TABLE DES MATIÈRES

NOTATIONS ET ABREVIATIONS

Notations

1. Minuscules latines

c	Célérité de la lumière
d	Distance
f	Fréquence
n	Nombre de spires

2. Majuscules latines

B	Champ magnétique
I	Intensité du courant

3. Minuscules grecques

λ	Longueur d'onde
μ_0	Perméabilité du vide

Abréviations

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASK	Amplitude Shift Keying
ATQ	Answer To ReQuest
ATS	Answer To Select
CD-ROM	Compact Disc Read Only Memory
COLD	Computer Output on Layer Disc
CPU	Central Processor Unit
DVD-ROM	Digital Versatile Disc Read Only Memory
ECMA	European Computer Manufacturer Association
EDM	Electronic Document Management
EEPROM	Electrically Erasable Programmable Read Only Memory
EMVCo	Europay Mastercard Visa Consortium
EPROM	Erasable Programmable Read Only Memory
ERMS	Electronic Records Management System
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Access Multiple
FSK	Frequency Shift Keying

GAB	Guichet Automatique de Banque
GED	Gestion Electronique des Documents
GSM	Global System for Mobile
HF	High Frequency
ICR	Intelligent Character Recognition
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IHM	Interface Homme Machine
IP	Internet Protocol
ISM	Industrial Scientific Medical
ISO	International Standardization Organization
IWR	Intelligent Word Recognition
JCB	Japan Card Bureau
JDK	Java Development Kit
JIS	Japanese Industrial Standard
JPEG	Joint Picture Expert Group
LCD	Liquid Crystal Display
LF	Low Frequency
MCD	Modèle Conceptuel des Données

MERISE	Méthode d'Etude et de Réalisation Informatique pour les Systèmes d'Entreprise
MLD	Modèle Logique des Données
MPD	Modèle Physique des Données
NFC	Near Field Communication
NRZ	Non Return Zero
NVM	Non Volatile Memory
OCR	Optical Character Recognition
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format
P2P	Peer to Peer
PC	Personal Computer
PHP	Hypertext Preprocessor
PIN	Personal Identification Number
PSK	Phase Shift Keying
PVC	PolyVinyl Chloride
RAM	Random Access Memory
REQ	REQuest
RF	Radio Frequency

RFID	Radio Frequency Identification
ROM	Read Only Memory
RTF	Reader Talk First
RZ	Return Zero
SAE	Système d'Archivage Electronique
SAK	Select AKnowledge
SGBDR	Système de Gestion de Bases de Données Relationnelles
SIM	Subscriber Identifier Module
SPI	Serial Peripheral Interface
SQL	Structured Query Language
TCP	Transmission Control Protocol
TTF	Tag Talk First
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UID	Unique IDentification
UIT	Union Internationale des Télécommunications
USB	Universal Serial Bus
WMRA	Write Many Read Always
WORM	Write Once Read Multiple

WPAN	Wireless Personnal Area Network
XML	eXtensible Markup Language

INTRODUCTION GÉNÉRALE

Le numérique a changé nos vies et nos activités. Nous vivons dans une période où le numérique devient un outil incontournable de notre vie quotidienne. On le retrouve dans quasiment tous les domaines et il est au cœur des problématiques de notre société, en améliorant nos modes de communication et d'information. Il offre de plus en plus de services non seulement aux spécialistes du domaine mais aussi à d'autres secteurs en quête de solutions.

Le développement de la dématérialisation des documents est une réalité dans le monde d'aujourd'hui. L'incessante progression du numérique nous pousse à manipuler des informations dématérialisées jusqu'à nous faire oublier l'existence du support traditionnel qu'est le papier. Les organismes comme les particuliers traitent de l'information dématérialisée, à travers des bases de données, des mails, des factures numériques, etc. La dématérialisation est l'ensemble des techniques qui consiste à supprimer le papier au profit de l'électronique.

La dématérialisation des documents « papier » apparait comme un moyen de résoudre les problèmes d'intégrité et de dégradation de ces documents. C'est le cas de façon concrète des documents d'identité, au sein des organismes publics ou privés, qui ne sont pas à l'abri de toutes sortes d'usurpation et qui subissent des dégradations dues au vieillissement du papier. Pour faire en sorte que ces documents puissent ne pas être modifiés pour des fins malintentionnées ou plus précisément falsifiés, et pour assurer une longévité de la durée de vie des documents, il s'avère nécessaire d'avoir recours à la dématérialisation. Elle n'est pas seulement synonyme de changement de support de l'information, elle offre aussi la possibilité d'une mise en place de nouvelles procédures et de nouveaux outils de travail. La solution de documents d'identité numérique permet d'une part, de réduire les risques d'usurpation d'identité et d'autre part, d'intégrer l'administration dans le monde du numérique qui à notre époque, constitue le principal vecteur d'information et de communication sans cesse en croissante évolution.

Le présent mémoire intitulé « Développement d'une application pour la dématérialisation des documents d'identité » est organisé en quatre chapitres dont le premier présentera une vue globale de la dématérialisation. Le second chapitre présente la technologie RFID (Radio Frequency Identification). Le troisième chapitre est consacré à l'étude des cartes à puce. Le quatrième chapitre détaillera la conception et la réalisation d'une application permettant la dématérialisation des documents d'identité.

CHAPITRE 1
LA DEMATERIALISATION

1.1 Introduction

La dématérialisation est le transfert sur un support numérique de tout type d'informations qui était sur des supports dits traditionnels, le plus souvent le papier ou encore le microfilm. [1]
L'information numérique présente deux caractéristiques fondamentales :

- elle n'est pas lisible ou visible à l'œil nu
- elle est binaire (constituée d'une suite de 0 ou de 1) et est indépendante du support

Voici un certain nombre de concepts que recouvre la dématérialisation :

- transformer des objets physiques en objets numériques
- automatiser, par des logiciels, des traitements réalisés par l'homme
- améliorer la rapidité des échanges entre personnes par l'utilisation de moyens techniques de communication

Tout organisme décidant d'opter pour la dématérialisation de ses documents, doit mettre en place un outil de GED (Gestion Electronique des Documents) et/ou un SAE (Système d'Archivage Electronique) qui constitue les éléments clés d'un procédé de dématérialisation.

1.2 GED

1.2.1 Définition

La GED est l'ensemble d'outils et de techniques qui permettent, à partir d'applications informatiques, de dématérialiser, organiser, gérer, stocker et diffuser des informations sous forme électronique. Elle résulte de la dématérialisation des documents. [2]
Le développement de la GED a été favorisé par l'augmentation des capacités de stockage, le développement des techniques de numérisation et de reconnaissance optique de caractères, ainsi que celui des réseaux de télécommunications. Sur ce dernier point, la continuelle optimisation des réseaux internet et intranet a permis des évolutions technologiques majeures en termes de solutions logicielles. La GED trouve de multiples applications dans toutes les organisations où les documents abondent et permet d'identifier et trier une multitude de types de documents (documents mail, documents papier, pages internet, fichiers bureautique, etc.).

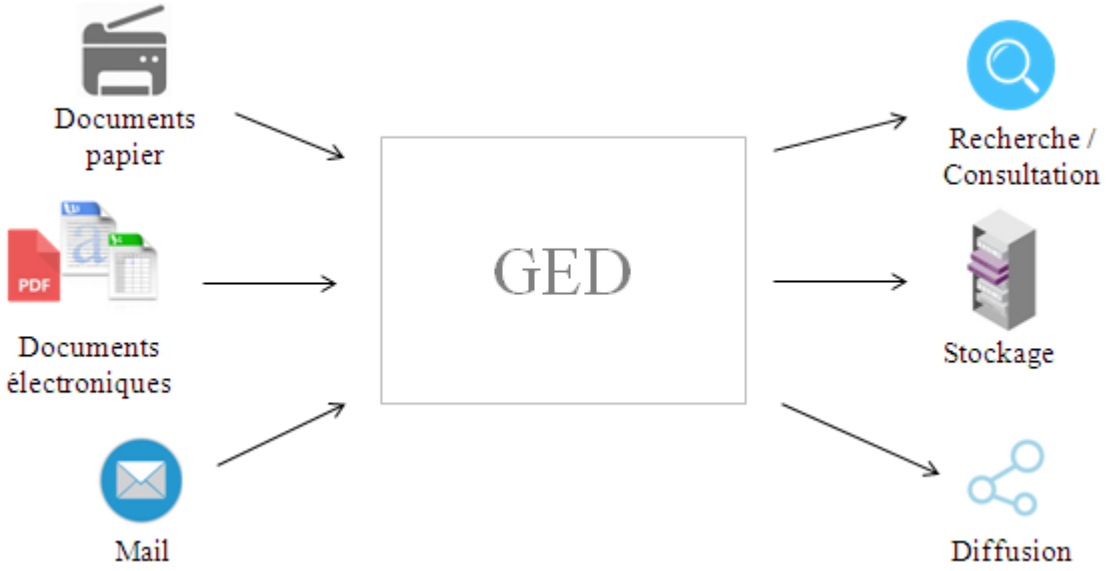


Figure 1.01 : *Schéma descriptif d'un système de GED*

La GED a pour vocation de rendre l'information accessible :

- plus facilement avec les indexations et les moteurs de recherche
- plus rapidement grâce à l'informatique qui abolit la distance entre l'utilisateur et le lieu où se trouve physiquement l'information
- plus sûrement car les accès sont contrôlés et les documents ne risquent pas d'être déclassés par un utilisateur négligent
- simultanément par plusieurs utilisateurs

Il existe cinq grandes catégories de GED selon les documents gérés :

- la GED administrative permet de numériser puis de classer les documents administratifs (factures, fiches techniques, devis, etc.).
- la GED bureautique se base sur les plateformes de bureautique permettant d'échanger et de lire des documents dans leur format d'origine (MS Word, MS Excel, MS Outlook, etc.).
- la GED COLD (Computer Output on Laser Disc) qui regroupe des programmes et des applications conçus pour récupérer les documents depuis le flux d'impression et ensuite, les indexer et les stocker automatiquement.
- la GED technique ou GED métier qui concerne la manipulation de documents dont le format et le contenu sont propres à un métier (plans, schémas, etc.).
- la GED documentaire consiste à définir un grand nombre de fichiers numériques aux formats les plus divers (texte, image, etc.) selon des critères définis par l'organisme. [3]

1.2.2 Mise en place

La mise en place d'une GED nécessite généralement un investissement et un effort conséquent puis un choix judicieux des technologies adéquates. Il est souvent constaté que les utilisateurs de ces nouveaux outils et services auraient du mal à s'en passer vu les multiples atouts qu'ils apportent : circulation de l'information, recherche rapide et efficace sur des centaines de milliers de documents à l'aide de mots-clés, sécurisation de l'accès et assurance de la bonne conservation des documents. La mise en place d'une GED doit être menée comme un projet. Un projet de GED ne se résume pas à une simple acquisition et installation d'un outil, il est indispensable de faire précéder la mise en place de l'outil de GED par une étude de faisabilité et d'opportunité.

1.2.3 Etapes de la chaine de traitement d'un document

Dans tout projet de dématérialisation, l'objet de la numérisation est essentiellement représenté par des documents textuels ou des images.
La mise en place d'un système de GED s'accompagne d'une nécessité de se poser toute une série de questions qui permettront de s'orienter vers des choix technologiques. Les réponses à ces questions passent, dans tout projet, par une analyse approfondie de toutes les étapes de la chaîne de GED, qui va de l'acquisition numérique jusqu'à la destruction éventuelle du document numérique. [3]

1.2.3.1 Acquisition numérique

La première étape de la chaîne est l'acquisition numérique. Pour que l'information soit gérable par un ordinateur, elle doit être disponible sous forme binaire.
Il existe trois possibilités d'acquisition numérique :

- l'acquisition directe de l'information par saisie directe du texte sur traitement de texte ou acquisition d'image à partir d'un appareil photo, etc.
- la collecte et l'assemblage de documents déjà numériques
- la conversion en numérique de documents analogiques

1.2.3.2 Formatage

Après la numérisation physique des documents, se situe le formatage. C'est la phase d'enregistrement sous un format de fichier. Les formats de fichiers se divisent en trois grandes

familles : les formats de fichier texte, les formats de fichier image et les formats de description de page. [9]

Le choix d'un format de fichier peut être plus ou moins critique selon la pérennité que l'on souhaite donner au document numérique.

