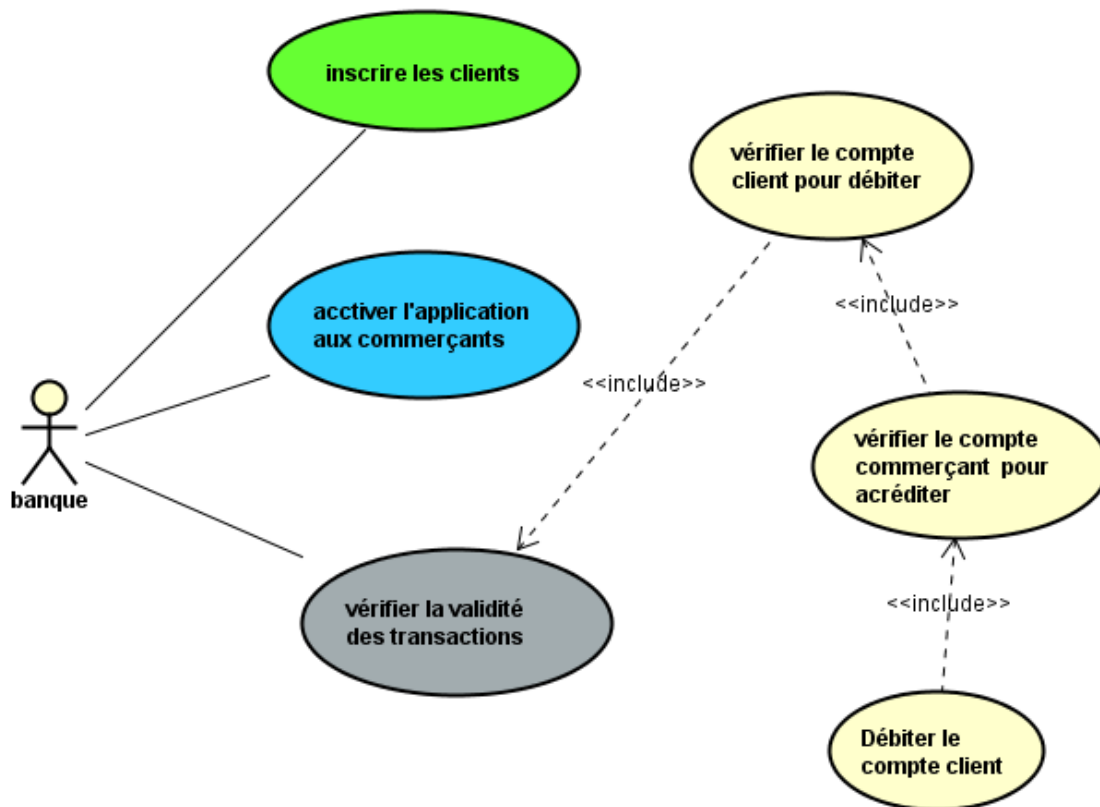


Figure IV.4 Diagramme de cas d'utilisation pour la banque.

La figure ci-dessus représente le diagramme de cas d'utilisation globale pour le l'acteur « banque », du côté de la banque le serveur doit :

- 1) Inscrire le client « acheteur » : le serveur doit vérifier l'existence du compte du client dans la base de données de la banque. Puis il va créer un profil correspondant aux données reçues de la part de l'application du client.
- 2) Activer l'application du commerçant : la banque doit aussi activer l'application aux commerçants.
- 3) Vérifier la validité des transactions, pour permettre cette vérification le système doit :

- Vérifier l'existence du compte du client ;
- Vérifier le crédit du client s'il n'est pas supérieur à la somme de la transaction.
- Vérifier l'existence du compte du commerçant.
- Le système va débiter la somme pour le client et l'accréditer pour le commerçant.
- Le serveur confirme pour le client sur la transaction :
  - Transaction réussi.
  - La somme supérieur au crédit.
  - Compte inexistant.

## **V. Conception**

L'objectif de cette partie est de fournir une étude conceptuelle suffisamment détaillée de notre travail. Pour cela, nous avons opté pour la modélisation des différents concepts du domaine d'application, afin de faciliter la compréhension, et la conception de notre système.

Au cours de cette partie on présentera la conception de notre application sous différents angles :

1. La conception de la couche application en utilisant quelques diagrammes UML tel que les diagrammes de séquence et diagramme de déploiement.
2. La conception de la communication NFC, elle portera sur :
  - a. Présentation de la technologie NFC.
  - b. Les normes utilisées.
  - c. Architecture du mode Emulation de carte.
  - d. Architecture du mode lecteur.
3. La conception de la base de données qui sera implémentée par :
  - a. Le model entité-association.
  - b. Le model relationnel.

### **V.1 Les diagrammes de séquence :**

Ils illustrent la dynamique d'enchaînement des traitements d'une application effectuée par le système. Ces traitements sont ordonnés dans le temps traduisant ainsi la chronologie des événements entre les différents objets du système.

Ce type de diagrammes a le principal intérêt d'illustrer les cas d'utilisation.

Le formalisme utilisé pour modéliser les diagrammes de séquence inclut les objets suivants:

- ❖ **Objets d'interface**: ils représentent l'interface entre l'acteur et le système.

L'icône :



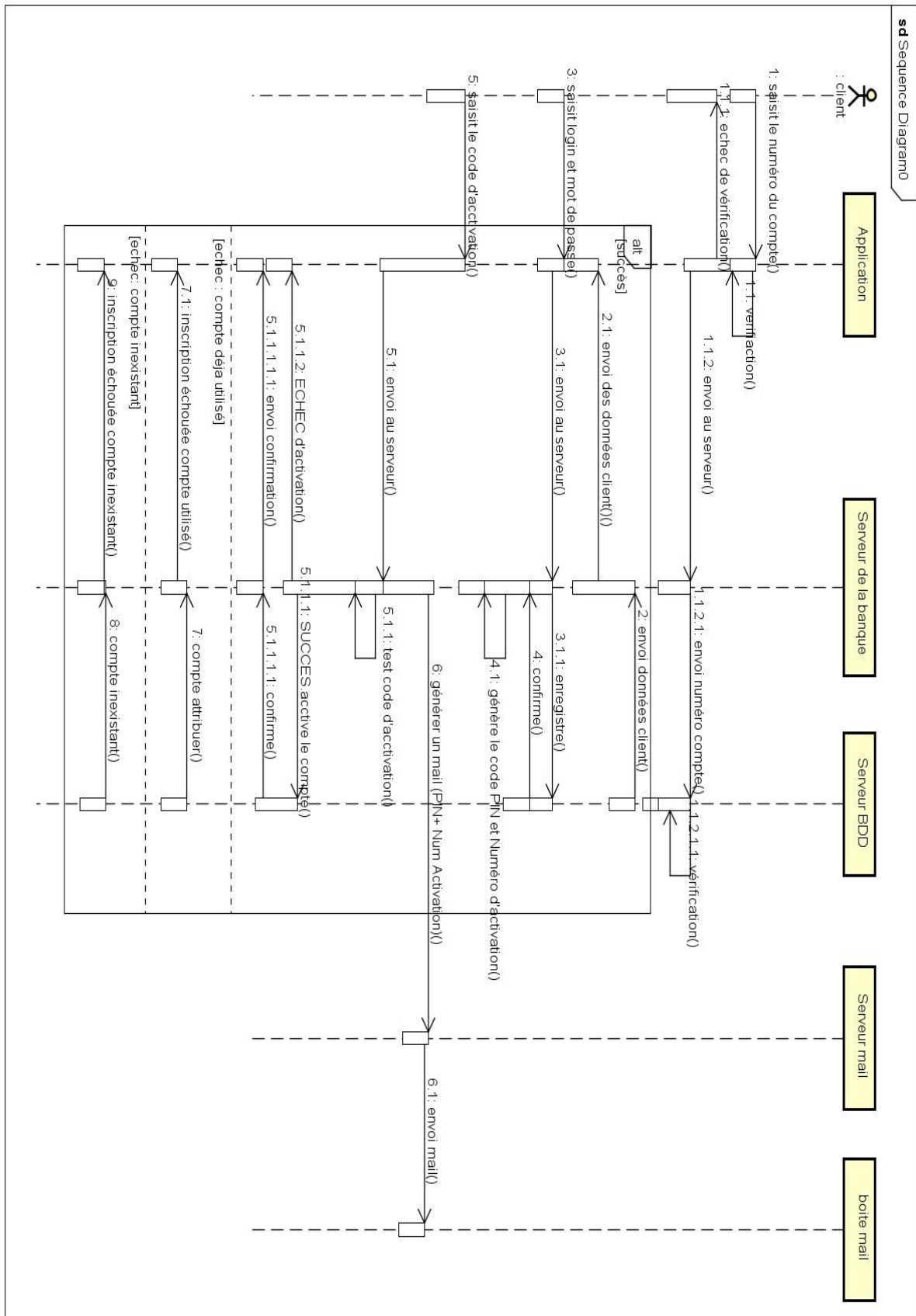
- ❖ **Objets contrôles** : il représente le processus, c'est à dire des activités systèmes significatives.

L'icône :

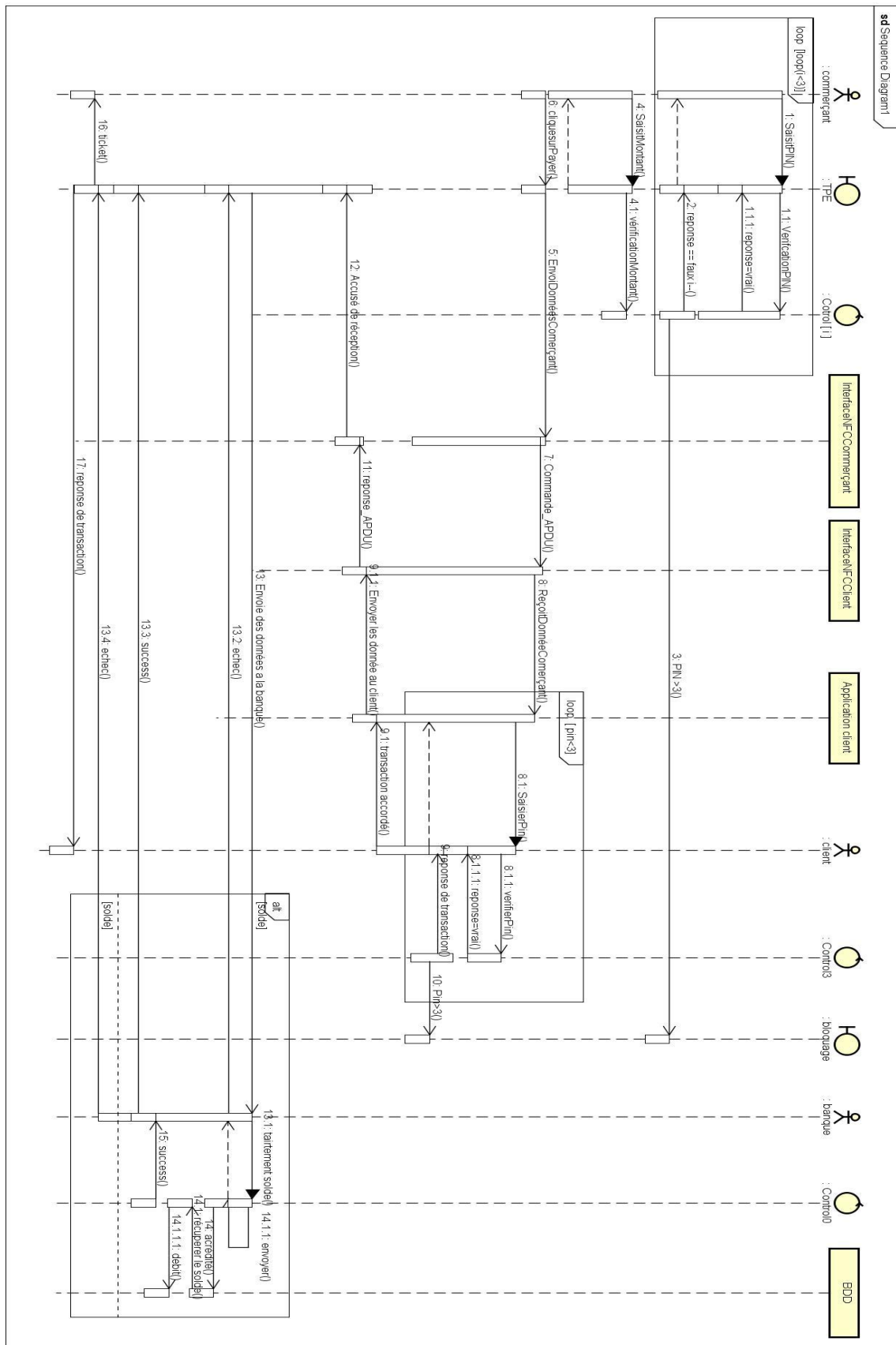


Les diagrammes de séquences correspondants aux cas d'utilisation de notre application sont définis ci-après.

V.1.1. Diagramme de séquence pour le cas d'utilisation inscrire client.



V.1.2. Diagramme de séquence pour le cas d'utilisation payé le commerçant.



## V.2. Diagramme de déploiement :

Le diagramme de déploiement définit l'architecture matérielle de l'application. Il présente les périphériques utilisés et la répartition du système sur ces différents éléments. Il montre aussi les liens de communication entre ces diverses entités.

Le diagramme de déploiement de notre application est représenté par le diagramme ci-après :

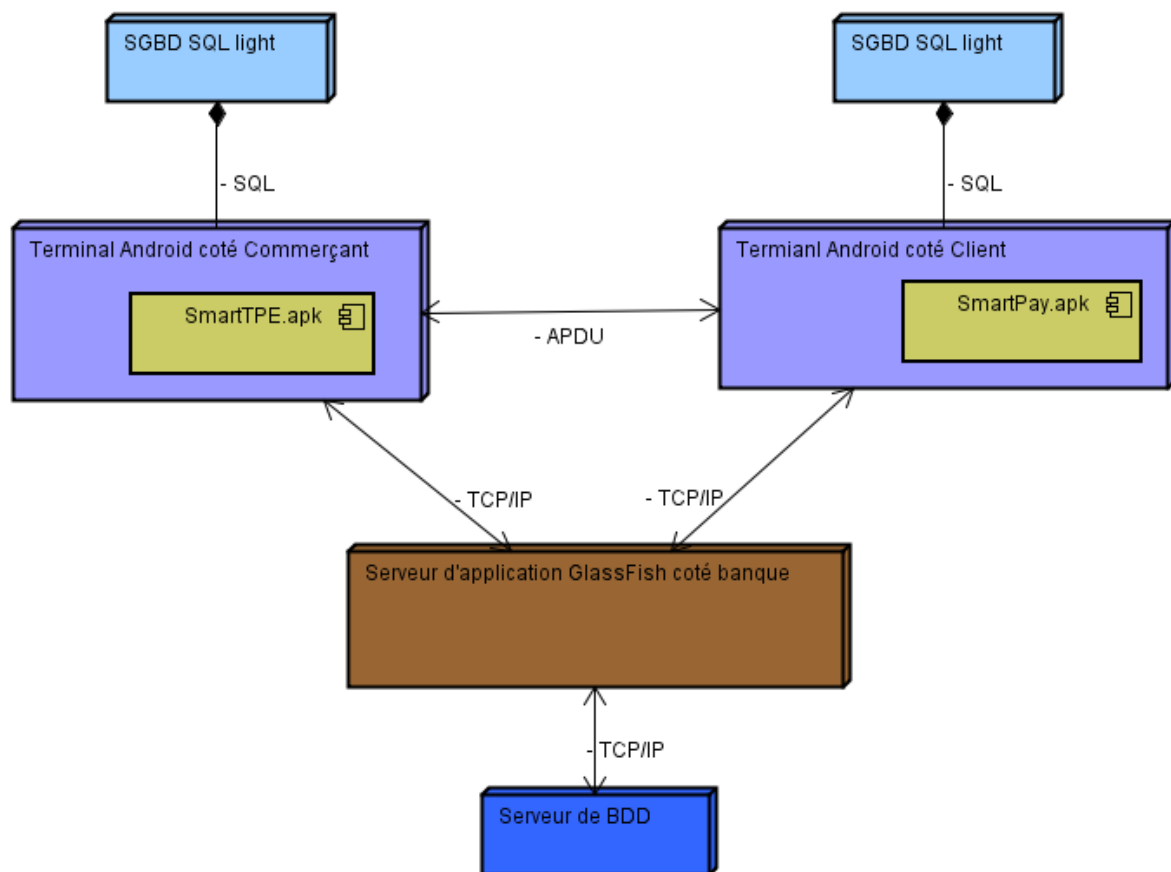


Figure IV.7 Diagramme de déploiement.