Voici les principaux critères qui doivent dicter le choix du format de fichier :

- la garantie de l'intégrité des données
- la rapidité de numérisation
- le poids du fichier, qui conditionne le volume de stockage et la vitesse d'affichage du document
- la compatibilité avec les logiciels applicatifs

Le format le plus utilisé dans la majorité des procédés de dématérialisation est le PDF (Portable Document Format). Le format PDF réunit en un seul fichier tous les fichiers composants de la mise en page d'un document électronique (texte, images, polices, objets graphiques, etc.). Ainsi, les fichiers numérisés sont fidèles aux documents originaux, quelles que soient l'application et la plate-forme utilisées pour le créer. Ils s'afficheront de la même manière sur tout PC (Personal Computer), et ce quel que soit le système d'exploitation utilisé. Cette portabilité en fait le format idéal pour l'archivage numérique. En outre, il présente également l'avantage de pouvoir sécuriser les documents et de préserver ainsi leur intégrité. [11]

1.2.3.3 Traitement

Dans la chaîne GED, après le formatage vient la phase de « traitement ». Cette phase comporte trois opérations essentielles qui sont la compression, la correction graphique ou la reconnaissance de caractères.

- Compression

Pour que les documents puissent à la fois être stockés en grande quantité ou transférés le plus rapidement possible, il convient de les compresser. Il existe différents moyens de compression :

- le CCITT Groupe 4 pour les images en noir et blanc. Il respecte l'intégralité du document et n'entraîne aucune perte. [5][6]
- l'algorithme JPEG (Joint Picture Expert Group) est un puissant algorithme de compression dédié à la compression d'images noir et blanc ou couleurs. C'est une méthode de compression dite « irréversible » car elle entraîne une perte de données. [6]

- Correction graphique

Le fichier numérique obtenu après numérisation d'un document peut parfois révéler des imperfections susceptibles de nuire à son traitement ou à sa consultation. Voici quelques exemples d'imperfections qui peuvent être réparées ou compensées par un traitement numérique.

- Un mauvais contraste : le mauvais contraste d'un document textuel peut considérablement diminuer l'efficacité et la fiabilité d'un traitement OCR.
- La présence de tâches : certains documents peuvent présenter des tâches dues par exemple au vieillissement du papier. Dans ce cas, ce peut être à la fois le traitement OCR et les lecteurs qui s'en trouvent affectés.
- Des lignes de textes désalignées : certains documents peuvent présenter des lignes de textes désalignées. Cette inclinaison est assez bien tolérée par l'OCR mais beaucoup moins acceptée par les lecteurs.

Des traitements numériques adéquats existent et peuvent être appliqués, de façon manuelle ou automatique, pendant ou après la numérisation physique. Ces traitements sont d'autant plus importants et ne doivent pas être négligés lorsqu'il est prévu de détruire le fonds papier après la dématérialisation. [6]

- La reconnaissance des caractères : OCR, ICR et IWR [7] [8]

L'OCR (Optical Character Recognition) : permet de reconnaître une suite de caractères sur un document scanné, par reconnaissance de forme.

L'ICR (Intelligent Character Recognition) : est un système d'OCR avancé intégrant des technologies d'intelligence artificielle. Il a la capacité d'identifier des lettres isolées écrites à la main. Un logiciel d'ICR peut compléter sa base de connaissance au fur et à mesure de la reconnaissance et donc étendre sa capacité de reconnaissance.

L'IWR (Intelligent Word Recognition) : permet de numériser des mots entiers, écrits à la main. Cette technologie peut fournir des résultats convaincants à condition que l'écriture cursive analysée soit de bonne qualité.

Grâce à ces technologies, il est donc possible de convertir l'image d'un document scanné en un texte ASCII (American Standard Code for Information Interchange).

Les algorithmes de reconnaissance de caractères se sont considérablement développés et perfectionnés. Ces technologies sont intégrées dans toutes les solutions de GED.

Pour obtenir des résultats satisfaisants avec ces technologies, c'est-à-dire pour bénéficier d'un taux de reconnaissance de caractères élevé, il est nécessaire que la résolution de l'image du document textuel soit, au minimum, de 200 dpi.
La résolution la plus souvent employée est 300 dpi. Lorsque les conditions satisfaisantes de traitement ont été réunies : résolution adéquate, bonne qualité d'impression, de contraste, typographie standard, etc., le degré de fiabilité de la reconnaissance est généralement très élevé, avec un taux de reconnaissance pouvant aller jusqu'à 99%. En revanche, ce taux chute rapidement lorsque les documents comportent des écritures manuscrites, ou des typographies très particulières.
D'une manière générale, la reconnaissance de caractères est dépendante de la qualité des documents à traiter, donc des éléments suivants :

- un mauvais contraste
- un mauvais alignement des lignes de texte
- des caractères tordus ou qui se touchent (cas des écritures manuscrites)
- l'existence de tâches

1.2.3.4 Indexation

L'indexation se définit comme un moyen destiné à représenter, au moyen des termes ou indices, les notions caractéristiques du contenu d'un document en vue d'en faciliter la recherche. L'indexation est aussi le cœur de la GED puisque c'est l'opération qui consiste à décrire et caractériser le document afin de permettre une exploitation sans nécessairement recourir à la consultation du document lui-même. Elle doit être une représentation fidèle et la plus exhaustive possible du document et de son contenu, afin de permettre une recherche facile et pertinente. [9]
La difficulté de cette opération réside dans la nécessité de produire une représentation formalisée et réduite d'un document et de son contenu, tout en retenant l'ensemble des éléments essentiels de ce dernier. La qualité et la pertinence de l'indexation deviennent ainsi absolument essentielles et cruciales lorsqu'il s'agit d'exploiter un système de GED comportant plusieurs milliers de documents.
Dans un système de GED, l'indexation du contenu d'un document peut être manuelle ou automatique :

- L'indexation manuelle : C'est une méthode qui consiste à créer une fiche descriptive associée au document dans l'application GED.

- L'indexation automatique : l'indexation automatique s'est imposée avec l'arrivée des technologies de reconnaissance de caractères. Elle permet d'indexer tous les mots du document. La recherche n'est plus alors limitée aux descripteurs mais porte sur l'intégralité du texte.

Le principal avantage de l'indexation automatique, qui est totalement prise en charge par l'ordinateur, est qu'elle est bien plus rapide à réaliser. Son principal inconvénient est qu'elle est moins pertinente et fiable, en termes de corrélation entre la requête effectuée et les documents obtenus après identification.

Les modes d'indexation manuelle et automatique peuvent être utilisés de manière combinée.

1.2.3.5 Nommage

Il faut définir une règle de nommage pour les documents numérisés. Ainsi, ils porteront un nom normalisé afin de les repérer plus facilement et de savoir ce qu'ils contiennent.

Voici un tableau récapitulatif des éléments à prendre en compte pour définir une règle de nommage : [12]

Date	Format : AAAA-MM-JJ, JJMMAA, etc. Emplacement : à la fin ou au début du nom du fichier
Intitulé (Nom des documents)	En majuscule et/ou minuscule
Signes de ponctuation et caractères spéciaux	Etablir des règles d'usage Exemple : ne pas mettre d'espace entre les mots, interdire l'utilisation d'apostrophe, etc.
Type de document	Intégrer un type de document à la dénomination Exemple : devis, facture, etc.

Tableau 1.01: *Tableau de quelques éléments indispensables à la dénomination d'un document*

On pourrait par exemple nommer Orange-facture-20160302-Smartphones.pdf le document contenant la facture des Smartphones achetés chez Orange le 02 mars 2016 en utilisant la règle de nommage suivante : <fournisseur>-<type de document>-<date>-<intitulé>.extension.

1.2.3.6 Stockage

En termes de stockage informatique, une solution de GED doit utiliser plusieurs types de support. Un système de GED doit être capable de concilier une vitesse rapide d'accès et de consultation des documents avec une bonne condition de conservation de ces derniers.

Les différents critères de choix pour les supports de stockage sont : la capacité de stockage, le temps d'accès aux données, la pérennité du contenu, la réinscriptibilité ou non réinscriptibilité, la sécurité d'accès aux données.

Pour satisfaire à tous ces critères, les solutions de GED combinent presque toujours les supports magnétiques, pour la consultation et la sauvegarde des informations, et les supports optiques essentiellement pour l'archivage électronique. [9]

- Les supports magnétiques

Actuellement, les supports magnétiques capables de stocker des documents numériques très lourds sont les disques magnétiques. Ces disques sont destinés à assurer la consultation on-line d'une base de données, étant donné leur vitesse de transmission très rapide et la grande taille de leur espace mémoire. Les disques magnétiques sont des dispositifs fixes, intégrés dans les appareils qui les utilisent. Communément dénommés « disques durs », ils sont aujourd'hui connus de tous puisqu'intégrés dans tous les ordinateurs, et constituent le moyen le plus simple et le plus efficace de sauvegarder de l'information. Ils offrent souplesse et rapidité, et les capacités de stockage sont de plus en plus conséquentes grâce à l'évolution des technologies.

- Les supports optiques

Ces supports sont adaptés pour le stockage offline des données numériques. Ils se divisent en deux catégories : les disques WORM (Write Once Read Multiple) inscriptibles une seule fois et les disques WMRA (Write Many Read Always) qui sont réinscriptibles.

Les disques WORM sont particulièrement adaptés pour l'archivage des documents numériques sur le long terme, car ils sont inscriptibles une seule fois et garantissent l'intégrité des données. Parmi ces supports, on trouve le CD-ROM, le CD-R, le DVD. Ce dernier est particulièrement recommandé pour les systèmes de GED grâce à sa capacité de stockage supérieure. On peut aussi évoquer la solution que représente le disque Blu-ray qui offre une capacité de stockage allant de 25 Go à 50 Go.

- Les librairies de sauvegarde (Jukebox)

Il existe pour les bandes magnétiques et aussi pour les disques optiques des librairies de sauvegarde appelées aussi Jukebox pouvant contenir une multitude de cartouches de bandes

magnétiques ou de disque optiques, accessibles via des systèmes robotisés. Ces librairies possèdent actuellement des capacités de stockage extrêmement importantes, de l'ordre de plusieurs dizaines de téraoctets. [10]

Figure 1.02 : *Jukebox IBM 3584*

1.2.3.7 Recherche

Un document est fait pour être consultable. Il n'a donc aucune valeur si on ne peut pas le retrouver. Un document non classé ne fait qu'occuper inutilement de I 'espace. Toute organisation ou tout individu qui souhaite gérer des documents doit imaginer un plan de classement qui permettra de retrouver le document recherché. Ce plan de classement permet de ranger un document selon des thèmes et des sous-thèmes. Il est parfois possible d'intégrer plusieurs plans de classement. La recherche dépend directement des possibilités d'indexation des documents. La pertinence des résultats de la recherche dans le système de GED est aussi directement dépendante de la qualité, de la justesse et de la précision fournie lors de la phase d'indexation des documents numérisés.

Il existe plusieurs modes de recherche dans un système de GED :

- La recherche directe : c'est le mode de recherche le plus aisé. Elle se fait à partir des descripteurs externes que sont le nom ou la référence du document.
- La recherche par mots-clés : se fait à l'aide d'index inclus dans un document qui comprend des descripteurs et d'autres informations utiles à la recherche.
- La recherche en texte intégral (full text) : se fait sur l'ensemble des mots contenus dans les documents.
- La recherche multicritère : la recherche se fait à partir d'une requête construite à l'aide d'une combinaison d'attributs reliés par des opérateurs logiques. Ce sont des fonctions permettant de lier différents mots ou groupe de mots caractérisant un document (ET, OU, etc.).

1.2.3.8 Consultation

La consultation et la modification d'un document dans une application de GED se fait à partir d'un écran informatique, et à l'aide d'un programme de visualisation qui comporte en général un certain nombre d'options dont celle du zoom, pour agrandir ou réduire l'affichage du document. La GED doit s'intégrer dans l'environnement matériel bureautique existant, tout en induisant une intensification de l'utilisation de l'affichage écran. Par conséquent, le moniteur devient un élément très important dans la consultation. Les critères de choix pour un moniteur informatique dans le cadre d'une utilisation de la GED sont la résolution, la taille, la fréquence de rafraîchissement et le nombre de couleurs.

D'une manière générale, sur le plan de la consultation des documents numériques, on constate que les évolutions technologiques et la baisse importante du coût du matériel informatique, permettent d'exploiter pleinement la puissance et le potentiel des logiciels de GED. La lecture à l'écran ne devrait pas poser problème aux utilisateurs de la GED que lors d'une consultation de documents papier. L'amélioration du confort de consultation passe donc par un investissement dans des moniteurs adaptés et performants.

1.2.3.9 Diffusion

La diffusion consiste à mettre en ligne les documents numériques sur le réseau internet ou sur un intranet via des serveurs web. Ces documents intégrés dans l'application de GED sont ainsi accessibles quasi immédiatement, depuis n'importe quel poste connecté au réseau de diffusion et

simultanément par plusieurs utilisateurs. Néanmoins, ces accès peuvent être bien entendu limités et contrôlés, puisque tous les logiciels de GED intègrent des options de gestion des droits de diffusion et d'utilisation, par personne ou par groupe d'utilisateurs.

1.2.3.10 Destruction

Les documents qui n'ont pas des raisons de perdurer sont condamnés à la destruction.

1.3 **SAE**

1.3.1 Définition

Un SAE est un outil informatique permettant la conservation pérenne et sécurisée des documents électroniques. Une fois intégré dans un SAE, un document n'est plus modifiable et conserve donc sa valeur probante. [13]

1.3.2 Objectifs

Un SAE a quatre objectifs principaux :

- Pérennité : assurer la lisibilité du document dans le temps
- Intégrité : assurer l'authenticité du document c'est-à-dire la non modification possible du contenu et de la forme
- Traçabilité : description de toutes les opérations effectuées sur un document (consultations, migrations, etc.)
- Sécurité : assurer la conservation à long terme et limiter la communication du document.

1.4 **Différences entre GED et SAE**

Une distinction doit être faite entre un système de GED et un SAE, qui répondent tous deux à un besoin de dématérialisation mais n'ont pourtant pas la même finalité et les mêmes fonctionnalités. Un SAE est un logiciel informatique de gestion de contenu. Il répond au besoin de conservation des documents, en proposant des solutions d'archivage, de stockage et de numérisation. Le SAE répond à quatre objectifs : traçabilité, sécurité, pérennité et intégrité. Ces deux derniers objectifs diffèrent de la GED. En effet, le propre d'une solution de SAE est d'assurer la valeur probante d'un document : lorsqu'un document est intégré au système, il devient alors impossible de le modifier, voire même de le supprimer.

La notion de GED au contraire, inclut la possibilité de modifier, supprimer, ou déplacer un document, tout en assurant une traçabilité des actions effectuées et une sécurisation optimale de l'ensemble des documents. [13]

GED et SAE apportent tous deux des solutions qui convergent dans certaines de leur utilisation. Ces deux solutions ne répondent pas au même besoin et comportent une finalité bien différente. Alors que la GED facilite la gestion des documents dans une entreprise et le travail collaboratif, le SAE offre une solution de conservation normée et sécurisée des documents. Par conséquent, il est primordial de se poser les bonnes questions sur la solution la plus adaptée aux besoins d'un organisme.

1.5 **Normes**

Lorsqu'il est question de gestion du cycle de vie de documents, des enjeux importants entrent en scène : description, stockage, conservation des documents, archivage à vocation probante, etc. La normalisation est primordiale et se pose lorsque les entreprises ou les administrations choisissent leurs solutions de GED et/ou de SAE. Différents organismes se chargent de la normalisation de l'archivage : en France, c'est l'association française de normalisation (Afnor) qui travaille à la mise en place de normes concernant l'archivage ; au niveau international, on retrouve l'ISO (International Standardization Organization).

Voici quelques normes applicables à la GED et au SAE :

- La norme ISO 22938 recense les conditions nécessaires à un processus d'échange entre systèmes de GED. Elle définit le XML (eXtensible Markup Language) comme format d'exportation des métadonnées.
- La norme NF Z 42-013 est une norme française (Afnor) qui précise de nombreuses mesures techniques et organisationnelles autour du fonctionnement d'un SAE. Cette norme met l'accent sur la traçabilité de tous les processus autour du SAE (enregistrement, stockage, restitution de documents électroniques au sein du SAE, etc.). L'objectif est de garantir l'intégrité des documents, autrement dit un archivage électronique qui peut être à vocation probante.
- La norme ISO 19005-1 est une norme internationale qui définit le format PDF/A-1 comme format de fichier de documents électroniques placés dans un SAE devant être conservés sur du long terme. Ce format est fidèle au document original (image, police et taille d'écriture, etc.).

1.6 **Avantages**

La dématérialisation apporte de nombreux avantages liés à la disparition du support physique :

- protection de l'environnement traduit par la diminution de l'utilisation du papier
- circulation des documents
- sécurisation des échanges de documents : les documents doivent pouvoir circuler et être diffusés sans risque de modification
- suppression d'une grande partie des surfaces de stockage
- gain de temps dans le classement ou la recherche des documents

1.7 **Inconvénients**

La dématérialisation présente parfois des inconvénients pour certaines entreprises :

- risque de perte de document dû par exemple à une attaque malveillante
- besoin de matériels performants pour le stockage et la visualisation des documents

1.8 **Conclusion**

Comme nous avons vu la GED et le SAE sont des outils ayant des finalités bien différentes : faciliter l'activité d'un organisme pour la GED, la sécuriser pour le SAE. Chacun gagne à avoir des fonctionnalités bien circonscrites à sa mission : une GED sera d'autant plus facile à utiliser qu'elle n'aura pas à gérer les questions d'intégrité et de pérennité qui sont normalement du ressort du SAE. Notre étude est axée sur la dématérialisation des documents d'identité afin de mettre fin aux documents d'identité sur support papier. Un des supports numérique d'information choisi pour notre projet est la carte à puce sans contact RFID, utilisant les ondes radio et mettant en jeu des techniques de télécommunication. La RFID est une technologie qui connait un essor important à l'heure actuelle. Le chapitre suivant portera une étude particulière à cette technologie.

CHAPITRE 2
LA TECHNOLOGIE RFID

2.1 Introduction

La technologie RFID (de l'anglais Radio Frequency IDentification) est un procédé permettant d'identifier un objet, d'en suivre le cheminement, et d'en connaitre les caractéristiques à distance grâce à un système composé :

- D'une radio-étiquette contenant des informations.
- D'un lecteur permettant de récupérer ces informations à distance. [14]

2.1.1 Les radio-étiquettes

Les radio-étiquettes appelées encore transpondeur ou étiquette RFID sont attachées ou incorporées dans des objets. Elles émettent des ondes radio grâce auxquelles les informations sont transmises vers le lecteur. Une radio-étiquette est composée d'une puce électronique de silicium reliée à une antenne encapsulée dans un support.

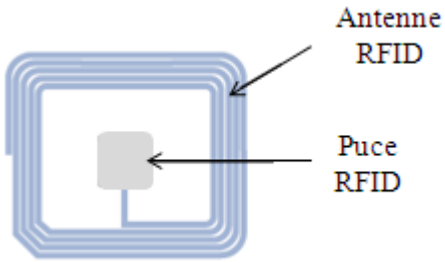


Figure 2.01 : *Etiquette RFID*

On distingue trois catégories d'étiquettes RFID :

- Les étiquettes en « lecture seule »
- Les étiquettes « écriture une fois, lecture multiple »
- Les étiquettes en « lecture réécriture »

Par ailleurs, il existe deux grandes familles d'étiquettes RFID :

- Les étiquettes actives : celles qui embarquent généralement une source d'énergie (pile, batterie).

- Les étiquettes passives : celles qui utilisent une quantité d'énergie provenant du lecteur pour pouvoir fonctionner. [15]

2.1.2 Les lecteurs

Les lecteurs ou stations de base sont des dispositifs actifs, émetteurs de radiofréquences qui vont activer les étiquettes qui passent devant eux en leur fournissant à courte distance l'énergie dont celles-ci en ont besoin. Outre de l'énergie pour l'étiquette, le lecteur envoie des commandes particulières auxquelles répond l'étiquette. L'une des réponses les plus simples possibles est le renvoi d'une identification numérique. [16]

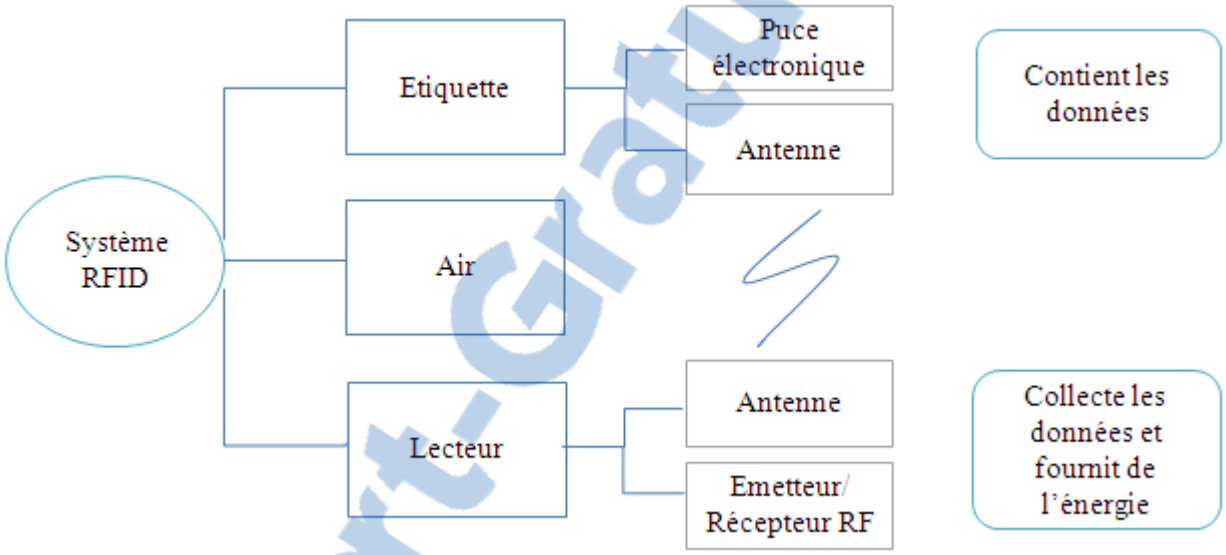


Figure 2.02 : *Les composants d'un système RFID*

La fréquence utilisée par les lecteurs est variable selon le type d'application visé et les performances recherchées. La technologie RFID utilise les théories et principes des ondes radioélectriques.

2.2 **Ondes radioélectriques**

Une onde est une vibration qui se déplace dans un environnement donné.
Elle est caractérisée par deux grandeurs physiques :

- La fréquence qui représente le nombre d'oscillations par seconde. Elle est mesurée en Hertz (Hz).
- La longueur d'onde qui est la distance séparant deux crêtes successives d'une onde périodique. Elle est inversement proportionnelle à la fréquence :

$$\lambda = \frac{c}{f} \tag{2.01}$$

où c représente la célérité de la lumière et f la fréquence

Ce sont ces différentes caractéristiques qui permettent de différencier les ondes et leur confèrent de multiples usages. [17]

2.2.1 Les ondes électromagnétiques

Une onde électromagnétique comporte à la fois un champ électrique et un champ magnétique oscillant à la même fréquence. Ces deux champs, perpendiculaires l'un par rapport à l'autre se propagent dans un milieu selon une direction orthogonale. La propagation de ces ondes s'effectue à une vitesse qui dépend du milieu considéré. Dans le vide, la vitesse de propagation est celle de la lumière : 3.10^8 m/s. [17]

2.2.2 Le spectre électromagnétique

Les ondes électromagnétiques utilisent un large éventail de fréquences et en conséquence, de longueurs d'ondes. Cette gamme de fréquences et de longueurs d'ondes est appelée spectre électromagnétique. La partie du spectre la plus connue par les humains est la lumière, la partie visible du spectre électromagnétique, qui se trouve entre les fréquences de $7{,}5.10^{14}$ Hz et $3{,}8.10^{14}$ Hz. L'homme est aussi régulièrement exposé à d'autres régions du spectre électromagnétique, y compris le courant alternatif ou réseau électrique à 50 ou 60 Hz, rayons X, ultraviolet (du côté des fréquences plus élevées de la lumière visible), infrarouge (du côté des plus basses fréquences de la lumière visible) et plusieurs autres. La radio est le terme utilisé pour la partie du spectre électromagnétique dont la plage de fréquence est comprise entre 3 Hz et 300 GHz. Entre la radio et l'infrarouge, on trouve une région de micro-ondes avec des fréquences d'environ 1GHz à 300 GHz. L'usage le plus populaire des micro-ondes est indubitablement le four à micro-ondes, qui de fait fonctionne exactement dans la même plage d'ondes que les standards sans fil. Ces plages se retrouvent au sein des bandes ouvertes pour usage général sans licence. Cette région est nommée bande ISM, pour Industriel, Scientifique et Médical. La plupart des autres parties du spectre électromagnétique est fortement contrôlée par les législations et licences, ces dernières constituant un important facteur économique.