Après avoir détaillé la conception de la couche application de notre système à concevoir, nous passons à la couche communication, qui explique les transmissions de données entre un mobile commerçant et celui d'un client.

**V.3. Conception de la couche communication avec les modes NFC :**

La technologie NFC possède trois types de fonctionnement sous Android le mode Peer to Peer, mode émulation de carte et le mode lecteur.

Dans notre cas d'étude nous allons utiliser le mode Emulation de carte pour concevoir l'application SmartPay coté client, et le mode lecteur pour concevoir l'application SmartTPE coté commerçant, «CF. l'Annexe 2» Dans ce qui suit nous allons donner l'architecture de nos applications « SmartPay » et « SmartTPE ».

**V.3.1. Architecture du mode Emulation de carte « SmartPay »**

Conceptuellement, la technologie du HCE permet la désynchronisation du NFC avec le SE<sup>27</sup> hébergé par le mobile ; le système d'exploitation (OS) pilote ainsi directement le NFC (Voir la figure IV.8). L'application mobile installée dans l'OS peut embarquer les données bancaires. Mais la technologie permet des choses bien plus intéressantes comme le stockage des données dans le cloud<sup>28</sup>.

Par ailleurs, afin de limiter le risque de récupération des données sensibles par un malware (logiciel malveillant) exécuté dans la mémoire du téléphone, les ingénieurs ont eu l'idée de générer des numéros de cartes jetables. Cette sécurité est appelée « Tokenisation ». Cette dernière a fait l'objet d'une spécification par l'organisme EMVCo permettant d'assurer l'interopérabilité (CF. V.4.4.3).

Dans un premier temps, nous allons expliquer comment fonctionne le HCE lorsque le smartphone est connecté au réseau, c'est-à-dire lorsqu'il peut aller chercher les données dans le cloud. Par la suite, nous verrons comment cela fonctionne en mode non connecté.

---

<sup>27</sup> SE Secure Element : est un microcontrôleur sécurisé contenu dans les cartes à puce, souvent utilisé pour enregistrer des données sensibles comme le code PIN le numéro de la carte, et aussi l'historique des transactions.

<sup>28</sup>Le cloud (« le nuage ») est un ensemble de matériels, de raccordements réseau et de logiciels qui fournit des services sophistiqués que les individus et les collectivités peuvent exploiter à volonté n'importe où dans le monde.



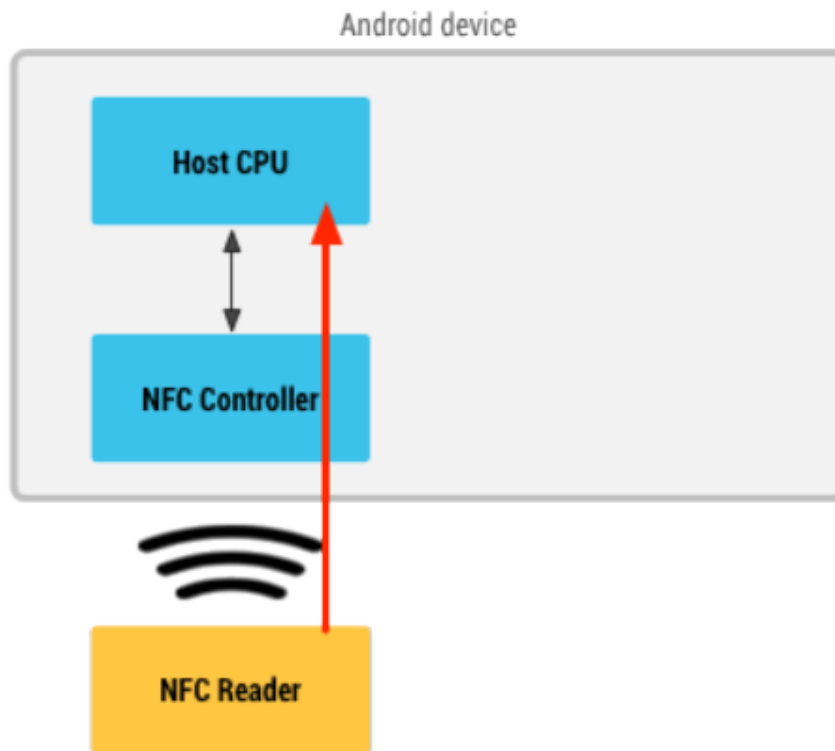


Figure IV.8 Schéma paiement NFC en mode HCE

#### V.3.1.1. Mode connecté

À l'approche du TPE, le smartphone sollicitera, via l'antenne NFC, le contrôleur NFC qui utilisera sa table de gestion des identifiants d'application (AID : CF. V.4.4.2 3.) la norme ISO/IEC 7816-5) afin de savoir où envoyer la requête sans contact.

- Si l'AID est présent dans la table des AID de la SIM, la requête sera envoyée directement au SE (cas du modèle « SIM-centric<sup>29</sup> »).
- Sinon, elle sera transmise à l'application hébergée dans le système d'exploitation du téléphone.
- L'application gère ensuite l'appel éventuel du SE dans le cloud afin d'envoyer les données sensibles au contrôleur qui les transmettra en NFC au TPE.
- Pour plus de sécurité, certaines données, comme le numéro de carte, peuvent être issues d'un serveur de Tokenisation.

<sup>29</sup> SIM-centric : mode de fonctionnement du mode émulation de carte en utilisant le SE intégré dans la carte SIM, voire L'annexe II pour plus de détails.

HCE ne concerne en effet que l'acquisition sans contact des données de la carte virtuelle. Le reste de la transaction est traitée comme pour un paiement « puce ».

**V.3.1.2. Mode déconnecté**

Afin de toujours permettre l'utilisation du paiement via HCE, la gestion du mode déconnecté a fait son apparition. Pour cela, l'application communique, en amont, avec le serveur de Tokenisation afin de télécharger des numéros de cartes qui pourront être utilisés lorsque le réseau sera inaccessible.

**V.3.1.3. La sécurité**

Le fait que les données sensibles remontent au système d'exploitation est risqué d'un point de vue sécuritaire, des mécanismes de sécurité participent ainsi à la sécurité du HCE comme :

- la Tokenisation.
- le scoring afin de savoir si une autorisation EMV doit être émise ou non.
- authentifiant biométriquement par le porteur avant tout paiement. Cette dernière apparaît généralement sous 3 formes :
  - empreinte digitale,
  - analyse faciale,
  - analyse vocale.

**V.3.1.4. Les normes utilisées :**

Pour concevoir une application qui permet une interaction avec l'ensemble des terminaux de paiement sans contact, notre application « SmartPay », doit respecter un ensemble de normes mondiales dédiées à la technologie NFC, mais aussi au paiement dont on peut citer les normes suivantes :

- ISO/IEC 14443-4 ;
- ISO/IEC 7816-4 ;
- EMVCo.

Le but de cette partie n'est pas de retranscrire les normes citées ci-dessus dans leur intégralité, mais plutôt d'en présenter la structure. Pour le détail complet de ces normes voir les travaux [17], [18] et [19].

## V.3.1.5. La norme ISO/IEC 14443-4[17]

La norme ISO/IEC 14443 possède plusieurs parties<sup>30</sup>, Dans notre cas nous nous sommes intéressés par la partie 4 qui définit la couche applicative de la norme 14443-4 la figure IV.9 montre une trame ISO 14443-4 transportant des APDUs (ISO 7816-4).

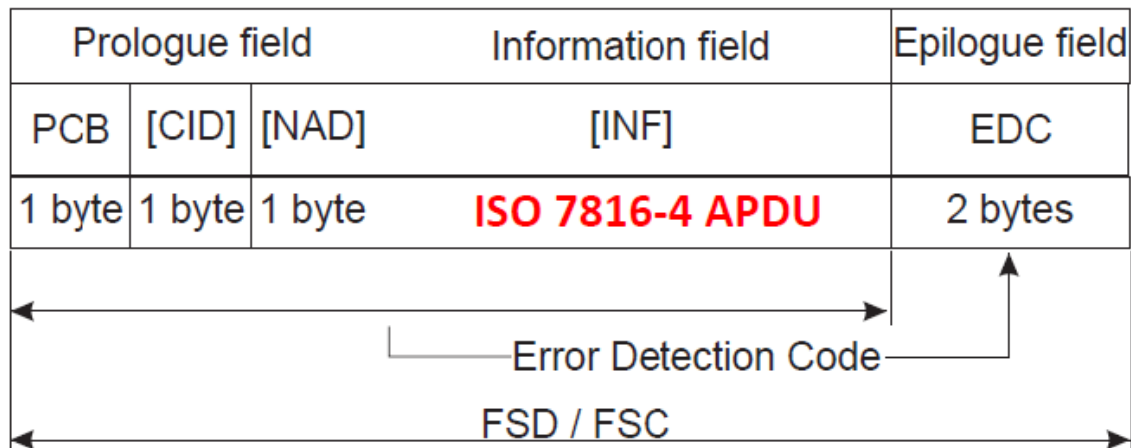


Figure IV.9 : Les trames ISO 14443-4 transportent des APDUs (ISO 7816-4).

PCB:Protocol Control Byte;

CID:Card Identifier;

NAD:Node Address;

EDC>Error Detection Code

FSC:Frame Size for proximity Card

FSD: Frame Size for proximity coupling Device.

Cette figure montre la syntaxe d'une trame ISO 14443-4 transportant un APDU (voire ISO 7816-4), dans le cas d'Android le programmeur ne gère pas les Prologues et les Epilogues des trames, mais c'est les API's<sup>31</sup> et les Framework du contrôleur NFC intégré dans le mobile qui

<sup>30</sup>Voire L'annexe II : Quelques Notions sur le NFC

<sup>31</sup> Application Programming Interface : ensemble de fonctions et de procédures placées dans des bibliothèques, fournies par un programme ou un système d'exploitation afin de faciliter la programmation d'applications qui l'utilise.

se charge de mettre les APDUs créés par le programmeur dans la bonne syntaxe et les envoyer au destinataire soit une carte sans contact, un autre smartphone NFC ou un Tag NFC.

Donc cette norme est utilisée pour l'échange des informations avec les ondes magnétiques gérées par le système d'exploitation Android, et dans notre cas le gros du travail se fait sur les normes ISO/IEC 7816-4 et la norme EMV qui s'occupe de mise en forme des données.

### V.3.1.6. La norme ISO/IEC 7816[18] [20]

ISO 7816 défini par l'International Standard Organization, contient un ensemble de normes qui couvre divers aspects des cartes à puce. 15 normes sont proposées pour les cartes à contact électrique.

Dans notre cas d'étude nous avons utilisé les normes suivantes :

- ISO 7816-3 : nature des signaux électriques et protocole de transmission entre le terminal et la carte
- ISO 7816-4 : organisation des données et sécurisation
- ISO 7816-5 : procédure d'inscription des applications

#### 1) Les protocoles de transport TPDU (ISO 7816-3)

Il existe deux protocoles T=0 et T=1 normalisés par l'ISO 7816-3, ces deux protocoles sont utilisés dans les communications entre TPE et cartes bancaires. Le protocole T=0 étant le plus utilisé, nous nous sommes basé sur ce dernier pour concevoir notre application.

#### 2) Les commandes APDU ISO7816-4

Les commandes APDUs (Application Protocol Data Unit) contiennent soit un message de requête, soit un message de réponse à une précédente requête.

Il existe quatre types d'APDUs :

- Cas 1, pas de données dans la requête, pas de données dans la réponse.
- Cas 2, pas de données dans la requête, mais des données sont présentes dans la réponse (ordre sortant).
- Cas 3, la requête comporte des données pas la réponse (ordre entrant).
- Cas 4, la requête et la réponse comportent des données (ordre entrant sortant). (Voir le Tableau IV.1)

Le tableau IV.1 décrit le format des commandes.

Commande APDU						
Entête obligatoire				Corps optionnel		
CLA	INS	P1	P2	Lc	Data field	Le
<ul style="list-style-type: none"> <li>•CLA (1 octet): Classe d'instructions --- indique la structure et le format pour une catégorie de commandes et de réponses APDU</li> <li>•INS (1 octet): code d'instruction: spécifie l'instruction de la commande</li> <li>•P1 (1 octet) et P2 (1 octet): paramètres de l'instruction</li> <li>•Lc (1 octet): nombre d'octets présents dans le champ données de la commande</li> <li>•Avec Le=0, - Si cde d'écriture =&gt; pas de données utiles - Si cde de lecture =&gt; la cde doit retourner 256 octets de données utiles</li> <li>•Data field (octets dont le nombre est égal à la valeur de Lc): une séquence d'octets dans le champ données de la commande</li> </ul>						

Tableau IV.1 : formats des commandes APDU's.

- La représentation des quatre types d'APDUs est en conséquence la suivante (la liste des commandes de base complète est donnée dans l'Annexe II) :
  - Cas1 : CLA INS P1 P2
  - Cas2 : CLA INS P1 P2 Le
  - Cas 3 : CLA INS P1 P2 Lc Data
  - Cas 4 : CLA INS P1 P2 Lc Data Le

La réponse comprend deux partie une liste d'octets optionnels (body) et un mot de status (trailer) comportant deux octets SW1 SW2 [liste d'octets optionnels] SW1 SW2 Le status 90 00 indique une exécution correcte de la commande additives (Voire le Tableau IV.2). En règle générale SW1 indique l'état de la carte, SW2 fournit des informations.

Réponse APDU		
Corps optionnel		Partie obligatoire
Data field	SW1	SW2
<ul style="list-style-type: none"> <li>•Data field (longueur variable): une séquence d'octets reçus dans le champ données de la réponse</li> <li>•SW1 (1 octet) et SW2 (1 octet): Status words (Mots d'état)—état de traitement par la carte</li> </ul>		

Tableau IV.2 : formats des réponses APDU's.

### 3) Identification des Applications – ISO7816-5

Un identifiant d'application (AID Application Identifier) est un nombre qui comporte 16 octets. Les 5 premiers octets (RID Registered application provider Identifier) identifient le fournisseur d'une application. Les 11 octets restant représentent un identifiant d'application. Son format est donné au Tableau IV.3.

L'ISO gère l'affectation des RIDs aux compagnies, chaque compagnie obtient son propre et unique RID de l'ISO. Les compagnies gèrent l'affectation des PIXs pour leurs AIDs. Une application embarquée peut être activée par la commande :

SELECT\_FILE (00A4 0400 10 [AID]) avec comme paramètre le champ AID.

Application identifier (AID)					
National provider (RID)	registered	application	Proprietary extension (PIX)	application	identifier
5 octets			0 to 11 octets		

*Tableau IV.3 : Format de l'AID*

#### V.3.1.7. La norme EMVCo [19]

La norme EMV 'Europay' 'MasterCard' 'Visa' est une norme internationale créée en Décembre 1993 par Europay, MasterCard, Visa puis rejoint par le japonais JCB International (depuis Déc. 2004), l'américain American Express (depuis Fév. 2009).

Son principal objectif c'est de normaliser les cartes bancaires avec contact et sans contact le mobile paiement, les TPE et les DAB.

Contrairement aux normes ISO/IEC les normes EMV sont gratuites, néanmoins les spécifications viennent pour compléter les normes ISO/IEC 7816 et ISO/IEC 14443. Elles doivent être lues conjointement. Si des définitions fournies dans EMV sont différentes de la norme ISO alors les définitions de la norme EMV remplacent celles de l'ISO.

#### V.3.2. Architecture du mode lecteur « SmartTPE » :

Le mode lecteur permet au mobile équipé du NFC de lire des « tags », avec cette technique le smartphone peut lire le contenu d'une carte bancaire qui sera considérée comme un tag NFC,

et aussi il permet d'interagir avec un smart phone hébergeant un service HCE, ce mode permet de communiquer avec plusieurs types de Tags et de technologie en utilisant plusieurs protocoles.

Dans notre cas on va utiliser la technologie IsoDep qui fournit l'accès aux propriétés et opérations de la norme ISO 14443-4 (voir CF. annexe 2 pour plus de détails sur les différentes technologies).

### V.3.2.1. Les étapes de la lecture des tags NFC

La figure IV.10 montre les étapes de la lecture des différents types de tags NFC, Afin d'utiliser le mode lecture fournie par le système Android ce dernier offre plusieurs interfaces programmables pour les différents types de technologies (NDEF, IsoDep, Tags), l'implémentation de ce mode sera détaillé dans le chapitre V : Réalisation.

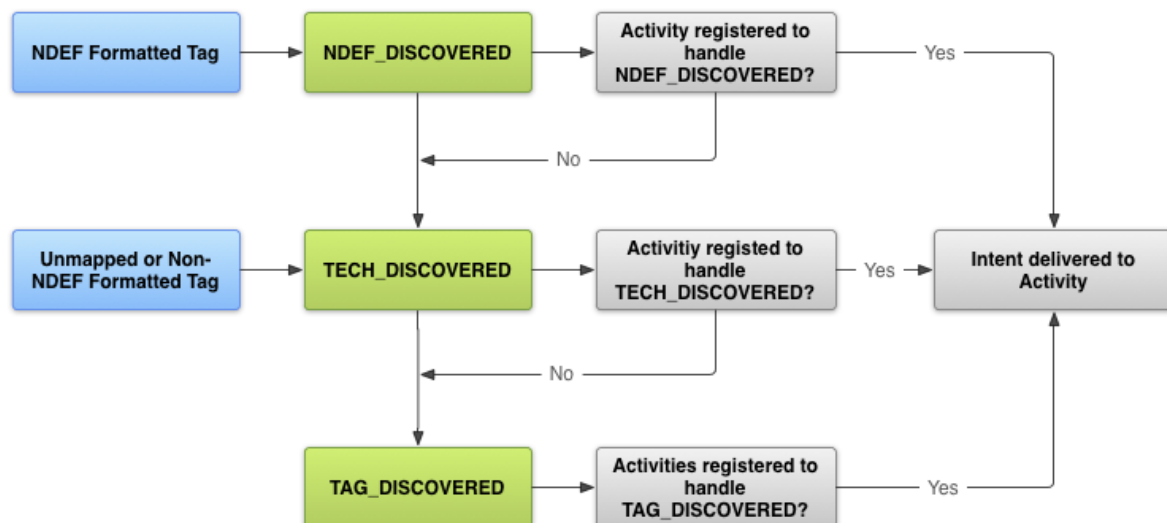


Figure IV.10 : les étapes de la lecture de tags par le contrôleur NFC dans le système Android

1. Le lecteur teste si le tag est de type NDEF, il lance l'écouteur 'Handel' NDEF\_DISCOVERED' qui est le format de données utilisées par Android Beam.
2. Sinon ; Si le type de messages n'est pas du type NDEF, le contrôleur NFC passe au type TECH, qui est l'écouteur des différents tags comme celui de la carte bancaire.

3. Sinon ; Si le type n'est pas du type TECH le contrôleur passe au type RFID<sup>32</sup>.

#### **V.3.2.2. Les normes utilisées dans le mode lecteur**

Afin concevoir une application qui permet une interaction avec l'ensemble des cartes de paiement sans contact, notre applications « SmartTPE », doit respecter les mêmes normes que l'application SmartPay à savoir :

- ISO/IEC 14443-4 ;
- ISO/IEC 7816-4 ;
- EMVCo.

#### **V.3.3. La Communication NFC entre le lecteur « SmartTPE » et le Mode Carte « SmartPay »**

L'application SmartTPE initie la communication avec l'application SmartPay en envoyant une commande SELECT\_AID<sup>33</sup> (voire la figure IV.11), cette commande est traitée par le système d'exploitation qui teste si cet AID est destiné au Secure Elément de la carte SIM ou au Service HCE (Host Card Emulation). Si l'AID est destiné au Service, le système cherche l'application qui gère cet AID, puis il redirige la commandes APDU de sélection vers ce service, le service répond par une réponse APDU SW1 = 90 et SW2 =00 (cette réponse signifie que la sélection est bien faite) en cas où son AID est égale à l'AID de la commande de sélection. Après la Sélection une connexion sera établit, l'application SmartTPE envoie un ensemble de Commandes APDU et chaque commande APDU reçus par le Smartphone du client sera redirigée vers le service HCE, selon les commandes reçues l'application SmartPay envoie des réponses APDU.

---

<sup>32</sup>RFID (**R**adio **F**requency **I**dentification) :Auto-identification des personnes, des objets, des services

<sup>33</sup> SELECT\_AID est une commande de base normalisée par l'iso 7816-4 et EMVCo, elle est utilisée pour la sélection des l'applications. La liste complète des commandes APDU's de base est donnée dans l'Annexe 2.



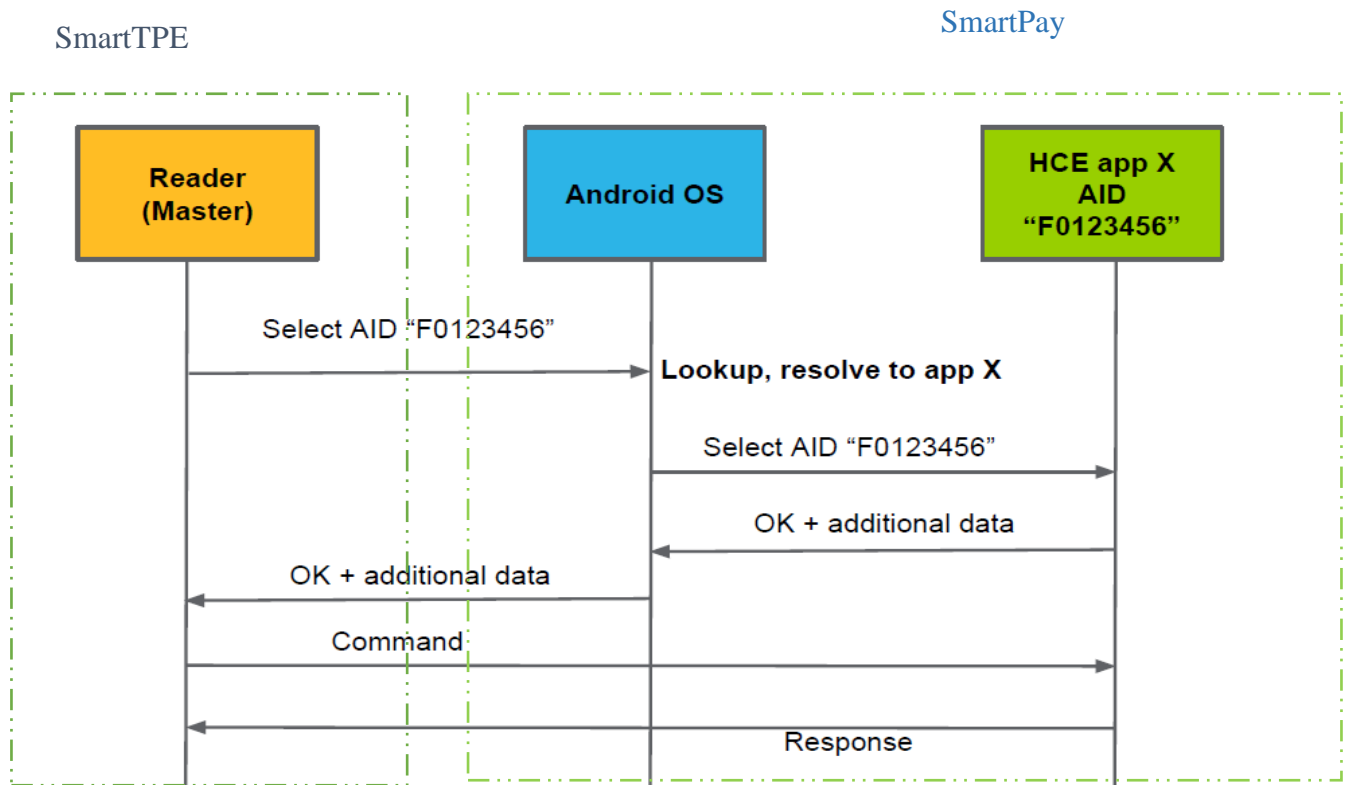


Figure IV.11 Séquencement de la sélection du service HCE

## V.4 Niveau organisationnel des données

Afin de concevoir la base de données du coté serveur nous avons opté pour le model entités associations et le schéma relationnel.

### V.4.1 Le modèle entités associations :

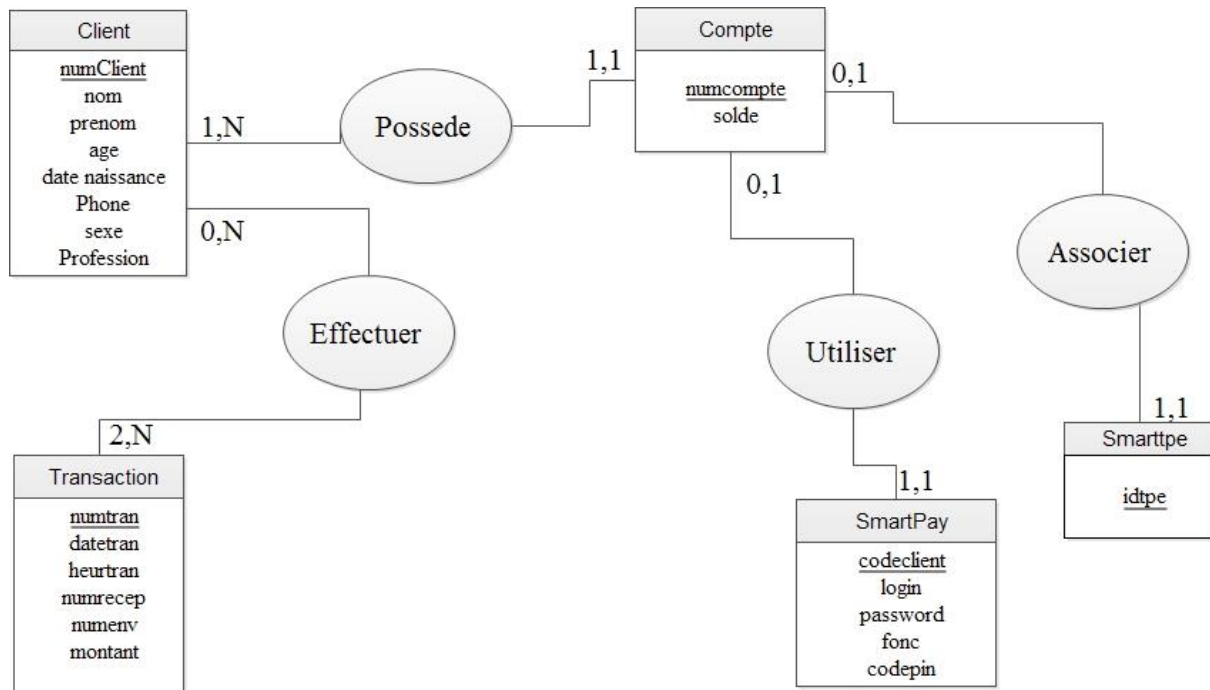


Figure IV.12 Le modèle entités associations

#### V.4.2 Schéma relationnel :

**Client** (numclient, nom, prénom, âge, date de naissance, téléphone, sexe, profession) ;

**Compte** (numcompte, solde, numclient\*) ;

**Transaction** (numtran, datetran, heurtran, numrecep, numenv, montant) ;

**Smartpay** (codeclient, login, password, fonc, codepin, numcompte\*) ;

**SmartTPE** (idtpe, numcompte\*) ;

**Effectuer** (numtran, numclient);

## VI. Conclusion :

Au cours de ce chapitre nous avons vu les détails de nos trois applications SmartPay, SmartTPE, BNAServerTest qui représentent respectivement la partie client, la partie commerçant et la partie banque de notre projet. Au fur et à mesure nous avons essayé de donner une conception rigoureuse de notre projet, en commençant par la représentation de l'étape d'analyse des besoins par un ensemble de diagrammes de cas d'utilisation. Puis nous avons

donné une présentation général de la couche applicative du système en la modélisant par quelques diagrammes de séquence, ensuite nous avons détaillé le niveau communication en précisant les normes et l'architecture adoptées, et enfin nous avons passé au niveau organisationnel des données qui concerne la définition et la détermination de la base de données.

Il ne reste qu'à mettre en œuvre une plateforme qui nous permettra la réalisation de nos applications respectives, ce qui sera l'objet du chapitre prochain.

# *Chapitre V*

## *Réalisation*

## **I. Introduction :**

L'implémentation d'application Android dédiée au monde du paiement nécessite la maîtrise de nombreuses technologies.

Le présent chapitre portera sur la description de l'environnement et les outils de développement de notre application, et nous terminerons par la présentation de ses fonctionnalités à travers ses différentes interfaces.

## **II. Les bases et le cadre du projet**

Le projet consiste à réaliser une application Android dédié au m-paiement, avant d'entamer la réalisation nous allons présenter ce système d'exploitation.

### **II.1. A propos d'Android**

#### **II.1.1. Système d'exploitation [21]**

Android est un système d'exploitation mobile pour smartphones, tablettes, Smart Watch et smart TV.

Développé en Java par l'Open Handset Alliance, ce système est en Open Source. Appartenant aujourd'hui à Google.

#### **II.1.2. Android API [21]**

L'API<sup>34</sup> Android est une collection de packages qui définissent des classes facilitant l'utilisation des fonctionnalités et des appareils Android.

De plus le SDK<sup>35</sup> Android propose les bibliothèques et outils de développements essentiels pour construire, tester et déboguer les applications Android.

#### **II.1.3. Développement d'application Android**

##### **II.1.3.1. Composants de l'application [22]**

Une application Android est structurée en blocks. Ses composants sont de quatre types :

---

<sup>34</sup> Application Programming Interface. C'est un ensemble d'outils aidant à la construction d'un logiciel ou d'une application. Le niveau d'API Android (API Level) correspond à une version d'Android. Par exemple la version 1.6 d'Android correspond au niveau d'API 4.