Ceci est particulièrement vrai pour les parties du spectre qui sont utilisées dans les émissions de télévision et de radio, ainsi que pour les communications vocales et le transport des données.
Dans la plupart des pays, les bandes ISM sont réservées pour un usage sans licence.

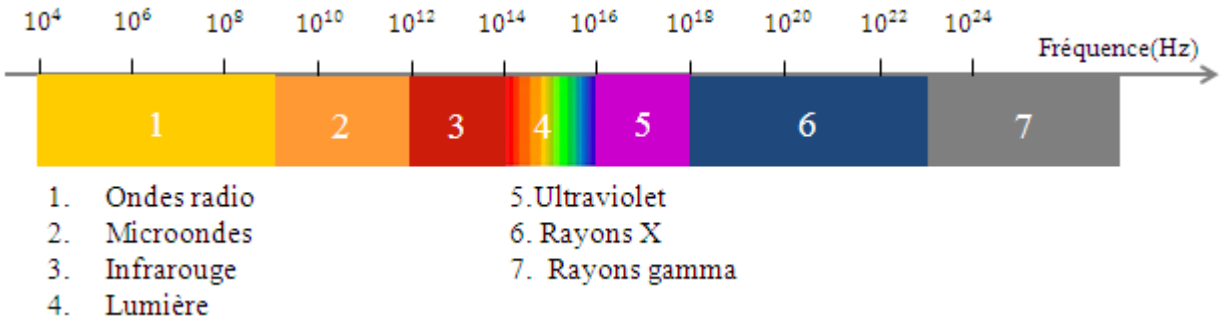


Figure 2.03 : *Le spectre électromagnétique*

2.2.3 Les ondes radio

Une onde radio (ou encore onde radioélectrique) est une onde électromagnétique dont la fréquence est inférieure à 300 GHz. [18]
L'UIT (Union Internationale des Télécommunications) a défini les ondes radioélectriques comme suit : « Ondes électromagnétiques dont la fréquence est inférieure à 300 GHz, se propageant dans l'espace sans guide artificielle » ; elles sont comprises entre 9 kHz et 300 GHz, ce qui correspond à des longueurs d'onde allant de 1mm à 33 km.
Une onde radio est classée en fonction de sa fréquence. L'ensemble de ces fréquences constitue le spectre radiofréquence.
Les ondes radio sont utilisées dans de nombreux domaines comme la diffusion d'émissions radiophoniques, la transmission des communications téléphoniques, la télévision, le radar, les systèmes de navigation et les communications spatiales.
La figure ci-dessous illustre des exemples d'utilisation des ondes radio :

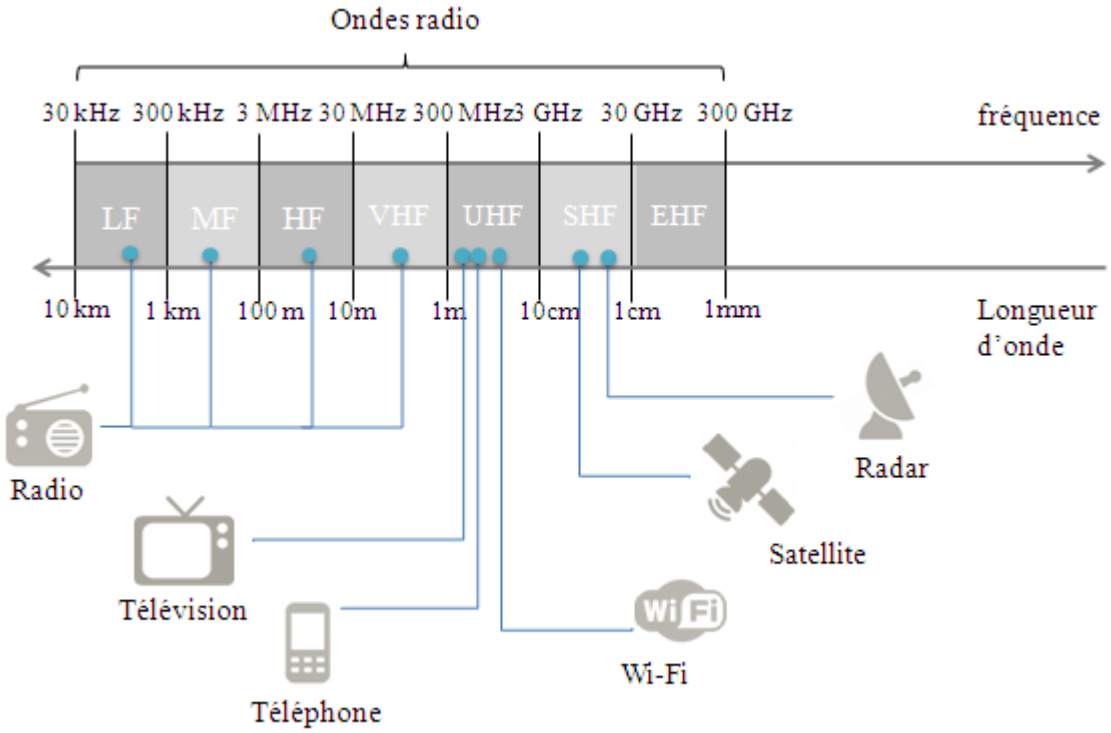


Figure 2.04 : *Exemples d'utilisation des ondes radio*

2.2.4 Propagation des ondes radio

Comme toutes les ondes électromagnétiques, les ondes radio se propagent dans l'espace vide à la vitesse de la lumière. Les ondes radio se propagent en ligne droite dans plusieurs directions.

Dans un milieu de propagation, le signal subit un affaiblissement dû aux phénomènes de :

- Réflexion : lorsque le milieu change, une partie de l'onde repart vers le milieu d'origine provoquant une perte de puissance.
- Absorption : lorsqu'une onde radio rencontre un obstacle, une partie de son énergie est absorbée, une partie continue à se propager et une autre peut éventuellement être réfléchie.
- Réfraction : lorsque le milieu change, l'onde se propage dans le second milieu mais avec une direction différente. Ceci a une grande influence sur la propagation des ondes radio.
- Diffusion : lorsque l'onde rencontre un obstacle dont la surface n'est pas parfaitement plane et lisse, elle est déviée dans de multiples directions.
- Interférence : lorsque deux ou plusieurs ondes de fréquences identiques ou voisines se superposent.

L'affaiblissement de la puissance du signal est dû en grande partie aux propriétés des milieux traversés par l'onde.

Le tableau suivant donne les niveaux d'atténuation pour différents matériaux :

Matériaux	Affaiblissement	Exemples
Air	Aucun	Espace ouvert
Bois	Faible	Porte
Plastique	Faible	Cloison
Verre	Faible	Vitre non teintée
Eau	Moyen	Aquarium
Etres vivants	Moyen	Humains, animaux, végétation
Briques	Moyen	Murs
Céramiques	Elevé	Carrelage
Métal	Tres elevé	Armoire métallique

Tableau 2.01: *Niveaux d'atténuation pour différents matériaux*

2.2.5 Les différentes zones de propagation

L'onde électromagnétique n'a pas les mêmes propriétés de propagation dans tout l'espace entourant une source. En s'éloignant d'une antenne émettrice, on distingue trois zones de propagation :

- La zone de Rayleigh : elle se situe à une distance de $0.63 \sqrt{\frac{D^3}{\lambda}}$ de l'antenne

, D étant la plus grande dimension de l'antenne et λ la longueur d'onde du rayonnement émis

- La zone de Fresnel : C'est une zone intermédiaire située entre $0.63 \sqrt{\frac{D^3}{\lambda}}$ et $\frac{2D^2}{\lambda}$
- La zone de Fraunhoffer : elle se situe au-delà de $\frac{2D^2}{\lambda}$ et constitue ce qu'on appelle la zone de champ lointain de l'antenne. [19]

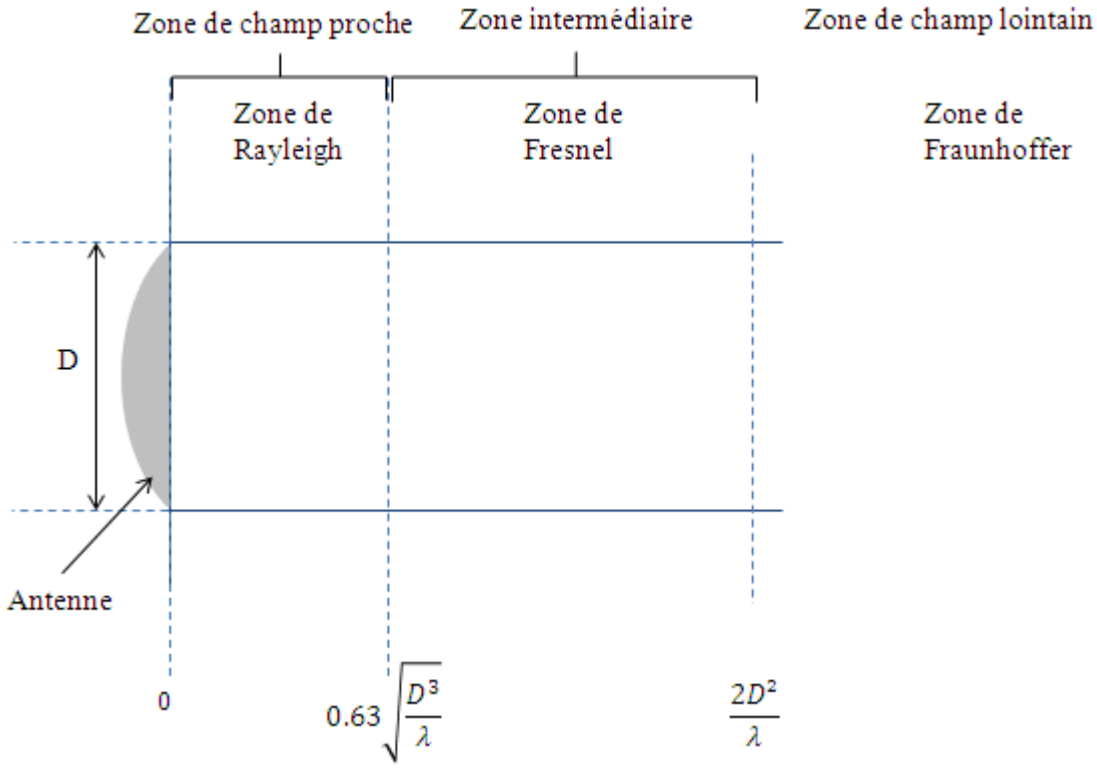


Figure 2.05 : *Les zones de rayonnement autour d'une antenne émettrice*

Dans le cas d'antenne de dimension très petite et à une distance r de cette antenne, on définit ces trois régions de l'espace selon les valeurs possibles de r par rapport à la valeur de la longueur d'onde λ à laquelle le système fonctionne, c'est-à-dire selon que la valeur de r est faible ou grande par rapport à $\frac{\lambda}{2\pi}$

Le champ proche correspond à une distance r << $\frac{\lambda}{2\pi}$ tandis que le champ lointain correspond à une distance r >> $\frac{\lambda}{2\pi}$ donc :

$$Champ\ proche < \frac{\lambda}{2\pi} < Champ\ lointain \tag{2.02}$$

2.3 **Fonctionnement et caractéristiques techniques de la RFID**

2.3.1 Domaines de fréquences

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques, ce sont donc des systèmes radio. Les ondes radio nécessaires à la transmission des informations dans les applications RFID font l'objet d'une normalisation qui dépend de chaque pays où ils sont utilisés. Les principales plages de fréquences utilisées par les systèmes RFID sont les basses fréquences (125 kHz et 133 kHz) et les fréquences ISM (13.56 MHz, 860 MHz, 960 MHz, 2.45 GHz). [14] Cependant, les bandes passantes font l'objet de réglementation par les autorités de télécommunication propres à chaque pays.

Un système RFID doit ainsi mettre en œuvre des fréquences et des bandes passantes, conformes d'une part aux contraintes techniques liées à l'application, et d'autre part à la réglementation imposée dans le pays d'utilisation.