<sup>35</sup> Software Development Kit. Il s'agit d'un ensemble complet d'outils de développement logiciel (débugueur, bibliothèques, émulateur...).

- *Activities*, qui représentent un unique écran avec une interface utilisateur ;
- *Services* qui fonctionnent en arrière-plan pour effectuer des opérations de longue durée ou effectuer des travaux pour les processus distants ;
- *Content Providers* qui gèrent un ensemble de données d'applications partagées ;
- *Broadcast Receivers* qui sont des composants répondant aux annonces diffusées à l'échelle du système.

Chaque type a des buts distincts et un cycle de vie qui définit comment créer et détruire le composant. Le système du téléphone utilise ces composants comme points d'entrée dans l'application.

### II.1.3.2. Activités

Une application Android est généralement composée de plusieurs activités liées les unes aux autres. Dans la figure V.1 nous allons donner le cycle de vie d'une activité.

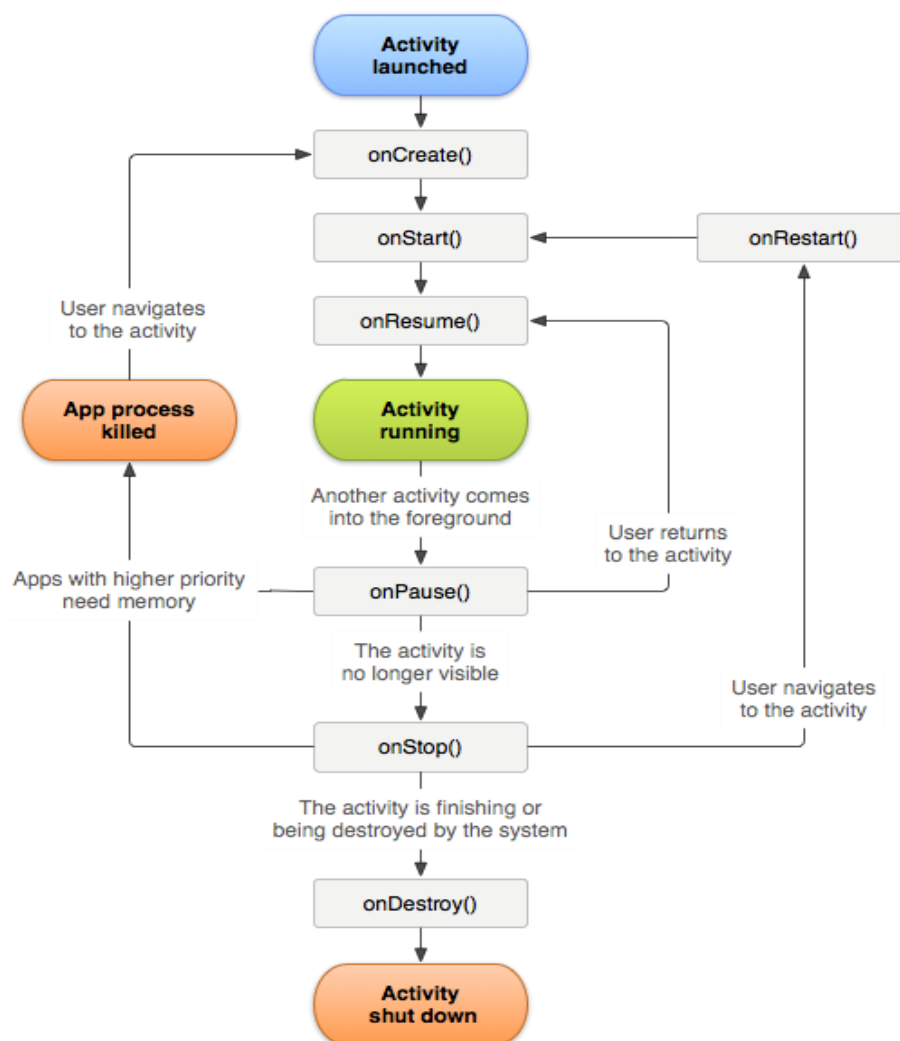


Figure V.1 : le cycle de vie d'une Activité

Nous allons décrire l'ensemble des fonctions liées au cycle de vie d'une application :

- onCreate() : est appelée au premier lancement de l'activité, ou si celle-ci est ressuscitée.
- onStart() : est exécutée après chaque onCreate() ou onRestart(), elle permet de charger les données lorsque l'activité est visible par l'utilisateur.
- onRestart() : est lancée lorsque l'activité repasse au premier plan après avoir été arrêtée via onStop().
- onResume() : est exécutée lorsque l'activité est passée en avant plan (permet la mise à jour des données).
- onPause() : est appelée chaque fois que l'utilisateur change d'activité ou quand celui-ci ferme l'activité (permet la sauvegarde des données)
- onStop() : est lancée avant chaque mise en sommeil de l'activité (permet la libération des ressources).
- onDestroy() : est exécutée lors de l'arrêt de l'activité, elle met fin au cycle de vie.

### **II.1.3.3. Layout**

La structure visuelle d'une activité est décrite dans un fichier .xml appelé layout. Ainsi, chaque activité a son propre fichier layout pour la décrire. Par exemple, on associera l'activité MainActivity au fichier activity\_main.xml qui est généré automatiquement lors de la création de l'activité dans le projet.

### **II.1.3.4. Fichier Manifest**

Le fichier Manifest indique au système qu'un composant qui veut se lancer existe déjà. L'application doit déclarer tous ses composants, notamment les activités, dans un fichier AndroidManifest.xml.

Ce fichier comprend également les informations concernant les permissions requises par l'application, le niveau minimum de l'API, les caractéristiques logicielles et matérielles et les librairies requises.

## **II.2. Les objectifs du projet**

La finalité du projet était de réaliser une application Android capable de lire et transmettre les informations à travers une puce NFC. L'application devrait ainsi jouer le rôle d'une carte

bancaire sans contact, et permettre d'effectuer le paiement mobile, on réalisant trois applications :

- une pour le client nommé SmartPay
- la deuxième pour le commerçant(TPE), nommé SmartTPE.
- Un serveur de test nommé BNAServerTest

### **III. La mise en œuvre du projet**

La réalisation du projet a nécessité la prise en main d'outils tels que l'environnement de développement Android Studio ou l'API Android NFC.

Dans ce qui suit nous allons présenter Android Studio, l'API Android NFC et les smartphones utilisés au cours du projet pour la réalisation de l'application.

#### **III.1. Android Studio.**

Android Studio est l'environnement de développement intégré (EDI<sup>36</sup>) officiel pour développer des applications Android. Il est basé sur IntelliJ IDEA<sup>37</sup> et a été développé par Google. [23]

#### **III.2. L'API Android NFC [24]**

L'API d'Android propose un accès à la fonctionnalité NFC d'un téléphone grâce au package `android.nfc`. Ce dernier permet aux applications de lire et écrire des messages dans les tags NFC.

Le package contient plusieurs classes dont on peut citer :

- *NfcManager* : Gestionnaire de haut niveau, utilisé pour obtenir le *NfcAdapter* de l'appareil
- *NfcAdapter* : Représente l'adaptateur NFC de l'appareil, qui est le point d'entrée pour effectuer des opérations NFC.

*CardEmulation* : c'est le package principale qui contient l'ensemble des outils et classes permettant la manipulation du mode emulation de carte (HCE : Host Card Emulation).

*HostApduService* : c'est le service HCE implémenté, il offre deux méthodes :

- `processCommandeApdu` : en implémentant cette méthode, le service pourra répondre aux commandes APDU reçus du TPE

---

<sup>36</sup>Les Environnement de Développement Intégrés rassemblent dans un même outil tous les éléments nécessaires à la programmation (éditeur de texte, compilateur, débogueur...).

<sup>37</sup>C'est un EDI Java pour le développement de logiciel développé par JetBrains.



- onDeactivated : en implémentant cette méthode, le service lancera des traitements en cas de perte de connexion NFC.
- IsoDep : la classe implémentée par le lecteur TPE, cette classe permet la manipulation des Tag répondant à la norme iso 14443-4.

Enfin, le package `android.nfc.tech` propose des classes qui donnent accès aux caractéristiques de la technologie d'un tag, qui varie selon le type de tag scanné (voir l'annexe 2). Un tag scanné peut supporter par plusieurs technologies.

### **III.3. Les APDU :**

**Application Protocol Data Unit** ou **APDU** est un message échangé entre une carte à puce et un lecteur de carte à puce. Il est normalisé et décrit dans l'ISO 7816 partie 4 « Cf. chapitre IV ».

### **III.4. Les smartphones**

L'application créée au cours de ce projet peut être lancée sur un émulateur (fonctionnalité fournie par SDK Android) ou sur un téléphone réel. Le test de l'application sur l'émulateur a montré les limites de l'émulateur qui ne possède pas la puce NFC.

Aussi, nous avons utilisé 3 téléphones réels pour tester notre application, ceux-ci étant doté de la version 4.4.2 d'Android au plus et bénéficiant de la fonctionnalité NFC.

Ces smartphones sont :

- Un Samsung Galaxycore prime
- Un LG G4;
- Samsung Galaxy S4.

### **III.5. Planification du projet**

Après s'être approprié le sujet et avoir fait quelques recherches sur le NFC ainsi que sur les applications Android existantes, nous avons entamé le projet en commençant par réaliser la partie client ensuite le TPE et à la fin le serveur qui doit jouer le rôle de la banque et de la SATIM.

## **IV. Réalisation**

Dans cette partie nous allons présenter les réalisations effectuées sur le projet.

#### IV.1. SmartPay

L'application se compose de 7 Activités, celles-ci sont déclarées dans un fichier *AndroidManifest.xml* et leur structure visuelle est décrite dans des fichiers *Layout* (fichier de mise en page).

##### IV.1.1. Layout

Chaque activité possède son propre *Layout* (fichier de mise en page). Celui-ci permet de décrire la structure visuelle de l'application.

Par exemple : la figure V.2 décrit la mise en page XML de l'activité d'entrée (*MainActivity*):



Figure V.2 : Interface principale de « SmartPay »

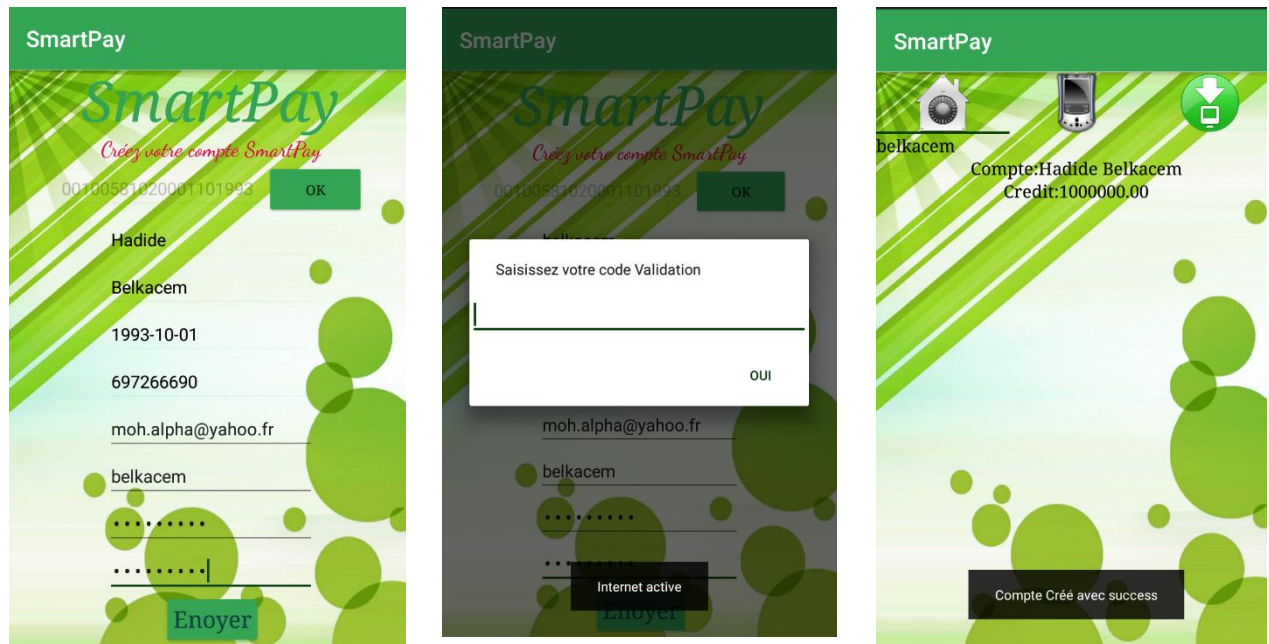
##### IV.1.2. Activities

Le point d'entrée de l'application est l'Activity *MainActivity*, elle offre la possibilité à l'utilisateur de choisir entre l'inscription ou la connexion à un compte déjà existant.

Si on choisit l'inscription, l'application ouvre une nouvelle activité *InscriptionActivity* qui permet à l'utilisateur de s'inscrire avec un compte de banque comme le montre la figure V.3.

Si il choisit de se connecter à l'espace compte l'application ouvre l'activité *ConnectionActivity*

• **Inscription :**



**FigureV.3 : Les étapes de l'inscription**

1. le client saisie le numéro du compte bancaire, une requête est envoyée au server pour la vérification ;
2. le server renvoie les données au client (nom, prénom, date de naissance, et numéro...) puis l'application les affichent ;
3. le client saisie le login et un mot de passe et envoie une requête d'inscription au serveur ;
4. le serveur traite les informations et envoie un code de validation par mail ;
5. Le client saisi le code, puis une requête de vérification est envoyée au serveur ;
6. Le serveur active l'application et envoie la réponse à l'application ;
7. L'application affiche l'interface principale avec des informations du compte.

- **Transaction** : La figure V.4 montre l'activité qui permet au client de payer.

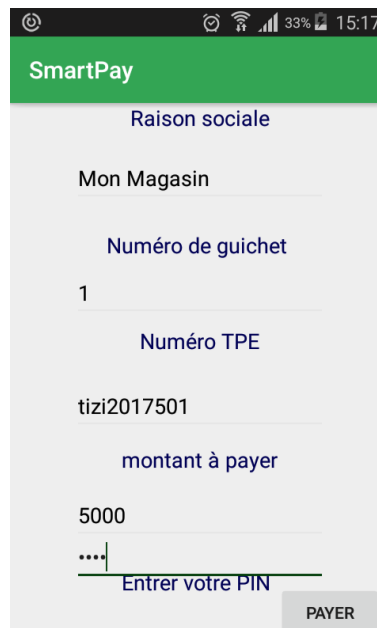


Figure V.4 :L'interface transaction du client

#### IV.1.3. Fichier Manifest

Pour pouvoir créer une application Android capable de gérer la fonctionnalité NFC du téléphone, le fichier AndroidManifest.xml doit être correctement préparé.