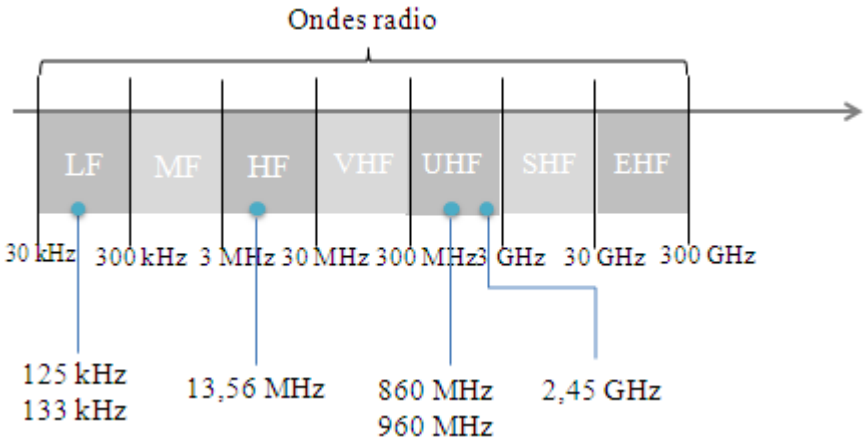


Figure 2.06 : *Fréquences de la RFID dans le spectre radio*

Il est toujours important de savoir dans quelles régions de champs « proches » ou « lointains » le système RFID envisagé va fonctionner.

En prenant pour vitesse de propagation des ondes celle de la lumière $c=3.10^8$ m/s, le tableau ci-dessous donne la relation entre quelques valeurs de fréquences et les distances $\frac{\lambda}{2\pi}$ associées. En LF et HF, les distances de fonctionnement souhaitées pour les systèmes RFID sont toujours

bien plus faibles que la valeur $\frac{\lambda}{2\pi}$. Dans ces applications, les étiquettes fonctionnent donc en champs proches.

En UHF, les distances de fonctionnement souhaitées pour les systèmes RFID sont toujours bien plus importantes que la valeur $\frac{\lambda}{2\pi}$. Dans ces applications, les étiquettes fonctionnent donc en champs lointains.

Fréquences (en MHz)	Longueurs d'ondes (en m)	$\frac{\lambda}{2\pi}$ (en m)
0,125	2400	382
0,133	2255,6	359
13,56	22,12	3,52
860	0,348	0,055
960	0,312	0,049
2450	0,122	0,019

Tableau 2.02: *Tableau de quelques valeurs de* $\frac{\lambda}{2\pi}$

2.3.2 Fonctionnement d'un système RFID

La technologie RFID est basée sur l'émission d'un champ électromagnétique par un lecteur, qui est reçu par l'antenne d'une étiquette située dans son champ de lecture.

La liaison entre le lecteur et l'étiquette se réalise par :

- Couplage magnétique dans le cas d'un champ proche : les systèmes utilisant un couplage magnétique fonctionnent avec des antennes bobinées aussi bien pour le lecteur que pour l'étiquette.

  Une tension alternative appliquée aux bornes de la bobine émettrice produit un courant I qui circule dans la bobine du lecteur, comportant n spires circulaires de rayon r. A la distance d du plan de la bobine, un champ magnétique B est créé tel que :

$$B(d) = \frac{\mu_0 I n r^2}{2(r^2 + d^2)^{\frac{3}{2}}} \tag{2.03}$$

où μ_0 est la perméabilité du vide

Lorsque l'antenne bobinée de l'étiquette entre dans le champ magnétique *B* créé par le lecteur, les deux bobines sont en couplage magnétique.

Les distances de communications varient de quelques centimètres à 1,5 m. Les fréquences utilisées sont les LF (125 kHz et 133 KHz) et les HF (13.56 MHz).

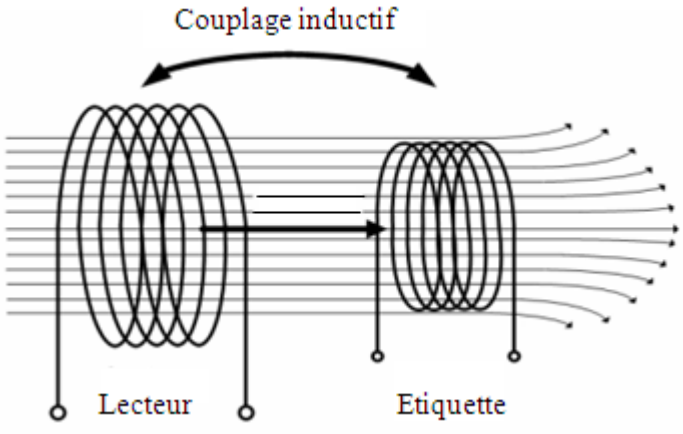


Figure 2.07 : *Couplage magnétique en champ proche*

- Couplage électromagnétique dans le cas d'un champ lointain : les systèmes utilisant un couplage électromagnétique fonctionnent avec des distances de communication allant au-delà du mètre et sont dits des systèmes à longue portée. Ils utilisent des UHF (300MHz à 3GHz).

Ces champs servent de vecteur à l'information entre l'étiquette et le lecteur mais aussi de support à l'énergie permettant de l'activer.

2.3.3 Communication

La communication consiste en un transfert de données associé à un transfert d'énergie. La communication des données est bidirectionnelle : la communication du lecteur vers l'étiquette est appelée liaison montante et celle de l'étiquette vers le lecteur est appelée liaison descendante. [20]

La communication RFID, comme dans la plupart des communications sans fil, est half-duplex. Cela signifie que chacun des interlocuteurs (lecteur et étiquette) communiquent à tour de rôle.

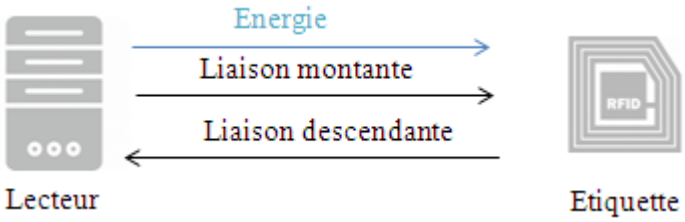


Figure 2.08 : *Représentation schématique d'une communication RFID*

On distingue deux principaux protocoles de communication entre un lecteur et une étiquette :

- Le protocole TTF (Tag Talk First) : dès qu'une étiquette rentre dans le champ d'action d'un lecteur, il se fait connaitre. Lorsque plusieurs de ces étiquettes sont dans le champ d'un lecteur, il y a un problème de collision.
- Le protocole RTF (Reader Talk First) : les étiquettes sont alimentées par le lecteur et entrent dans un état d'attente d'une requête de la part du lecteur pour signaler leur présence.

2.3.4 Transmission des données

Plusieurs types de modulations sont utilisés dans les systèmes RFID tels que la modulation d'amplitude ASK (Amplitude Shift Keying), la modulation de fréquence FSK (Frequency Shift Keying), la modulation de phase PSK (Phase Shift Keying) mais la plus utilisée est la modulation d'amplitude pour porter la donnée. Le type de modulation utilisé par les étiquettes télé alimentés passifs sans batterie est une modulation de charge. Cependant, à partir du moment où l'étiquette est actif, d'autres types de modulations peuvent être plus avantageux pour le débit, la vitesse de transaction, etc.

Associé à cette modulation, le codage permet de mettre en forme la donnée binaire. Le type de codage utilisé varie selon le sens de la communication et dépend des phases de fonctionnement : phase de test de fonctionnement, phase d'anticollision, phase utile de communication. Les principaux codages utilisés sont : NRZ (Non Return to Zero), Manchester, Miller, Miller modifié, RZ (Return to Zero). [20]

Le choix du codage est nécessaire pour l'obtention des performances souhaitées telles que :

- avoir une bonne efficacité de transfert d'énergie,
- assurer un bon rapport signal sur bruit,
- minimiser la consommation énergétique pendant le fonctionnement,

- faciliter la détection par la station de base, même en présence de bruit et en présence d'autres étiquettes.

2.3.5 Collision

La collision survient lorsqu'il y a présence d'au moins deux étiquettes dans le champ d'action d'un lecteur. Dans ce cas, il est possible que les étiquettes deviennent des sources de bruit pour les transmissions issues de leurs voisines. Les données reçues par le lecteur seront alors erronées.

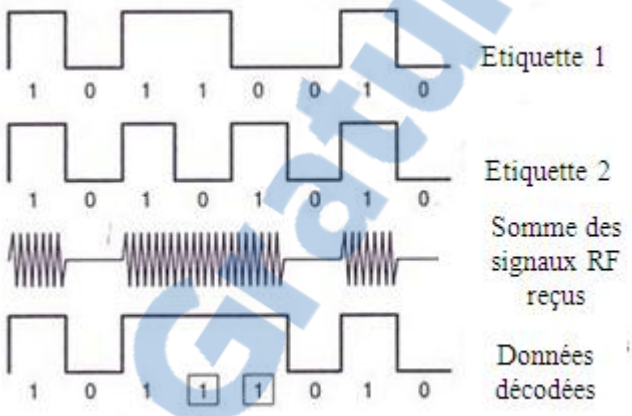


Figure 2.09 : *Exemple de collision en RFID*

Le codage des données utilisé est le codage NRZ et la modulation utilisée pour transmettre le message est une modulation d'amplitude ASK. Les étiquettes 1 et 2 diffusent leurs messages respectifs à la station de base. Les signaux fréquentiels sont alors superposés et la station de base reçoit et décode ce message. Par collision, les données reçues ne correspondent ni à celles provenant de l'étiquette 1, ni à celles provenant de l'étiquette 2. On conclut donc à des erreurs.

Pour résoudre ce problème de collision, des méthodes d'anticollision ont été développées afin d'assurer l'intégrité de la transmission des données.

La répartition spatiale des communications propose de réduire l'angle d'ouverture du champ électromagnétique du lecteur. Celui-ci devra alors effectuer un balayage pour trouver une étiquette. Cela réduit la probabilité de rencontrer plusieurs étiquettes simultanément.

La répartition fréquentielle propose d'utiliser plusieurs fréquences pour les communications. Il est cependant possible de trouver, par exemple, des systèmes utilisant le FDMA. Il s'agit d'un mode de multiplexage consistant à diviser la gamme de fréquence disponible en canaux d'une largeur de bande spécifique.

La majorité des systèmes sans contact optent pour la répartition temporelle dans laquelle on peut trouver la méthode déterministe. Les algorithmes déterministes utilisent l'UID (Unique IDentificaton) - numéro unique identifiant l'étiquette lors de sa fabrication - propre à chaque étiquette RFID. Le principe consiste en un système de vote qui autorise le lecteur à sélectionner une étiquette présente dans son champ d'action, à partir d'une liste contenant les identités des étiquettes. Ceci nécessite donc de la mémoire et un nombre limité d'étiquettes associés au lecteur.
La figure suivante recense les principales méthodes d'anticollision :

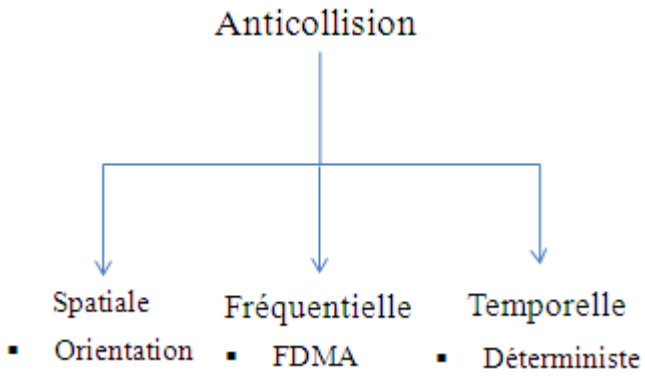


Figure 2.10 : *Méthodes d'anticollision*

2.4 **Normes**

Il existe plusieurs normes qui régissent le domaine de la RFID. Celles-ci ont pour but de garantir l'interopérabilité des systèmes RFID et de protéger les utilisateurs des impacts de cette technologie sur la santé et le respect de la liberté individuelle. La normalisation des systèmes RFID est régie par l'ISO (International Standardisation Organisation) et l'IEC (International Electrotechnical Commision).
On distingue différents types de normes :

- Les normes techniques, telles que les normes relatives aux interfaces d'air de la série ISO 18000, ISO 15693 et ISO 14443.
- Les normes relatives aux données, telles que l'ISO 15693, l'ISO 15418, la série ISO 7816 et ISO 15434 qui régissent les identifiants.
- Les normes relatives à la conformité, telles que la série ISO 18047 et ISO 10373, afin de permettre l'interopérabilité entre les produits de divers fabricants.