- **Permission d'utiliser NFC**

Pour pouvoir utiliser la fonctionnalité NFC du téléphone, la permission suivante doit être déclarée :

```
<uses-permission android:name="android.permission.INTERNET" />

<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

<uses-permission android:name="android.permission.NFC" />
```

- **Version minimale d'Android SDK**

Le support de l'écriture, de la lecture et l'utilisation au premier plan du mode HCE sont disponibles depuis l'API 19 d'Android.

```
defaultConfig {
    applicationId "com.example.captainmohakli.smartpay"
```

```

    minSdkVersion 19
    targetSdkVersion 23
    versionCode 1
    versionName "1.0"
    testInstrumentationRunner
"android.support.test.runner.AndroidJUnitRunner"
}

```

- **Fonctionnalité NFC**

Dans le but de faire apparaître notre application sur le PlayStore uniquement aux appareils équipés du matériel NFC, nous avons dû déclarer cette fonctionnalité :

```

<uses-feature
    android:name="android.hardware.nfc.hce"
    android:required="true" />

```

- **Service:**

```

• <service
    android:name=".CardService"
    android:exported="true"
    android:permission="android.permission.BIND_NFC_SERVICE">
    <intent-filter>
        <action
            android:name="android.nfc.cardemulation.action.HOST_APDU_SERVICE" />
        </intent-filter>

    <meta-data

        android:name="android.nfc.cardemulation.action.host_apdu.service"
        android:resource="@xml/apduservice" />
    </service>

```

- **Implémentation du service HCE:**

```

• public class CardService extends HostApuService {
    private static final String PIN_FILTER =
"com.exemple.belkacem.hceapp.PIN_VERIFICATION";

    // Abstract super class constant overrides
    public static final String KEY_DATA = "data";
    public static final int MSG_RESPONSE_APDU = 1;

    //l'AID de l'applet

```

```

private static final String AID = "F222222222";
//-----
//les déclaration des reponses et des erreurs gérer
// "OK" Mot d'état envoyé en réponse à la commande SELECT AID
(0x9000)
private static final byte[] OK_SW = HexStringToByteArray("9000");

// "UNKNOWN" Mot d'état envoyé en réponse à une commande APDU non
valide (0x0000)

private static final byte[] SELECT_APDU = BuildSelectApu(AID);
private static final byte[] CLASS_NOT_SUPPORTED =
HexStringToByteArray("6E00") ;//normalisé iso 7816-4 page 11
private static final byte[] UNKNOWN_CMD_SW =
HexStringToByteArray("0000");

private static final byte[] UNKHOWN_AUTHENTICATION_KIND =
HexStringToByteArray("6983");
private static final byte[] UNKNOWN_CHANGE_DATA_CMD =
HexStringToByteArray("6A01");
private static final byte[] FUNCTION_NOT_SUPORTED =
HexStringToByteArray("6A81");
private static final byte[] INCORRECT_PARAMETERS =
HexStringToByteArray("6A86");

```

....

```

• public byte[] processCommandApu(byte[] commandApu, Bundle extras) {

    switch (commandApu[0]) {
        //tester le bit class CLA
        case BNA_CLA:
            switch (commandApu[1]) {
                case INS_SELECT:
                    String account = "12536225145";
                    byte[] accountBytes = account.getBytes();
                    //Log.i(TAG, "Sending account number: " +
account);

                    return ConcatArrays(accountBytes, OK_SW);
                case INS_CHANGE_REFERENCE_DATA:

```

```

        switch (commandApu[2]) {
            case 0x00:
                nomCommercant=
decodeByteArray(getDataFromApu(commandApu));

            case 0x01:

prenomCommercant=decodeByteArray(getDataFromApu(commandApu));
                return OK_SW;
            case 0x02:
                codeCommercant=
decodeByteArray(getDataFromApu(commandApu));
                return OK_SW;

            case 0x03:
                montantApayer=
decodeByteArray(getDataFromApu(commandApu));

sendInformation(nomCommercant,prenomCommercant,codeCommercant,montant
Apayer);

                return OK_SW;
            default:
                return UNKNOWN_CHANGE_DATA_CMD;
        }
    }
}

```

## IV.2. SmartTPE

L'application se compose de 6 Activités, celles-ci sont déclarées dans un fichier *AndroidManifest.xml* et leur structure visuelle est décrite dans des fichiers *Layout*.

### IV.2.1. Layout

Chaque activité possède son propre *Layout*. Celui-ci permet de décrire la structure visuelle de l'application.

Par exemple, la figure V.5 décrit la mise en page XML de l'activité d'entrée *AccueilActivity*:



Figure V.5 :L'interface principale de SmartTPE

#### IV.2.2. Activités

Le point d'entrée de l'application est l'Activity *AccueilActivity*, elle offre la possibilité au commerçant de lancer le TPE, en s'identifiant avec un Login et un mot de passe donnés par la banque (la figure V.6).

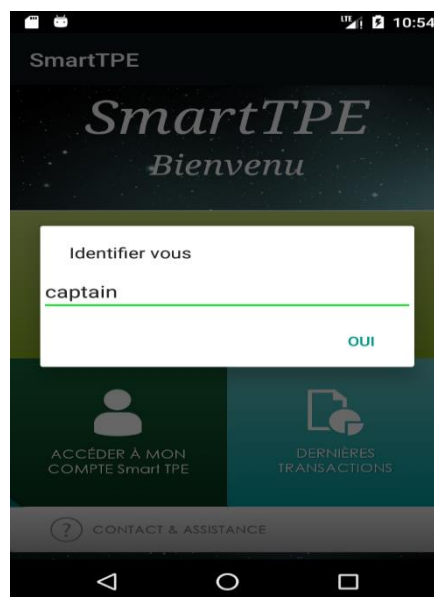


Figure V.6 :L'activité Accueil de SmartTPE

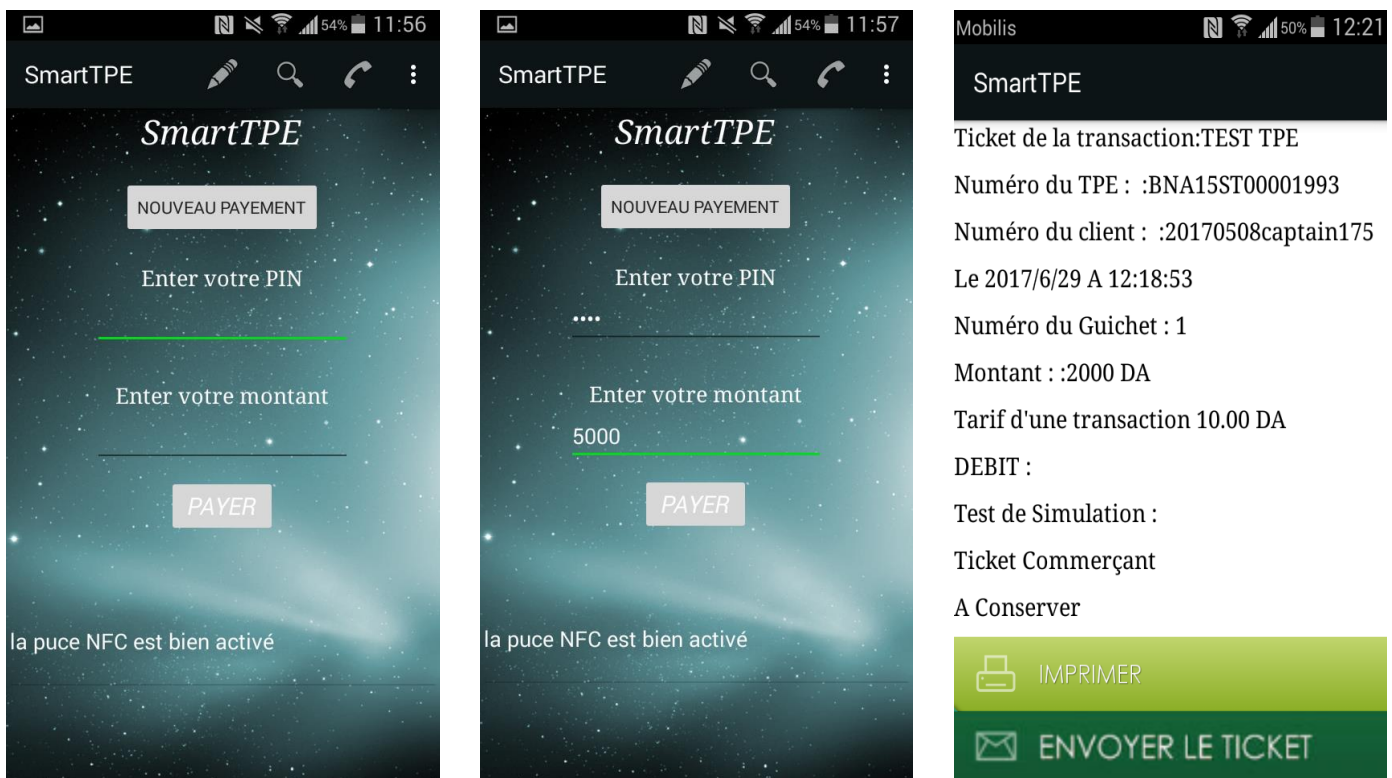


L'application ne peut être utilisée que par un smartphone validé au niveau de la banque avec les identifiants du téléphone.

**Déroulement :**

1. Le commerçant saisie le login et valide ;
2. Le commerçant saisie le mot de passe et valide ;
3. Le système affiche l'interface principale de l'application « *SmartTPE* »

- **Transaction** : La figure V.7 explique les étapes d'une transaction NFC.



**Figure V.7 : Le déroulement de transaction**

**Déroulement :**

1. Le commerçant saisie le code PIN ;
2. Il saisit le montant ;
3. Puis clique sur payer ;
4. La connexion NFC s'établit ;
5. Après la validation du code PIN par le client, l'application envoie les coordonnées du client pour le serveur afin de les vérifier.

6. Après la validation le système confirme la transaction au client, et envoi le bon de caisse ;
  7. L'application affiche au commerçant le bon de caisse envoyé.
- **Historique des transactions** : La figure V.8 présente l'historique des transactions.

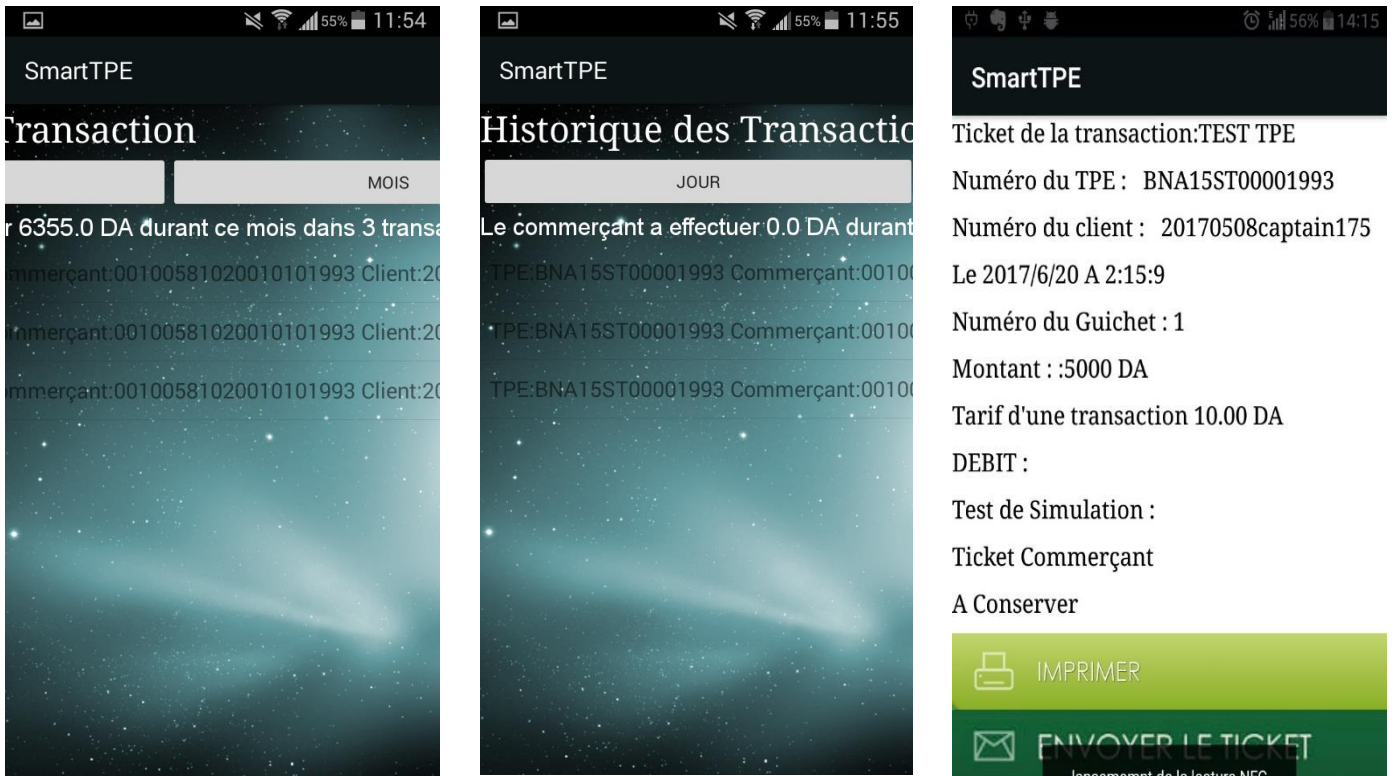


Figure V.8 : Historique et statistique des transactions

#### Déroulement :

1. Le commerçant accède à son compte ;
2. Il clique sur le bouton « Historique des transactions ».
3. Le système lui affiche toutes les transactions effectuées durant la journée, le mois ou l'année.
4. En cliquant sur une transaction, l'application lui affiche le bon de caisse.

#### IV.2.3. Fichier Manifest

Pour pouvoir créer une application Android capable de gérer la fonctionnalité NFC du téléphone, le fichier AndroidManifest.xml doit être correctement préparé.