Le tableau suivant donne une liste de quelques normes ISO appliquées à la technologie RFID :

Norme	Description
ISO 14443	Produits à couplage de proximité avec une distance de fonctionnement jusqu'à 10 cm
ISO 15961	Identification par radiofréquence pour la gestion d'objet
ISO 15693	Produits à couplage éloigné avec une distance de fonctionnement jusqu'à 70 cm
ISO 11785	Identification animale

Tableau 2.03: *Quelques normes ISO appliquées à la RFID*

2.5 **Applications**

Les systèmes RFID sont actuellement utilisés pour de très nombreuses applications :

- Paiement électronique : comme les cartes de paiement, les tickets d'entrée, etc.
- Identification de personnes ou de biens : comme les badges d'identification à lecture sans contact, les systèmes antivol, etc.
- Suivi de produits sensibles : pour le contrôle des aliments par exemple : des tags sont placées sur les aliments afin de mesurer et d'enregistrer la température.
- Produit communiquant et domotique : aux Etats-Unis, un réfrigérateur est capable de détecter l'inexistence d'un produit pour pouvoir faire une commande sur internet.
- Etiquetage des animaux : des troupeaux de vaches, moutons, chevaux, etc. portent des puces RFID dans le but d'assurer leur traçabilité et/ou localisation.

2.6 **Avantages**

Les avantages de la RFID sont nombreux :

- Lecture en masse d'étiquettes
- Lecture à distance, sans contact et sans visibilité directe
- Détection automatisée d'objets identifiés
- Toute perte ou vol de la puce est quasi impossible
- Possibilité de différencier plusieurs objets simultanément grâce à un système d'anticollision

- Meilleure résistance de la puce aux agressions extérieures car elle peut être recouverte d'un emballage
- Grande durée de vie et une grande fiabilité
- Diminution du temps de réaction devant une information nouvelle
- Dimension réduite des étiquettes passives : il y a possibilité pour les étiquettes d'être placées directement sous l'emballage et même à l'intérieur du produit.

2.7 **Inconvénients**

Les avantages énumérés ci-dessus ne sont pas sans contrainte :

- Perturbation possible du signal radio par la présence de métal, ou avec d'autres radiofréquences
- Coût élevé pour les étiquettes actives
- Problème de santé publique

2.8 **Technologie NFC**

La technologie NFC ou Technologie de communication de proximité (en anglais, Near Field Communication) est une technologie de communication sans fil permettant l'échange de données entre deux dispositifs équipés de cette technologie, jusqu'à une distance d'environ 10 cm.
La NFC est un dérivé de la technologie RFID. [21]

2.8.1 Fonctionnement et caractéristiques techniques

2.8.1.1 Les tags NFC

Les tags NFC sont similaires aux radio-étiquettes RFID. Ce sont des étiquettes électroniques équipées de la technologie NFC.
Ils sont composés d'une puce de stockage contenant les données destinées à effectuer une action sur un périphérique situé dans son champ d'action et d'une antenne. Ils peuvent contenir tout type de données de façon sécurisée comme des informations de carte bancaire, des textes, etc.
Les tags NFC se basent sur des spécifications standard du « NFC forum ». Ce dernier a défini quatre types de tags qui fournissent des vitesses et des capacités différentes en termes de mémoire, de sécurité et de réécriture. [21] [22]

Nom	Norme	Mémoire	Vitesse	Exemple
Type 1	ISO/IEC 14443A	96o à 2Ko	106 Kbps	Topaz 512
Type 2	ISO/IEC 14443A	48o à 2Ko	106 Kbps	Ultralight
Type 3	JIS X 63194	Jusqu'à 1Mo	212 Kbps	Sony Felica
Type 4	ISO/IEC 14443A-B ISO 7816-4	Jusqu'à 32Ko	106 Kbps	NXPDESfire

Tableau 2.04: *Tableau descriptif des quatre types de tags*

2.8.1.2 Communication

La NFC reprend les principes de communications utilisées par la RFID. L'échange d'informations se fait entre deux équipements sans contact : un lecteur et un tag. [15]

Il existe deux modes de communication en NFC :

- Mode actif : dans un premier temps, le lecteur va générer un champ afin d'envoyer les requêtes au tag. Puis, dans un second temps, ce dernier va générer son propre champ de réponse. Les deux dispositifs disposent d'une alimentation et émettent des ondes pour créer une connexion
- Mode passif : seul le lecteur émet des ondes et le tag utilise l'énergie du lecteur pour transmettre des données. Il lui répond sans générer à son tour un champ mais en utilisant celui du lecteur.

2.8.1.3 Modes de fonctionnement

La NFC a trois modes de fonctionnement :

- Mode lecture :

  Un appareil équipé de la technologie NFC se charge de lire des tags NFC pour en tirer des informations.

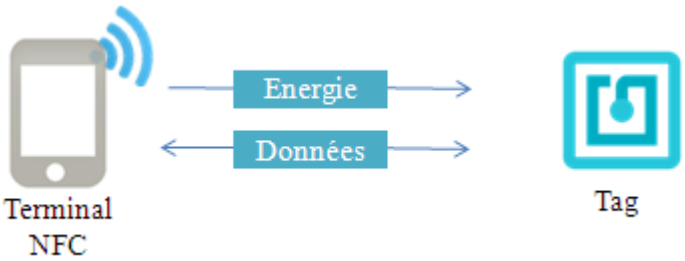


Figure 2.11 : *Mode lecture*

- Mode émulation de carte :

  L'appareil fonctionne comme une carte à puce sans contact sur lequel sont stockées des informations.

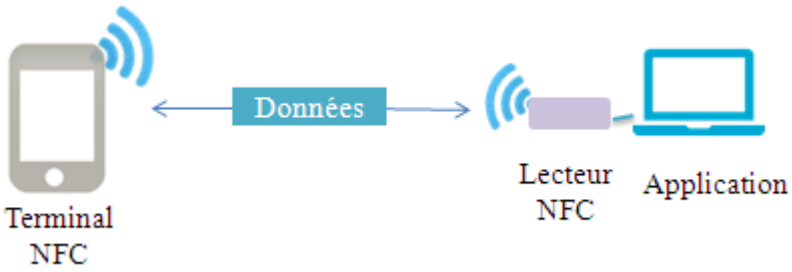


Figure 2.12 : *Mode émulation de carte*

- Mode peer to peer :

  Ce mode de fonctionnement permet l'échange de données entre deux appareils équipés de la NFC.

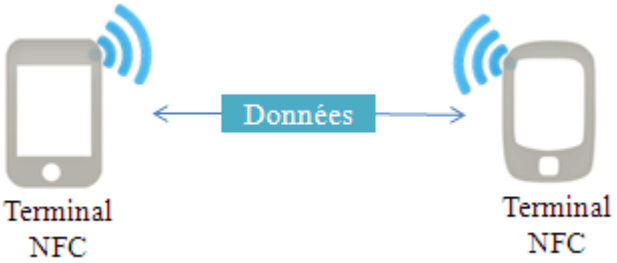


Figure 2.13 : *Mode peer to peer*

2.8.1.4 NFC et les communications sans fil

La NFC est une technologie sans fil. Au même titre que Bluetooth, elle fait partie des WPAN (Wireless Personal Area Network). C'est une famille des réseaux sans fils à courte portée.
La NFC opère sur une fréquence de 13.56 MHz et à des taux allant de 100Kb/s à 1Mb/s, nécessitant une distance pratique de 10 cm.

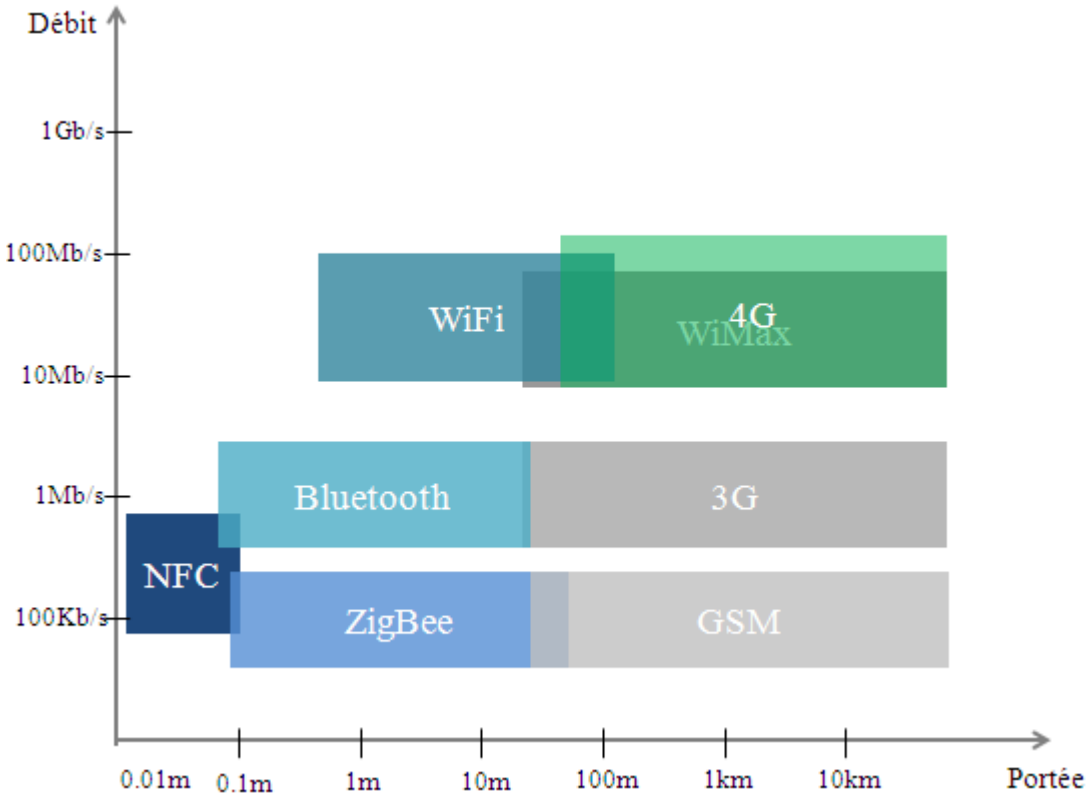


Figure 2.14 : *Positionnement de la NFC par rapport aux autres communications sans fil*

2.8.1.5 Collision

La collision n'existe pas en NFC. Ceci est dû à la faible distance de communication entre les deux périphériques lors de la communication.

2.8.2 Normes

La technologie NFC est présente dans divers dispositifs tels que les téléphones portables, les cartes à puce, les lecteurs de cartes, etc. Pour obtenir l'adoption des utilisateurs de cette technologie, les acteurs concernés tels que les fabricants, les développeurs, etc. doivent travailler en collaboration dans le but d'assurer une interopérabilité des applications. De ce fait, cela nécessite une accréditation de la part d'organismes de normalisation.

Les normes NFC sont éditées par les organismes suivants : ISO/IEC, ECMA (European Computer Manufacturers), ETSI (European Telecommunications Standards Institute). [22]

La norme ISO/IEC 14443 est une norme portant sur les cartes de proximité. Elle décrit plusieurs couches (de 1 à 4). Le tableau suivant présente les différentes couches de la norme ISO/IEC 14443 :

Norme	Intitulé	Description
ISO/IEC 14443-1	Physical Layer	Caractéristiques physiques de la carte
ISO/IEC 14443-2	RF Signal	Fréquence à laquelle l'émetteur et le récepteur doivent fonctionner. Il existe deux variantes A et B qui différent sur la modulation et l'encodage binaire utilisé
ISO/IEC 14443-3	Activation and anticollision	Initialisation de la communication entre l'émetteur et le récepteur et principe d'anticollision
ISO/IEC 14443-4	Transmission protocol	Protocole utilisé dans la transmission d'information.

Tableau 2.05: *Les couches de la norme ISO/IEC 14443*

Deux acteurs industriels majeurs dont Philips et Texas Instruments n'ont pas pu s'entendre sur la façon dont la modulation radiofréquence (ISO 14443-2) devait se faire. Ils ont opté ainsi pour deux types de dispositifs, nommés Type A (NFC-A) pour Philips et type B (NFC-B) pour Texas Instruments.

A part la norme ISO/IEC 14443, il existe d'autres normes mises en jeu pour la NFC.