- **Permission d'utiliser NFC**

Pour pouvoir utiliser la fonctionnalité NFC du téléphone, la permission suivante doit être déclarée :

```


- <uses-permission android:name="android.permission.NFC" />
- <uses-permission android:name="android.permission.INTERNET" />
- <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
- <uses-permission android:name="android.permission.READ_PHONE_STATE" />

```

- **Déclaration d'un Intent :**

Pour être sûr que l'application se lance à la détection d'un tag TECH, l'intente suivant doit être utilisé.

```
<activity android:name=".AccueilActivity"
android:screenOrientation="portrait">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />

        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
    <intent-filter>
        <action android:name="android.nfc.action.TECH_DISCOVERED" />
    </intent-filter>

    <meta-data
        android:name="android.nfc.action.TECH_DISCOVERED"
        android:resource="@xml/nfc_tech_filter" />
</activity>
```

- **Déclaration des technologies**

Afin de pouvoir traiter les différentes technologies NFC, celles-ci doivent être déclarées dans un fichier .xml situé dans les ressources du projet :

```
<?xml version="1.0" encoding="utf-8"?>
<!-- This file is used as part of the filter for incoming NFC
TECH_DISCOVERED intents. -->
<resources xmlns:android="http://schemas.android.com/apk/res/android">
    <!-- Android's host card emulation feature only supports the IsoDep
protocol. -->
    <tech-list>
        <tech>android.nfc.tech.IsoDep</tech>
    </tech-list>
</resources>
```

- *Implémentation de la classe lecture IsoDep dans le Lecteur:*

```
public class PaiementCardReader implements NfcAdapter.ReaderCallback {
    private static final String TAG = "BnaSmartTPE";
    // AID for our loyalty card service.
    private static final String CARD_AID = "F222222222";

    // ISO-DEP command HEADER for selecting an AID.
    // Format: [Class | Instruction | Parameter 1 | Parameter 2]
    private static final String SELECT_APDU_HEADER = "00A40400";
    private static final String VERIFIE_PIN_HEADER="00820100";

    private static final String NOM_MAGASIN_HEADER ="00240000";
    private static final String NUM_GUICHET_HEADER ="00240100";
    private static final String NUM_TPE_HEADER ="00240200";
    private static final String MONTANT_HEADER="00240300";
```

....

```
@Override
public void onTagDiscovered(Tag tag) {

    isoDep= IsoDep.get(tag);
    if (isoDep != null) {

        try {
            // Connect to the remote NFC device
            isoDep.connect();
```

```

        // Build SELECT AID command for our loyalty card service.
        // This command tells the remote device which service we wish
to communicate with.
        Log.i(TAG, "Requesting remote AID: " + CARD_AID);
        byte[] command = BuildSelectAdu(CARD_AID);

        // Send command to remote device
        Log.i(TAG, "Sending: " + ByteArrayToHexString(command));
        byte[] result = isoDep.transceive(command);
        // If AID is successfully selected, 0x9000 is returned as the
status word (last 2
        // bytes of the result) by convention. Everything before the
status word is
        // optional payload, which is used here to hold the account
number.

        /*-----data -----sw1*****sw2*/

        int resultLength = result.length;

        byte[] statusWord = {result[resultLength-2],
result[resultLength-1]};
        byte[] payload = Arrays.copyOf(result, resultLength-2);
        // si l'applet n'est pas sélectionné on va la sélectionner
        if(!SELECT_OK){
            if (Arrays.equals(SELECT_OK_SW, statusWord)) {
                // The remote NFC device will immediately respond with its
stored account number
                String accountNumber = new String(payload, "UTF-8");
                //          Log.i(TAG, "Received: " + accountNumber);
                // Inform CardReaderFragment of received account number
                mCardCallback.get().logMessageCard(accountNumber);

                SELECT_OK = true;
            }else {
                mCardCallback.get().logMessageCard("echecs de selection");
                //----- traiter le cas de non sélection de la
carte -----
            }
        }

```

```

    }

    if (SELECT_OK && (!nomMagasinIsSend)) {

        mCardCallback.get().logMessageCard("connexion établit
\n envoi du nom \n" +
            " attente de la reponse");
        byte[] reponse1 =
isoDep.transceive(makeApuData(NOM_MAGASIN_HEADER,
            nomMagasinAPDU, (byte) 0));
        if (reponseIsOk(structureR_APDU(reponse1))) {
            mCardCallback.get().logMessageCard("nom bien
reçus");
            nomMagasinIsSend = true;
        } else {
            mCardCallback.get().logMessageCard("nom pas recus
!!!!");
            //----- traiter le cas de non reception
du nom de la carte
            // -----
        }
    }
}

```

### IV.3. Simulation d'un serveur de la banque

Notre serveur est constitué d'une classe ServerS.java présentée dans la figure V.9 programmée par les sockets qui gère toutes les demandes du client et du commerçant. Et un serveur mail illustré dans la figure V.10 qui envoie des données à la boîte mail du client.

```
1
2 import java.io.BufferedReader;
3 import java.io.IOException;
4 import java.io.InputStreamReader;
5 import java.io.ObjectInputStream;
6 import java.io.ObjectOutputStream;
7 import java.io.PrintWriter;
8 import java.net.InetAddress;
9 import java.net.NetworkInterface;
10 import java.net.ServerSocket;
11 import java.net.Socket;
12 import java.util.Arrays;
13
14 import javax.naming.Context;
15
16 public class ServerS {
17
18     public static void main(String[] args)
19     {
20
21         // TODO Auto-generated method stub
22
23         ServerSocket socket;
24         try
25         {
26             socket = new ServerSocket(93);
27
28
29             Thread t = new Thread(new acceptor_client(socket));
30
31             t.start();
32             System.out.println("le serveur est démarré");
33 }
```

Figure V.9 : le code java de la classe ServerS

```
1 import java.util.Properties;
2 import javax.mail.Message;
3 import javax.mail.MessagingException;
4 import javax.mail.Session;
5 import javax.mail.Transport;
6 import javax.mail.internet.InternetAddress;
7 import javax.mail.internet.MimeMessage;
8
9 public class AnotherMail {
10
11 public static void main(String... args) {
12
13 }
14 public void Mailsend(String v, String m,String pin){
15     String host = "smtp.gmail.com";
16     String from = "mouhhakli@gmail.com";
17     String pass = "captain moh akli 2017";
18     Properties props = System.getProperties();
19     props.put("mail.smtp.starttls.enable", "true"); // added this line
20     props.put("mail.smtp.host", host);
21     props.put("mail.smtp.user", from);
22     props.put("mail.smtp.password", pass);
23     props.put("mail.smtp.port", "587");
24     props.put("mail.smtp.auth", "true");
25
26     String[] to = {m}; // added this line
27     try {
28         Session session = Session.getDefaultInstance(props, null);
29         MimeMessage message = new MimeMessage(session);
30         message.setFrom(new InternetAddress(from));
31
32         InternetAddress[] toAddress = new InternetAddress[to.length];
33     }
```

Figure V.10 : le code java de serveur mail

## V. Conclusion

Durant ce chapitre on a donné une vue générale sur les différents outils et IDE utilisés pour développer notre projet de fin d'étude.

On a terminé par donner une présentation générale des différentes interfaces graphiques présent sur nos trois applications SmarPay, SmartTpe, et BNAServerTest et quelques morceaux de codes source.



# *Conclusion*

## *générale*

## ***Conclusion générale***

---

L'objectif fixé au début de notre travail consistait en la conception et la mise en œuvre d'une application Android dédié au paiement électronique en utilisant le standard NFC.

Au terme de notre travail, nous avons pu atteindre notre objectif, l'application réalisée permet :

- Au client grâce au service SmartPay :
  - ✓ Payer le commerçant via son Smartphone ;
  - ✓ Avoir un compte SmartPay ;
  - ✓ Consulter son compte bancaire en ligne ;
  - ✓ Accéder à l'historique des transactions et des bons de caisse ;
  - ✓ Visualiser ses statistiques d'achats.
- Au commerçant via l'application SmartTPE:
  - ✓ D'encaisser sur le client ;
  - ✓ Avoir son compte SmartTPE ;
  - ✓ Consulter son compte bancaire en ligne ;
  - ✓ Accéder à l'historique des transactions et des bons de caisse ;
  - ✓ Visualiser ses statistiques de vente.
- Enfin pour la banque auquel on a conçu une extension pour son serveur existant, lui permettant :
  - ✓ D'enregistrer ses clients (commerçants et acheteurs) ;
  - ✓ De générer les transactions ;
  - ✓ De garder trace de la transaction.

Bien que tous nos objectifs initiaux soient atteints, notre système doit cependant être amélioré en y apportant les caractéristiques suivantes :

- Développer un module pour l'application SmartPay pour payer les commerçants sur un TPE compatible NFC standard.
- Développer un module pour l'application SmartTPE pour encaisser les cartes bancaire sans contact.
- Développer un module de géolocalisation pour localiser les magasins offrant le service de paiement sans contact.
- Développer des modules de sécurité biométrique pour les applications SmartPay et SmartTPE.
- Accroître la sécurité en implémentant des méthodes cryptographiques.

## ***Conclusion générale***

---

- Développer une extension pour le web afin de permettre le paiement sécurisé dans les sites e-commerce.

Arrivé à terme de notre travail, Nous espérons que les résultats auxquels nous sommes parvenus puissent répondre aux besoins des commerçants et de leurs clients. Tout comme nous espérons que ce présent mémoire puisse servir de référence de travail pour les étudiants à venir

## ***Bibliographie***

[1] : Benchohra KARA, Le Commerce électronique en Algérie : défis et perspective, Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'Etat en planification et statistique. Option : « Analyse de la conjoncture économique et technique de prospective », **Institut National de la Planification et de la Statistique**, 2007/2008.

[3] : Ben Si Amara Lyazid, Ait Aouit Tahar, La personnalisation dans le commerce électronique, Mémoire de fin d'étude master 2 en informatique option CPI, université UMMTO, 2013/2014.

[9] : Joly Cathie-Roaslie, Paiement en ligne : Sécurisation juridique et technique, 2005, cote [Inf 41/1].

[11] : BOUBAKER Nobel El Houssine, Le paiement sur internet, Université Du Centre, Institut Supérieur De Gestion De Sousse, Master Spécialisé : Commerce International et Technologie de l'Information, 2002/2003

[20] Samia Bouzebrane et Pirre Paradina : les cartes à puce, éditeur Lavoisier, Paris 2013 cote [AFO23]

[22] : Mark L. Murphy, L'art du développement Android : Traduit par Éric Jacoboni, avec la contribution d'Arnaud Farine, éditeur : Pearson, 2009

[24] : Pierre Métivier, Le NFC mobile télécommande de notre quotidien, éditeur : Afnor, 2015

## ***Webographie***

- [2] : <http://www.definitions-marketing.com/definition/M-commerce/?page=article>
- [4] : <https://business.trustedshops.fr/blog/2016-chiffres-professionnels-e-commerce/>
- [5] : <http://www.journaldunet.com/ebusiness/commerce/1009561-chiffre-d-affaires-e-commerce-monde/>
- [6] : [http://www.huffpostmaghreb.com/2016/05/03/algerie-e-commerce-pas-pr\\_n\\_9829126.html](http://www.huffpostmaghreb.com/2016/05/03/algerie-e-commerce-pas-pr_n_9829126.html)
- [7] : [http://www.huffpostmaghreb.com/2014/08/16/e-commerce-algerie-vente-en-ligne\\_n\\_5684317.html](http://www.huffpostmaghreb.com/2014/08/16/e-commerce-algerie-vente-en-ligne_n_5684317.html)
- [8] : [http://www.huffpostmaghreb.com/2016/10/04/paiement-en-ligne\\_n\\_12336286.html](http://www.huffpostmaghreb.com/2016/10/04/paiement-en-ligne_n_12336286.html)
- [10] : [https://fr.wikiversity.org/wiki/Paiement\\_mobile\\_\(m-paiement\)/Introduction\\_et\\_d%C3%A9finition](https://fr.wikiversity.org/wiki/Paiement_mobile_(m-paiement)/Introduction_et_d%C3%A9finition)
- [12] : <https://fr.wikipedia.org/wiki/Mon%C3%A9tique>
- [13] : [www.definitions-marketing.com/definition/nfc/](http://www.definitions-marketing.com/definition/nfc/)
- [14] : <http://www.journaldunet.com/business/pratique/dictionnaire-economique-et-financier/16506/banque-definition-traduction-et-synonymes.html>
- [15]: <http://www.bna.dz/index.php/fr/>
- [16] : <http://www.satim-dz.com/>
- [17] : <https://www.iso.org/fr/home.html>
- [18] : [http://www.cardwerk.com/smartcards/smartcard\\_standard\\_ISO7816-4\\_5\\_basic\\_organizations.aspx](http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx)
- [19] : <http://www.emvco.com/>
- [21] : <https://www.android.com/>
- [23] : [https://fr.wikipedia.org/wiki/Android\\_Studio](https://fr.wikipedia.org/wiki/Android_Studio)

# *Annexe*

### **I. Aspects juridiques :**

La société humaine est entrée depuis près d'un quart de siècle ou plus, dans une ère de communication et de développement technologique sans précédent. En plus, des espaces juridiques classiques (terrestre, maritime et aérien), un nouvel espace est apparu, à savoir l'espace virtuel. Ainsi, de nouveaux médias ont commencé à envahir la société, dont l'Internet est de loin le média le plus influant dans la vie sociale des gens.

#### **I.1 Les problèmes causés par l'informatique :**

L'informatique en générale et internet en particulier remettent en cause toute notre vision et toute l'architecture du droit national, communautaire et international. De ce fait, l'informatique pose de nombreux problème :

- ✓ dans la structuration du droit : le droit est territorial et national. Il n'existe pas ou peu de réglementation commune mondiale : droit français, droit européen, DIP. L'informatique (internet) n'a pas de frontière et est de plus en plus compliqué par la création de réseaux mondial : plates-formes de développement, moteurs de recherche, hébergeurs...
- ✓ dans le respect des libertés publiques : respect de la vie privé, de la liberté d'expression, liberté de la presse, échange d'information, mouchard électronique, base de données sensible.
- ✓ dans le respect de l'ordre public : fichier Edwige, lutte contre le terrorisme, racisme, antisémitisme.
- ✓ dans la conclusion des contrats : le droit des contrats est fondé sur un écrit et une signature manuelle entre deux personnes soumise au même droit.
- ✓ des règles en matière de responsabilité : responsabilité civile, pénale, responsabilité des hébergeurs, des prestataires, de Google.
- ✓ dans le droit du travail : surveillance des salariés, chartes informatiques, tracts par internet, contrôle des e-mails, utilisation de l'outil informatique par les salariés.
- ✓ dans les pratiques commerciales : délai de livraison, fraude, abus de position dominante, contrefaçon, recel, escroquerie.

### I.2 La fraude informatique :

Lorsque l'on évoque la fraude informatique, nous distinguons trois types d'infractions pénales :

- ✓ la fraude sur les STAD<sup>38</sup>
- ✓ l'atteinte aux libertés individuelles
- ✓ les infractions classiques appliquées à l'informatique (vol, contrefaçons...)

#### I.2.1 L'action frauduleuse sur les STAD

##### 1) L'intrusion frauduleuse dans le système

Le fait d'accéder ou de se maintenir frauduleusement dans un STAD est puni de **2 ans de prison et de 30 000 €** d'amende ou **3 ans de prison et 45 000 €** d'amende lorsque la présence provoque un préjudice<sup>39</sup>, Pour que cette infraction existe, il faut :

- ✓ une condition préalable : l'existence d'un STAD
- ✓ un élément matériel : un accès ou un maintien dans le STAD
- ✓ un élément moral : une intention frauduleuse

Exemple : modification du système de vérification pour ne pas déclencher des blocages de sécurité.

*Dans la loi algérienne est puni d'une peine d'emprisonnement de 3 mois à 1 ans et d'une amende de 50.000 DA à 100.000 DA se maintient frauduleusement dans tout ou partie d'un système automatique, l'article 394 bis de loi n°04-15 du 10 novembre 2004 modifiant et complétant l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal. JO n°71 du 10 novembre 2004.*

##### 2) La manipulation des STAD

Le piratage d'un STAD pour y introduire volontairement des perturbations est plus grave. On distingue trois cas de figure :

---

<sup>38</sup> STAD : système de traitements automatisé de données

<sup>39</sup>Préjudice : la suppression, modification des données ou altération du système



- ✓ la perturbation des données : le fait d'entraver ou de fausser le fonctionnement d'un STAD est puni de **5 ans de prison et 75 000€**. Ex virus, bombes logiques, logiciels piégés, détournements de code secrets.
- ✓ l'altération des données: le fait d'introduire frauduleusement des données ou de supprimer ou de modifier des données sont puni de **5 ans de prison et de 75 000 €**.  
Ex : les cookies
- ✓ importation, détention, offre, mise à disposition d'outils pour commettre l'infraction: Le fait, sauf motif légitime, d'importer, de détenir ou d'offrir un équipement, un instrument, un programme pour commettre une infraction informatique est punie de la même manière que ceux qui commettent l'infraction. Ex : auteurs de virus, vers, cheval de Troie, spywares...

Est légitime de posséder ce type de dispositifs, les laboratoires de recherches, les sociétés qui conçoivent des systèmes de lutte contre ces outils.

*Dans la loi algérienne est puni d'un emprisonnement de 6 mois à 3 ans et d'une amende de 500.000 DA à 2000.000 DA introduit frauduleusement des données dans un système automatisé au supprime ou modifie. (Article 394 ter de loi n°04-15 du 10 novembre 2004).*

### 3) Les modalités de répression

Au-delà des peines d'emprisonnement et des amendes, d'autres sanctions pourront être prises comme :

- ✓ la confiscation du matériel : ceci doit être compris au sens très large du terme avec notamment les logiciels, les documents les notes, les modes d'emploi...
- ✓ les privations de certains droits : **pendant 5 ans**, le fraudeur sera privé de ses droits civiques, ne pourra pas accéder aux marchés publics, ne pas émettre de chèque...