2.8.3 Différences entre RFID et NFC

La NFC est un genre de RFID. Cette dernière comprend trois grandes familles qui se distinguent principalement par leurs fréquences de fonctionnement et par la distance de lecture/écriture :

- La famille LF : utilisée pour l'identification des animaux.
- La famille HF : se retrouve dans le transport, les cartes à puce sans contact et les mobiles. Cette famille HF porte le nom générique de NFC.
- La famille UHF : utilisée à des fins industrielles, telles que la vérification des stocks dans un entrepôt ou la réalisation d'inventaire. Cette famille UHF est régulièrement appelée RFID par les industriels.

Le tableau suivant montre les principales différences entre la RFID et la NFC :

RFID	NFC
Les étiquettes RFID peuvent être lues à partir d'une plus grande distance (jusqu' à 100m)	Les étiquettes NFC ne peuvent être lues que sur une courte portée (10cm maximum)
Lecture de plusieurs étiquettes RFID à la fois	Lecture d'une seule étiquette NFC à un moment
-	Fonctionnalité P2P

Tableau 2.06: *Différences entre RFID et NFC*

Toutefois, ces deux technologies présentent des points communs du point de vue principe de fonctionnement : un lecteur, une étiquette et un échange de données.

2.8.4 Applications

Les applications de la NFC sont nombreuses :

- Contrôle d'accès ou e-ticketing : l'utilisateur place seulement le dispositif stockant le code d'accès ou le billet électronique à proximité du lecteur
- Paiement mobile
- Transfert pair à pair de données entre deux dispositifs compatibles NFC
- Téléchargement d'application, ouverture d'un lien vers une page web, etc. suite à un tag présent sur une affiche (smart poster).

2.8.5 Avantages

Les principaux avantages de la NFC sont les suivants :

- Il est possible d'utiliser des puces sans batterie, ce qui permet d'avoir des étiquettes NFC de la taille et de l'épaisseur d'un timbre, rendant possible et économiquement viable des applications.
- Avec l'arrivée de la NFC sur la plupart des Smartphones, on peut désormais considérer qu'il s'agit d'une technologie qui va se généraliser, rendant les différents composants interopérables.
- Les puces NFC sont moins sensibles aux contraintes environnementales (électromagnétisme, température, etc.), rendant leur portabilité plus aisée.

- Niveau de sécurité accru car il est impossible d'exploiter les informations au-delà d'une courte portée.
- Facilité d'exécution

2.8.6 Inconvénient

Cependant, la NFC nécessite d'avoir de l'énergie en réserve dans son téléphone portable pour pouvoir bénéficier de certains services comme le paiement mobile.

2.9 **Conclusion**

La technologie RFID repose sur l'utilisation d'une puce électronique reliée à une antenne miniature émettrice d'ondes radio et d'un lecteur. Cette technologie utilise les bandes de fréquences LF, HF et UHF. La RFID est une technologie puissante et révolutionnaire qui a un potentiel d'application énorme dans de nombreux secteurs comme la production, l'identification des animaux, l'accès sécurisé, e-Passeport, etc. et va devenir de plus en plus présente dans notre vie quotidienne.
Une version plus évoluée de la technologie RFID est très présente actuellement ; il s'agit de la technologie NFC. Celle-ci n'est autre que la RFID utilisant les HF. Cependant, des différences existent entre ces deux technologies. L'usage de cette technologie ouvre beaucoup de perspectives dans plusieurs domaines. Les services proposés sont innovants et offrent un côté pratique pour l'utilisateur. La majeure partie des cartes à puce sans contact ont vu le jour grâce à cette technologie.

CHAPITRE 3
LES CARTES A PUCE

3.1 Introduction

Depuis son apparition dans les années 70, les cartes à puce font partie intégrante de notre vie quotidienne et leur utilisation n'a cessé d'augmenter et de se diversifier : télécartes, cartes bancaires, cartes Vitale, cartes de décryptage de télévision par satellite, etc.

3.2 Caractéristiques et familles de cartes à puce

Une carte à puce est une carte en matière plastique de quelques centimètres de côté et moins d'un millimètre d'épaisseur, portant une puce électronique. [23]

3.2.1 Caractéristiques

Les caractéristiques d'une carte à puce électronique sont les suivantes :

- Objet portable stockant des données
- Objet sécurisé
- Nécessite un lecteur pour pouvoir fonctionner
- Transmission radiofréquence en lecture et écriture (pour les cartes à puce sans contact)

3.2.2 Familles de cartes à puce

Il existe deux grandes familles de cartes à puce que l'on peut classer suivant les technologies utilisées en interne :

3.2.2.1 Carte à puce à mémoire

Il s'agit du premier modèle de carte à puce électronique. Elle possède une mémoire mais pas de microprocesseur. Les seules possibilités d'opérations sont des lectures/écritures en mémoire. Sa programmation n'est pas possible puisqu'elle ne contient aucun microprocesseur La taille de la mémoire est minime car elle est seulement de quelques kilo-octets. [26]

3.2.2.2 Carte à puce à microprocesseur

Il s'agit d'une carte à puce beaucoup plus évoluée que la précédente. C'est un véritable micro-ordinateur avec un microprocesseur, de la mémoire RAM (Random Access Memory), et de la

mémoire allouée aux données. Elle est de ce fait nommée « smart card ».
La puce embarque un microprocesseur lui permettant d'être programmée pour effectuer un ou plusieurs types d'applications. Elle possède soit une interface électronique par contact, soit elle est sans contact et fonctionne par fréquence radio.
Parmi les cartes à microprocesseur, il faut distinguer trois catégories différentes :

- Les cartes à puce « vierges » : qui ne contiennent préalablement rien.
- Les cartes à puce « personnalisables » : qui contiennent un OS (Operating System) programmé par le fabriquant.
- Les cartes à puce « à OS ouvert » : dans lesquelles on peut réaliser une application « sur mesure » à l'aide d'une programmation plus facile car elle est réalisée à l'aide de langage évolué comme Java ou C.

La première implémentation de la smart card était la CP8 avec 36 octets de RAM, 1Ko d'EPROM (Erasable Programmable Read Only Memory) et 1.6 Ko de ROM (Read Only Memory). [24] [26]

3.3 **Différents types de cartes à puce**

On distingue trois grands types de cartes à puce qui se différencient par la technique utilisée pour communiquer avec le lecteur :

- Carte avec contact : l'interface entre les contacts de la puce et ceux du lecteur est le micromodule.
- Carte sans contact : par radiofréquence à courte ou moyenne portée, via une antenne interne dont les spires sont moulées dans l'épaisseur de la carte.
- Carte mixte : appelée encore « dual interface », c'est une combinaison des deux précédentes.

3.4 **Composants essentiels d'une carte à puce**

3.4.1 Carte à puce à contact

Une carte à puce avec contact est physiquement composée de trois éléments :

- La carte plastique
- Le micromodule
- La puce

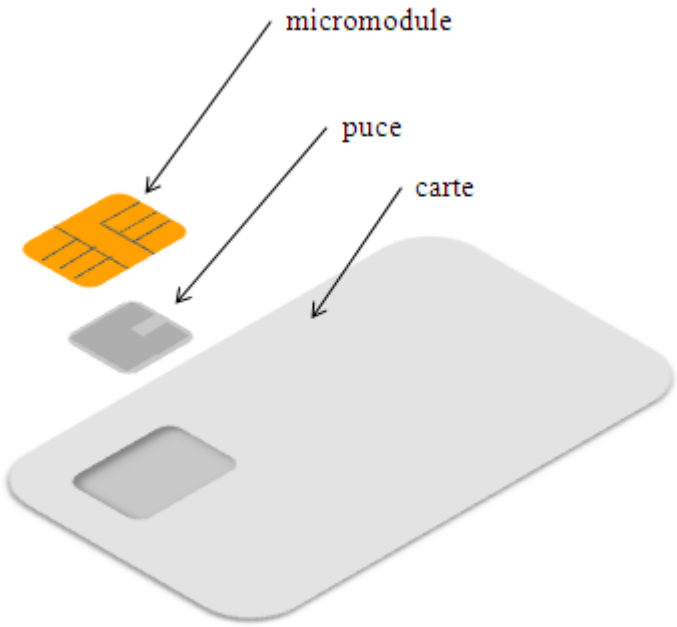


Figure 3.01 : *Schéma d'une carte à puce à contact*

La carte plastique est le socle physique de base de la carte. Sur celle-ci se trouve la puce qui contient des données ou des programmes à exécuter.

Le support plastique de la puce a des dimensions précises définies selon les standards de normalisation. Le standard ISO 7816-2 par exemple, définit les dimensions de la puce : surface < 25 mm² et épaisseur < 0,3 mm.

Le format a effectivement une grande importance pour les lecteurs de cartes : une carte dont le format n'est pas conforme ne pourra pas être lue par un terminal.

Le micromodule est un circuit imprimé très mince logé à l'intérieur de la carte, seule la partie visible depuis l'extérieur et dont les contacts servent d'interface avec le lecteur. La puce se trouve sous le micromodule.

La puce est un circuit électronique capable de manipuler des données de façon sécurisée. Elle n'a pas besoin d'accéder à une base de données distante pour pouvoir effectuer une transaction puisqu'elle possède sa propre capacité de stockage et sa propre capacité de calcul.

3.4.2 Carte à puce sans contact

Une carte à puce sans contact fonctionne sans contact mécanique et sans alimentation directe. A la différence de la carte à contact, elle ne possède plus de micromodule et embarque une antenne bobinée dans la carte qui reçoit de l'énergie radiofréquence transmise par un lecteur de carte.

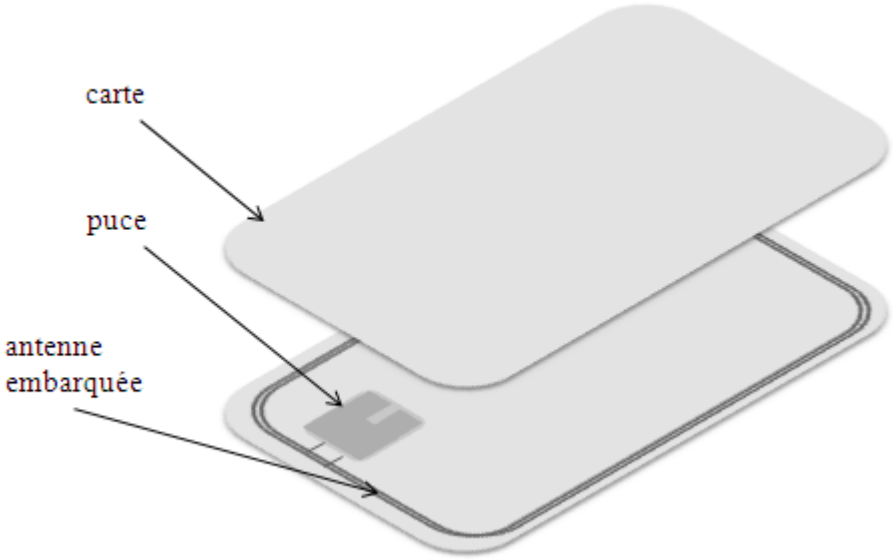


Figure 3.02 : *Schéma d'une carte à puce sans contact*

Les cartes à puce sans contact font partie des produits RFID. Elles utilisent le champ électromagnétique d'un lecteur pour son alimentation et pour le transfert des données.

3.5 **Lecteurs de cartes à puce**

La carte à puce seule ne serait d'aucune utilité sans un lecteur, elle ne peut fonctionner de manière autonome. Du fait des différents types de cartes à puces qui existent, les lecteurs elles-mêmes sont de deux types : les lecteurs par contact et les lecteurs sans contact.

3.5.1 Lecteurs par contact

Les lecteurs par contact présentent une entaille dans laquelle s'insère la carte à puce à contact. Le contact se fait plus précisément au niveau du micromodule qui sert aussi bien à l'alimentation de la carte que le transfert de données.

Lors de son utilisation, une carte suit trois étapes bien distinctes :

- Introduction de la carte : lorsque la carte est insérée dans le lecteur elle se trouve alimentée en énergie et est réinitialisée
- Exécution de commande : elle consiste en la réception d'une commande et à l'exécution de celle-ci.
- Déconnexion : elle correspond à une coupure de l'alimentation électrique de la carte. Celle-ci se retrouve alors dans l'impossibilité de faire quoi que ce soit

Figure 3.03 : *Lecteur de carte à puce à contact d'un GAB*

3.5.2 Lecteurs sans contact

La lecture de la carte à contact nécessite toujours un lecteur par contact. La tendance actuelle est au « sans contact » : la carte et le terminal échangent leurs informations grâce à un signal radio, d'une portée de quelques centimètres (NFC).