4) Il y a infraction dès le stade de l'essai donc de la tentative. De plus, la participation à un groupement formé qui commet des fraudes équivaut à avoir commis la fraude (association de malfaiteurs).

### I.2.2 L'atteinte informatique aux libertés individuelles

Exemple : divulgation d'information nominative, collecte frauduleuse de données, enregistrement de données interdites faisant apparaître par exemple les origines raciales ou religieuses, dépassement de la durée de conservation des données.

Les sanctions sont principalement **5 ans de prison et 300 000€** d'amende.

*Dans la loi algérienne est puni d'un emprisonnement de 6 mois à 3 ans et d'une amende de 50.000 DA à 300.000 DA porte volontairement atteinte à l'intimité de la vie privée d'autrui en captant, enregistrant sans l'autorisation des communications des paroles prononcées à titre privé ou confidentiel ( article 303 bis (nouveau) ajouté par la loi n°06-23 du 20 décembre 2006 modifiant et complétant l'ordonnance n°66-156 du 8 juin 1966 portant code pénal. JO n° 84 du 24 décembre 2006).*

### I.2.3 Les délits généraux

#### 1) la falsification de documents informatisés

Est une fausse toute altération frauduleuse de la vérité de nature à causer un préjudice par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée. En principe, il est puni de **3 ans d'emprisonnement et de 45 000€**.

*Dans la loi algérienne est puni d'un emprisonnement de 6 mois à 3 ans et d'une amende de 1.500 DA à 15.000 DA la falsification des permis, livrets, cartes, bulletins ou autres documents (article 222 de l'ordonnance n°66-156 du 8 juin 1966 portant le code pénal).*

Attention, la falsification d'une carte de paiement est sanctionnée par **7 ans de prison et 750 000 € d'amende** ainsi que la confiscation de tout le matériel.

*En Algérie est puni d'un emprisonnement de 2 ans à 10 ans et d'une amende de 10.000 DA à 100.000 DA à des fins frauduleuses dans l'exécution des comptes de l'Etat (art 228 bis (nouveau) ajouté par la loi n°01-09 du 26 juin 2001 modifie et complétant l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal. JO n° 34)*

#### 2) le viol du secret

Il est possible de distinguer plusieurs infractions :

- ✓ la violation du secret de fabrication : lorsqu'un logiciel ou un ensemble informatique a été constitué dans l'entreprise et n'est pas encore commercialisé mais se trouve divulgué, il y a viol du secret de fabrication. C'est **2 ans de prison et 30 000 €**.

- ✓ la corruption passive et le trafic d'influence : lorsqu'un employé s'est fait circonvenir par un concurrent, il y a corruption ou influence. Selon le cas la sanction peut aller jusqu'à **10 ans de prison et 1 500 000€ d'amende**
- ✓ délit d'initié ou d'initiateur : c'est le fait d'acheter ou de vendre des informations secrètes sur une entreprise ayant des répercussions sur les cours de la bourse. **2 ans de prison et jusqu'à 1500 000€.**
- ✓ la violation du secret professionnel : **1 an et 15 000 €.**

*Dans la loi algérienne quiconque un travaillant à quelque titre que ce soit dans une entreprise y avoir été communiqué des secrets de l'entreprise, est puni d'un emprisonnement de 2 ans à 5 ans et d'une amende de 500 DA à 10.000 DA (Article 302 de l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal).*

### 3) la contrefaçon

Lorsque un bien informationnels (logiciels, base de données, pages web, produits multimédia...) fait l'objet d'un acte qui n'est pas autorisé par son auteur (reproduction, adaptation, utilisation sans droit...), la personne à l'origine de cet acte commet une contrefaçon. **C'est 3 ans de prison et 300 000 € d'amende.**

Pour le Peer to Peer, il y a un problème. Juridiquement, il y a clairement contrefaçons.

Maintenant, ne faut-il pas distinguer sont qui se contente de télécharger les œuvres offertes par un tiers diffuseur, de ceux qui partagent leurs fichiers au mépris des droits d'auteurs. En effet, dans le premier cas, il y a copies privées dans le cadre d'une utilisation personnel et exclusive, ce qui est toléré. Dans le second cas, il y a clairement diffusion donc contrefaçon.

La future loi tend à régler ce problème.

*En Algérie le coupable du délit de contrefaçon d'une œuvre ou d'une prestation, est puni d'un emprisonnement de 6 mois à 3 ans et d'une amende de 500.000 DA à 1000.000 DA (art 153 de l'ordonnance n°03-05 du 19 juillet 2003 relative aux droits d'auteur et aux droits voisins. JO n° 44 du 23 juillet 2003).*

### 4) L'escroquerie

C'est une manœuvre frauduleuse dans le but d'induire une personne en erreur.

Exemple : l'escroquerie nigérienne encore appelée le scan ou fraude 419 qui consiste à envoyer un courrier électronique proposant une forte récompense pour une aide à sortir de l'argent soi-disant bloqué à l'étranger.

### 5) Le recel

C'est la dissimulation, la détention ou la transmission d'une chose que l'on sait provenir d'un crime ou d'un délit.

Exemple: diffusions de messages publicitaires pour des livres, cassettes... **C'est 5ans et 375000 €.**

*En droit algérien quiconque, sciemment, recèle en tout ou en partie des choses enlevées à l'aide d'un crime ou d'un délit, est puni d'une 1 année au moins et 5 ans au plus et d'une amende de 500 DA à 20.000 DA (Article 387 de l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal).*

### 6) Les atteintes aux intérêts de la nation :

C'est par exemple : livraison d'information à une puissance étrangère (**15 ans et 225 000 €**), *en Algérie toute trahison ou livraison d'information à une puissance étrangère est puni de mort (Article 61 de la loi n° 06-23 du 20 décembre 2006 modifié et complétant l'ordonnance n°66-156 du 8 juin 1966 portant code pénal. JO n°84).*

Sabotage c.-à-d. un attentat technologique (idem sauf s'il est fait pour une puissance étrangère et c'est **20 ans et 300 000€**), atteinte aux secrets de la défense nationale (**7 ans et 300 000 €**), actes de terrorisme (perpétuité)

*En droit algérien est puni de la réclusion perpétuelle, dans l'intention de les livrer à une puissance étrangère des renseignements, objets sont de nature à nuire à la défense nationale ou à l'économie nationale (Article 65 de l'ordonnance n°75-47 du 17 juin 1975 modifié et complétant l'ordonnance n°66-156 du 8 juin 1966. Jon° 53).*

## I.3 Les textes juridiques :

On entend par le cadre juridique formel du commerce électronique, l'ensemble de textes juridiques qui ont été élaborés et adoptés par des institutions étatiques et destinées à être appliqués que ce soit au niveau interne ou international.

### I.3.1 Sur le plan maghrébin

Il existe dans le droit tunisien un ensemble de textes juridiques qui ont vocation pour être appliqués au commerce électronique, l'importance de ces textes n'est pas la même.

**Textes de première importance :**

- ✓ La loi N° 117 du 7 décembre 1992 relative à la protection du consommateur.
- ✓ La loi n°40 du 2 juin 1998 relative aux techniques de vente et à la publicité commerciale.
- ✓ Le code des obligations et des contrats, y compris la loi N°57 du 13/6/2000 modifiant et complétant certains articles du Code des obligations et des contrats.
- ✓ La loi N°83 du 9/8/2000 relative aux échanges et au commerce électroniques.
- ✓ Loi n° 2005-51 du 27 juin 2005, relative au transfert électronique de fonds.

### **Textes de seconde importance :**

- ✓ Loi organique du 27 juillet 2004, relatives à la protection des données à caractère personnel.
- ✓ Loi d'orientation N°2007-13 du 19 février 2007, relative à l'établissement de l'économie numérique.

### **I.3.2 Sur le plan international**

Sur le plan international de nombreux textes relatifs au commerce électronique ont été adoptés, dont notamment :

#### **Textes universels**

- ✓ La loi type sur le commerce électronique : CNUDCI (21ème session 28 mai, 14 juin 1996), modifiée en 2001.

#### **Textes européens :**

- ✓ Directive européenne du 24 octobre 1995 sur la protection des données personnelles.
- ✓ Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance.
- ✓ Directive 1999/93/ce du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, L13/12, JOCE, 19 janvier 2000.
- ✓ Directive européenne du 8 juin 2000, « relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur » («directive sur le commerce électronique»).

Il est à noter qu'il est difficile de délimiter une liste exhaustive des textes internationaux relatifs au commerce électronique. En fait, les textes déjà existants, régissant le commerce international, s'appliquent indirectement au commerce électronique : Telle que la convention de Vienne sur la vente de marchandise de 1980.

## **II. Quelques Notions sur le NFC**

### **II.1 Qu'est-ce que le NFC ?**

Le NFC, Near Field Communication, (ou communication en champ proche) est une technologie permettant d'échanger des données à moins de 10cm, entre deux appareils équipés de ce dispositif. Le NFC est intégré à la plupart de nos terminaux mobiles sous forme de puce, ainsi que sur certaines cartes de transport ou de paiement.

### **II.2 Les modes de fonctionnement**

Le NFC a trois modes de fonctionnement différents :

- Mode peer to peer ;
- Mode émulation de carte ;
- Mode lecteur.

#### **II.2.1 Mode peer to peer**

Ce mode de fonctionnement permet l'échange d'informations entre deux appareils équipés du NFC.

Exemple d'utilisation :

- Un échange de photos entre une tablette et un Smartphone.
- l'ouverture des portières de sa voiture

#### **II.2.2 Mode émulation de carte**

Le terminal mobile fonctionne comme une carte sans contact. La carte SIM du portable peut être utilisée pour stocker des informations chiffrées, et les sécuriser.

Exemples d'utilisations :

- Paiement sans contact.
- Gestion des coupons de réduction ou des points de fidélité dans un magasin.

#### **II.2.3 Mode lecteur**

Le mobile équipé du NFC est capable de lire des « tags » (étiquettes électroniques), pour récolter des informations pratiques, ou pour lancer une action de manière automatique sur un Smartphone.

Exemples d'utilisations :

- Parcours dans un musée
- Automatisation d'une tâche : changer la sonnerie de son téléphone, ou lancer une application, à l'approche du tag NFC.

### ***A propos des tags NFC :***

Un « tag NFC » est une étiquette électronique équipée de la technologie NFC. L'intérêt étant de pouvoir le programmer, de façon à envoyer une information aux appareils situés dans son champ d'action. On peut acheter des tags NFC, à programmer soi-même sur Internet, mais on peut transformer son smartphone en Tag NFC.

## **II.2.4 Sécurité des données avec le NFC**

L'échange de données entre deux appareils équipés du NFC est sécurisé pour deux raisons :

- Le respect de normes (14443 et FeliCa) utilisant des algorithmes de chiffrement et d'authentification.
- La courte distance de communication entre les appareils, qui réduit fortement le risque de vol des données.

## **II.3 Les normes utilisées dans le NFC :**

Pour concevoir des applications qui permettent une interaction avec l'ensemble des terminaux de paiement l'ensemble des cartes de paiement sans contact, nos applications « SmartPay » et « SmartTPE », doivent respecter un ensemble de normes mondial dédié à la technologie NFC, mais aussi au paiement dont on peut citer les normes suivante :

- ISO/IEC 14443-4 ;
- ISO/IEC 7816-4 ;
- EMV.

Le but de cette partie n'est pas de retranscrire les normes citées ci-dessus dans leurs intégralités, mais plutôt d'en présenter la structure. Pour le détail complet de ces normes, il est conseillé de se reporter aux documents de l'ISO.

### II.3.1 La norme ISO/IEC 14443-4

S'il existe plusieurs normes autour des produits sans contact, la plupart d'entre elles ne sont pas utilisées dans des applications de grand volume. On peut citer l'ISO 10536 relative au close coupling pour laquelle la distance de fonctionnement est inférieure au cm ou les ISO 11785 et 14 223 relatives à l'identification animale. Nous ne détaillerons pas ces normes et allons-nous intéresser à la norme ISO/IEC 14443 relatives respectivement aux produits de proximité, fonctionnement jusqu'à 10 cm dédiée en principe pour les cartes de paiement sans contact, les cartes d'identification biométrique comme les passeports et les cartes d'identité.

La norme ISO 14443 se décompose en quatre parties :

- Partie 1 : définit les caractéristiques physiques et mécaniques des produits.
- Partie 2 : décrit la manière dont la carte sans contact est alimentée, ainsi que la fréquence de fonctionnement et les signaux de communication entre la carte et le lecteur. Cette partie de la norme ainsi que la partie 3 sont découpées en deux sections définissant chacune un schéma de communication différent, que l'on nommera type A et type B.
- Partie 3 : définit les phases d'initialisation entre les parties et le traitement de l'anticollision pour le type A et B.
- Partie 4 : décrit la couche applicative des produits ISO. Cette couche est identique quel que soit le type (A ou B) du produit. Elle définit les règles d'échanges des blocs ou le chaînage des commandes.

Dans notre cas nous sommes intéressés par la partie 4 qui définit la couche applicative de la norme 14443-4 la figure 4.12 montre Les trames ISO 14443-4 transportent des APDUs (ISO 7816-4).

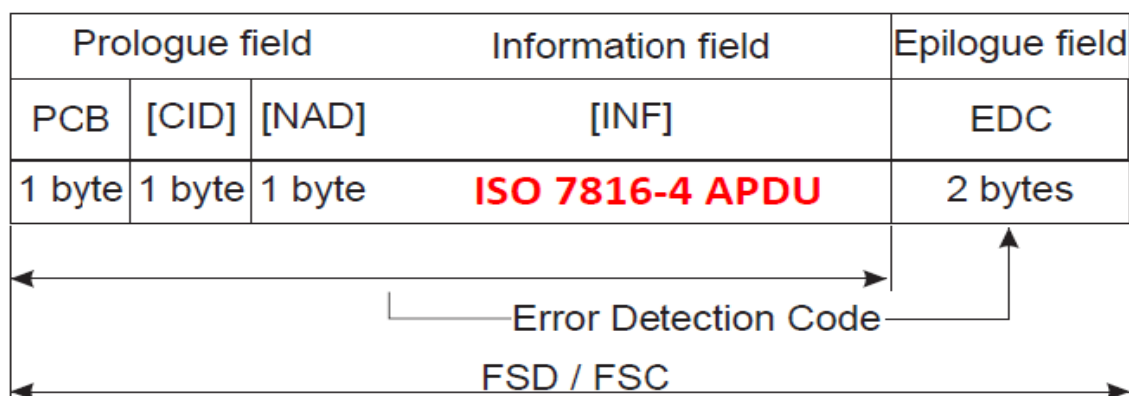


Figure 1 : Les trames ISO 14443-4 transportent des APDUs (ISO 7816-4).



PCB:Protocol Control Byte

CID:Card IDentifier

NAD:Node ADdress

EDC:Error Detection Code

FSC:Frame Size for proximity Card

FSD:Frame Size for proximity coupling Device

Cette figure montre la syntaxe d'une trame ISO 14443-4 transportent un APDU (voire ISO 7816-4), dans le cas d'Android le programmeur ne gère pas les Prologues et les Epilogues des trames, mais c'est les API's <sup>40</sup> et les Framework du contrôleur NFC intégré dans le mobile qui se charge mettre les APDU's créés par le programmeur dans la bonne syntaxe est les envoyés au destinataire soit une carte sans contact, un autre smartphone NFC, un Tag NFC.

Donc le gros du travail se fait sur les normes ISO/IEC 7816-4 et la norme EMV.

### II.3.2 La norme ISO/IEC 7816

ISO 7816 défini par l'International Standard Organization, contient un ensemble de normes qui couvre divers aspects des cartes à puce. 15 normes sont proposées pour les cartes à contact électrique.

- ISO 7816-1 : caractéristiques physiques de la carte
- ISO 7816-2 : emplacement des contacts électriques
- ISO 7816-3 : nature des signaux électriques et protocole de transmission entre le terminal et la carte
- ISO 7816-4 : organisation des données et sécurisation
- ISO 7816-5 : procédure d'inscription des applications
- ISO 7816-6 : données communes et règles de codage

---

<sup>40</sup> Application Programming Interface : ensemble de fonctions et de procédures placées dans des bibliothèques, fournies par un programme ou un système d'exploitation afin de faciliter la programmation d'applications l'employant.

Dans notre cas nous nous sommes intéressé par la couche transport qui est présentée dans la norme 7816-4, cette norme définit l'organisation des données et les protocoles utilisés.

### II.3.3 Les protocoles de transport (ISO 7816-3)

➤ T=0.

Les octets sont transmis selon un protocole série (1 start, 8 bit, 1 bit parité, 2+N bits stop). La détection d'une erreur de parité est signalée par le récepteur (carte ou lecteur) en appliquant un zéro logique sur la ligne de transmission pendant 1 ou 2 etu.

Le nombre de répétitions n'est pas limité par la norme.

➤ T=1.

C'est un protocole orienté bloc. Il est rarement utilisé en mode contact, la norme ISO 14443-4 (dite contactless) a défini un protocole de transport très proche du T=1.

Un bloc de données comporte un prologue de trois octets (NAD, PCB, LEN), un champ information (INF) de 0 à 254 octets, et un épilogue (LRC de 1 octet ou CRC de 2 octets).

- Le NAD contient pour l'essentiel une adresse source (3 bits) et une adresse de destination (3 bits).
- PCB comporte trois types d'information
  - I (#bloc,more), les blocs sont numérotés en modulo 2, le bit more indique que le bloc n'est pas le dernier d'une liste chaînée.
  - R (#bloc,erreur), les blocs sont numérotés en modulo 2. #bloc indique le numéro du prochain bloc attendu si erreur est égal à 0.
  - S, ce champ indique la présence de diverses commandes (RESYNC, IFS, ABORT, WTX).
- LEN, longueur du champ information
- INF, tout ou partie d'une APDU
- LRC/CRC, somme de contrôle ou CRC. CWT indique le délai maximum entre caractères BWT indique la latence maximale entre deux blocs consécutif.

**Remarque :** ce protocole est rarement utilisé dans la carte bancaire.

### II.3.4 Format des APDUs.

➤ CLA.

Ce paramètre est défini pour des types de cartes particuliers ou par des fabricants particuliers. 00 est la valeur ISO, A0 pour les cartes SIM, BC a été utilisé par Bull CP8, FF est réservé pour le protocole PTS.

➤ INS – Commandes de bases

1. READ\_BINARY. CLA B0 P1 P2 Le. Réalise la lecture de Le octets à partir d'offset dans un fichier transparent.
  - Si le bit de poids fort de P1 est égal à 1, EF est désigné par les 5 bits de poids faible, P2 représente l'offset.
  - Sinon l'offset est égal à  $(256 * P1) + P2$
2. WRITE\_BINARY. CLA D0 P1 P2 Lc [Lc octets] Réalise l'écriture de Le octets à partir d'offset dans un fichier transparent.
  - Si le bit de poids fort de P1 est égal à 1, EF est désigné les 5 bits de poids faible, P2 représente l'offset.
  - Sinon l'offset est égal à  $(256 * P1) + P2$
3. UPDATE\_BINARY. CLA D6 P1 P2 Lc [Lc octets]. Réalise l'écriture de Le octets à partir d'offset dans un fichier transparent.
  - Si le bit de poids fort de P1 est égal à 1, EF est désigné les 5 bits de poids faible, P2 représente l'offset.
  - Sinon l'offset est égal à  $(256 * P1) + P2$
4. ERASE\_BINARY. CLA 0E P1 P2 [Lc=2 ou non présent] [2 octets ou rien] Efface le fichier à partir de l'adresse jusqu'à la fin du fichier.
  - Si Lc=2, l'offset est indiquée par les deux octets de données ;
  - Sinon si le bit de poids fort de P1 est égal à 1, EF est désigné les 5 bits de poids faible, P2 représente l'offset.
  - Sinon l'offset est égal à  $(256 * P1) + P2$
5. READ\_RECORD CLA B2 P1 P2 Le Lit un enregistrement dans un fichier
  - P1, numéro d'enregistrement ou premier enregistrement à lire égal à 00 indique l'enregistrement courant

- P2= 04 lecture de l'enregistrement P1=05 lecture des enregistrements à partir de P1 jusqu'à la fin du fichier.
6. WRITE\_RECORD CLA D2 P1 P2 Lc [Lc octets] Ecriture d'un enregistrement.
    - P1 numéro d'enregistrement
    - P2=04 enregistrement P1
  7. APPEND\_RECORD CLA E2 P1 P2 Lc [Lc octets] Pour P1 = P2 =0, cette commande ajoute un nouvel enregistrement à la fin d'un fichier à structure linéaire ou réalise l'écriture du premier enregistrement d'un fichier cyclique.
  8. UPDATE\_RECORD CLA DC P1 P2 Lc [Lc octets] Cette commande réalise la mise à jour d'un enregistrement. Lorsque P2=04 P1 indique la valeur de l'enregistrement.
  9. GET\_DATA. CLA CA P1 P2 Le. Cette commande permet d'obtenir un objet identifié par son tag (P1 P2) dans le contexte courant (par exemple le DF sélectionné ou relatif à une implémentation particulière).
  10. PUT\_DATA CLA DA P1 P2 Lc [Lc octets] Cette commande insère un objet dans le contexte courant (DF sélectionné ou relatif à une implémentation particulière). P1 P2 désigne le type (tag) de l'objet.
  11. SELECT\_FILE CLA A4 P1 P2 Lc [Lc octets] [Le ou omis]. P1 = 00 (sélection par identifiant MF DF EF) P1= 01 (sélection DF) P1=02 (sélection EF) P1= 03 (Sélection du père du DF courant) P2 =00 première occurrence.
  12. VERIFY CLA 20 P1 P2 Lc(ou omis) [Lc octets] Cette commande réalise la vérification d'un mot de passe. Le nombre d'essai peut être limité. En général P1=P2=0.
  13. INTERNAL\_AUTHENTICATE CLA 88 P1 P2 Lc [Lc octets] Le Cette commande réalise un calcul d'authentification relativement à une clé interne en transférant un nombre aléatoire (challenge) délivré par le lecteur. P1 représente la référence d'un algorithme. P2 est égal à zéro par défaut. Le challenge est contenu dans les Lc octets sortants.
  14. EXTERNAL\_AUTHENTICATE CLA 88 P1 P2 Lc [Lc octets] Le Cette commande met à jour l'état d'une carte en fonction du résultat d'un calcul réalisé par le lecteur à partir d'un nombre aléatoire délivré par la carte (CHALLENGE). P1, référence d'un algorithme P2 est égal à zéro par défaut.

15. GET\_CHALLENGE CLA 84 P1 P2 Le Cette commande produit un nombre aléatoire de Le octets
16. GET\_RESPONSE CLA C0 P1 P2 Le Cette commande est utilisé pour lire de l'information depuis la carte lorsque le protocole de transport ne le permet pas directement (par exemple T=0).
17. ENVELOPE CLA C2 P1 P2 Lc [Lc octets] Le ou omis Cette commande est utilisée par les ordres entrant/sortant lorsque le protocole de transport ne les supportent pas (par exemple T=0).

### II.3.5 La norme EMVCo

La norme EMV 'Europay' 'MasterCard' 'Visa' est une norme international créer en Décembre 1993 par :

- **Europay** International (racheté par Mastercard en 2002) ;
- **MasterCard** International ;
- **Visa** International ;

Rejoint par :

- le japonais **JCB International** (depuis Déc. 2004)
- l'américain **American Express** (depuis Fév. 2009)

Son principale objectif c'est de normalisé les cartes bancaires avec contact et sans contact le mobile paiement, les TPE et les DAB.

Contrairement aux normes ISO/IEC les normes EMV sont gratuite, elles peuvent être téléchargé gratuitement sur le site officiel <http://www.emvco.com>, néanmoins **les spécifications viennent pour compléter les normes ISO/IEC 7816 et ISO/IEC 14443**. Elles doivent être lues conjointement

Si des définitions fournies dans EMV sont différentes de la norme ISO alors les définitions de la norme EMV remplacent celles de l'ISO

Ces spécifications doivent être utilisées par :

- Les fabricants de ICC (Integrated Circuit(s) Card ) et de terminaux
- Les concepteurs de systèmes de paiement
- Les institutions financières qui implantent des applications financières sur ICC

La norme EMV possède plus de 1000 pages divisées en plusieurs livres :

**Book 1:** Application Independent ICC to Terminal Interface Requirements. Décrit

- les caractéristiques mécaniques : contact, dimension, etc.
- les caractéristiques électriques : voltage, impédance
- Answer to Reset
- Description du protocole de transaction
- Sélection d'application
- Conforme aux spécifications de l'ISO 7816

**Book 2:** Security and key management. Il contient des spécifications sur la sécurité et la cryptographie. On peut citer :

- Static Data Authentication
- Dynamic Data Authentication
- Cryptage du code PIN hors ligne
- Intégrité et confidentialité
- Mécanismes de sécurité : cryptage symétrique, asymétrique, signature numérique.
- Algorithmes cryptographiques : RSA, DES, SHA-1

**Book3 :** Application specification : ce livre est divisé en 2 parties :

- Partie 1 : Les données et les commandes
- Partie 2 : Flux transactionnel

**Book4 :** Cardholder, Attendant, and Acquirer, ce livre définit :

- Les besoins fonctionnels et caractéristiques physiques
- La gestion des données et du logiciel
- Les interfaces utilisées

**Book 5 :** Contactless Specifications for Payment Systems, ce livre est une extension des livres 1,2,3,4 il décrit les spécifications pour le paiement sans contact.

### **II.4 Architecture du mode Emulation de carte**

La communication réalisée par le Groupement des Cartes Bancaires, l'émission massive de cartes sans contact et les failles s'y rapportant ont contribué à la notoriété du paiement sans contact NFC. Comme pour un paiement EMV, le paiement mobile NFC

actuel se base sur un élément sécurisé dit Secure Element (SE<sup>41</sup>) : la carte SIM Majoritairement. Cette dernière, propriété de l'opérateur mobile, est source de contraintes pour les fournisseurs de solutions de paiements mobiles. Pour y remédier, les acteurs monétiques ont créé l'émulation de cartes hébergées plus connue sous le sigle anglais HCE (Host Card Emulation).

Pour bien comprendre le fonctionnement du HCE, il est important de rappeler celui du modèle actuel : le SE est embarqué dans le mobile.

### II.5 Présentation rapide du paiement mobile NFC SIM-centric

Le paiement mobile NFC « classique » est un paiement où le smartphone fait office de carte bancaire. L'antenne NFC permet au smartphone de dialoguer avec le terminal de paiement électronique (TPE). Le contrôleur NFC sollicitera le SE (souvent la carte SIM, on parle alors de « SIM-centric ») qui contient les données bancaires sensibles (numéro de carte appelé aussi PAN, clés cryptographiques, ...). À aucun moment, le système d'exploitation n'a donc connaissance de ces données. C'est là que réside la robustesse du NFC SE.

L'installation de l'application de paiement au sein de la carte SIM a fait émerger de nouveaux acteurs comme les tiers de confiance (Trusted Service Manager : TSM) ; implique les opérateurs mobiles (Mobile Network Operator : MNO) ; et d'une manière plus générale complique l'écosystème NFC, aussi bien pour les acteurs que pour les porteurs, voire la figure 4.13.

---

<sup>41</sup> Secure Element : est un microcontrôleur sécurisé contenue dans les cartes à puce, souvent utilisé pour enregistrer des données sensibles comme le code PIN le numéro de la carte, et aussi l'historique des transactions.

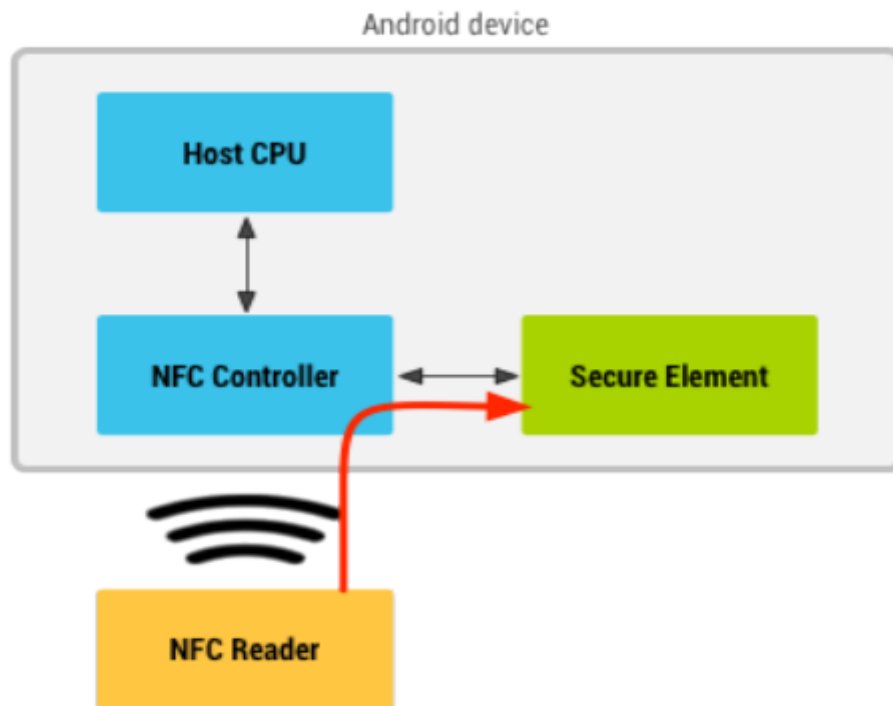


Figure 2 : Architecture du mode paiement mobile NFC SIM-centric

### II.6 Les technologies des tags

Les tags implémentent différentes technologies indépendamment développées en fonction de leur type. Il existe dix technologies :

- IsoDep : fournit l'accès aux propriétés et opérations de la norme ISO 14443-4.
- MifareClassic : fournit l'accès aux propriétés et opérations du MIFARE Classic3.
- MifareUltralight : fournit l'accès aux propriétés et opérations du MIFARE Ultralight.
- Ndef : fournit l'accès au contenu du NDEF ainsi qu'à ses opérations.
- NdedFormatable : fournit l'accès au formatage d'un tag, c'est-à-dire qu'il permet de formater un tag pour qu'il contienne du NDEF.
- NfcA : fournit l'accès aux propriétés et opérations de la norme ISO 14443A.
- NfcB : fournit l'accès aux propriétés et opérations de la norme ISO 14443B.
- NfcBarcode : fournit l'accès aux tags contenant uniquement un code barre.
- NfcF : fournit l'accès aux propriétés et opérations de la norme JIS 6319-44.
- NfcV : fournit l'accès aux propriétés et opérations de la norme ISO 156935.