Figure 3.04 : *Lecteur de carte à puce sans contact*

Le dialogue entre la carte et le lecteur débute lorsque la carte entre en contact avec l'antenne d'un lecteur :

- la carte fait un reset et attend une commande du lecteur appelée REQ (REQuest)
- la carte répond par ATQ (Answer To ReQuest)
- le processus d'anticollision est enclenché
- le lecteur procède à l'élection d'une carte

- la carte sélectionnée envoie une réponse ATS (Answer To Select) qui contient les caractéristiques de la carte
- l'échange des données est établi

La communication prend fin lorsque la carte quitte la zone d'influence du lecteur.

La figure suivante présente l'algorithme d'identification d'une carte qui précède toute opération d'échange de données.

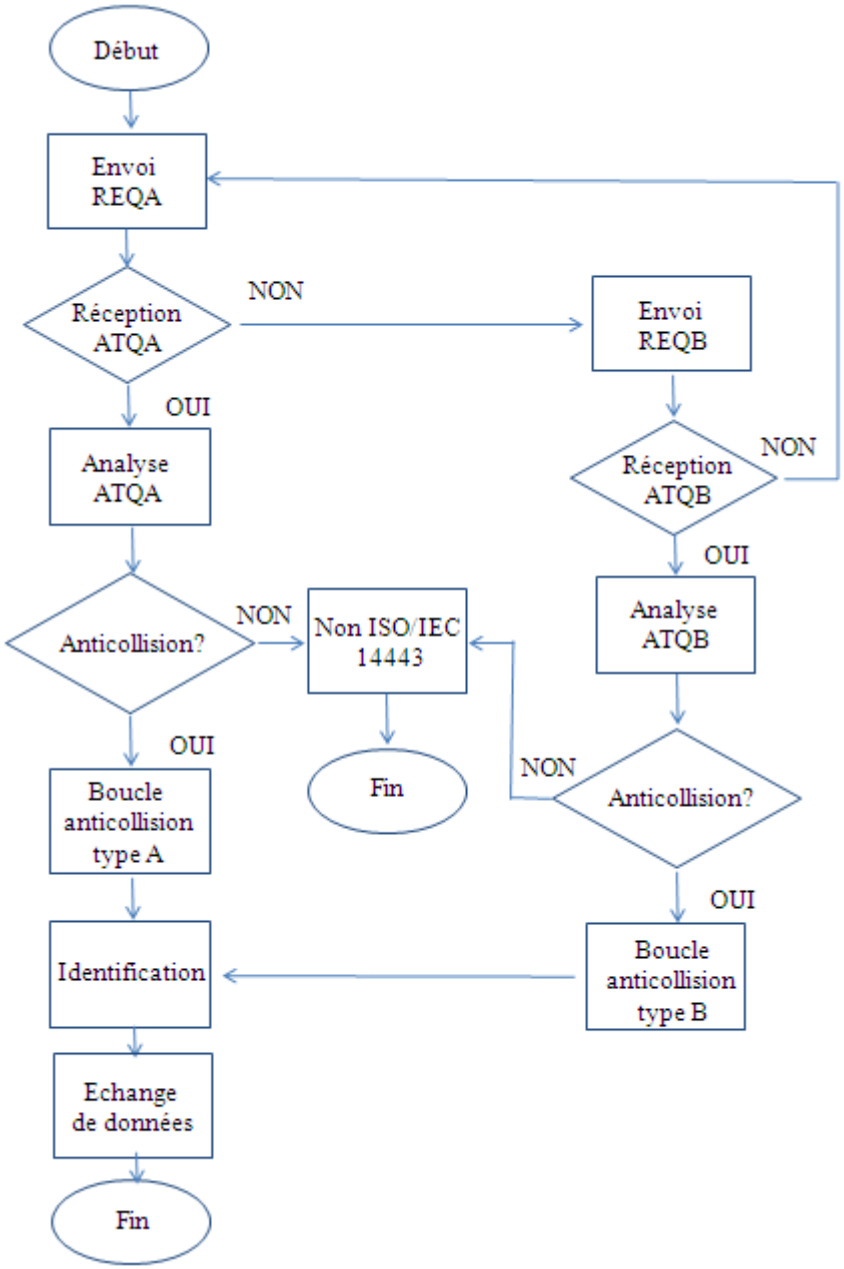


Figure 3.05 : *Organigramme de l'identification d'une carte par un lecteur*

En réalité, l'existence des deux variantes A et B de la norme ISO/IEC 14443-2 (**Tableau 2.05**) contraint le lecteur à procéder successivement à une requête REQA puis REQB.
Si la carte répond à la requête REQA avec une réponse ATQA, alors c'est une variante A, s'il répond à la requête REQB avec une réponse ATQB, alors c'est une variante B.
Après réception des réponses ATQ, l'étape qui suit est d'identifier si la carte gère l'anticollision. Pour cela on analyse la valeur ATQA ou ATQB. Cette valeur, sur deux octets contient plusieurs informations dont la taille de l'ID et la gestion ou non de l'anticollision. Toutes les cartes conformes à la norme ISO/IEC 14443 doivent gérer l'anticollision.
Si la carte gère l'anticollision, la boucle anticollision est déclenchée. Cette étape est essentielle car elle permet en fait de lier le lecteur à une seule carte vu la possibilité d'avoir plusieurs cartes dans le champ magnétique du lecteur.
A l'issue de la boucle anticollision, une seule carte est sélectionnée et le lecteur se trouve en possession de deux informations : l'UID et le SAK (Select AKnowledge). Selon la valeur des bits de ce dernier, il est possible d'identifier si la carte supporte la couche ISO/IEC14443-4 ou pas afin d'utiliser le protocole adéquat pour la transmission de l'information.
Les cartes « dual » qui offrent des interfaces contact et sans contact sur une seule et même carte sont compatibles avec les deux types de lecteur.

3.6 **Technologies des puces électroniques**

3.6.1 Les différents types de mémoires

Une mémoire est un composant électronique capable de stocker des données. On distingue deux grandes catégories de mémoires :

- La mémoire centrale : permet de mémoriser temporairement des données lors de l'exécution des programmes. La mémoire centrale correspond à ce qu'on appelle la mémoire vive.
- La mémoire de masse : permet de stocker des informations à long terme, y compris lors de coupure d'alimentation. La mémoire de masse correspond aux dispositifs de stockage magnétique, tels que le disque dur, aux dispositifs de stockage optique, comme les CD-ROM et DVD –ROM, ainsi qu'aux mémoires mortes. [27]

3.6.1.1 La mémoire vive ou RAM

C'est une mémoire utilisée comme espace de stockage temporaire de données ou de programmes.

Elle perd son contenu dès qu'elle est hors tension. Elle peut être lue et écrite à l'infini.

3.6.1.2 La mémoire morte ou ROM

C'est une mémoire qui n'a pas besoin d'énergie pour sauvegarder l'information qu'elle contient. Le contenu de cette mémoire n'est pas modifiable : elle est programmée une fois pour toute en usine.

3.6.1.3 L'EEPROM

C'est une variante de la ROM dont le contenu peut être effacé par des impulsions électriques. Elle est souvent désignée sous le terme de NVM (Non Volatile Memory). Elle permet le stockage de données même si elle est hors tension.

3.6.2 Le Microprocesseur

Un microprocesseur est un circuit intégré complexe caractérisé par une très grande intégration et doté des facultés d'interprétation et d'exécution des instructions d'un programme. Il est chargé d'organiser les tâches précisées par un programme et d'assurer leur exécution.
Physiquement, un microprocesseur se présente sous la forme d'un circuit intégré muni d'un nombre important de broches.

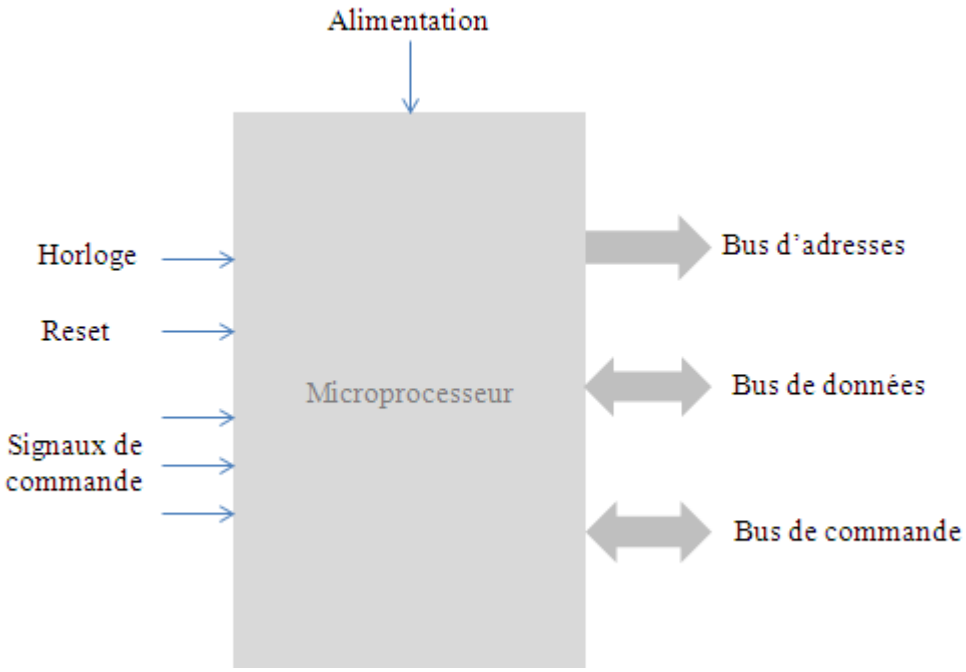


Figure 3.06 : *Schéma fonctionnel d'un microprocesseur*

L’interfaçage d’un microprocesseur nécessite des lignes de communications appelées : « bus ». Il existe trois types de bus ayant chacun une fonction particulière :

- Bus d’adresses : il permet d’adresser un élément par le microprocesseur. Il est unidirectionnel
- Bus de données : il permet de véhiculer des données du microprocesseur vers un composant ou d'un composant vers le microprocesseur. Il est donc bidirectionnel.
- Bus de commande : il permet de véhiculer les signaux de contrôles et de commandes tels que les signaux Write Enable, Chip Enable, etc. Ce bus sert à coordonner tous les échanges d'informations décrits précédemment. Il véhicule des données qui valident la mémoire et les ports d'entrées sorties. [27]

3.6.3 Technologies des puces électroniques

Les puces électroniques sont différentes sur le plan de la technique et de l'utilisation. On distingue deux familles de puces électroniques : les puces à mémoire et les puces à microprocesseur.

3.6.3.1 Les puces à mémoire

Les puces à mémoire servent à stocker des informations. Elles comportent un bloc de sécurité qui contrôle l’accès à une mémoire de type EEPROM. Les données applicatives sont transférées via un port d’entrée/sortie et sont stockées dans l’EEPROM. [26]. La ROM stocke un code PIN (Personal Identification Number) permettant de restreindre l’accès à l’EEPROM.

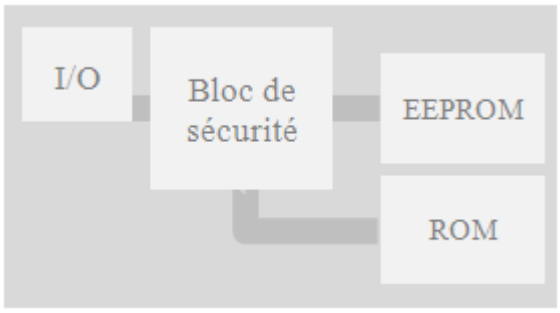


Figure 3.07 : *Architecture interne d’une puce à mémoire*

3.6.3.2 Les puces à microprocesseur

Contrairement aux puces à mémoire, les puces à microprocesseur sont capables de stocker des informations mais possèdent en surplus une capacité de traitement et de sécurité. Les capacités

mémoires sont comprises entre 128 et 256 Ko pour la ROM, 64 et 128 Ko pour l'EEPROM, 4 et 8 Ko pour la RAM.

La ROM contient un système d'exploitation.

Le cryptoprocesseur est un processeur optimisé pour les tâches de cryptographie.

Le processeur est très faible comparé aux processeurs des PC, et ne contient qu'un jeu d'instructions très limité.

La RAM, effacée à chaque nouvelle utilisation de la carte, stocke les données d'un programme à l'exécution et des données sensibles (clés de cryptographie).

L'EEPROM stocke une ou plusieurs applications à exécuter sur la carte. Elle n'est pas effacée et les données sont donc réutilisables dans le même état à chaque utilisation de la carte. [26]

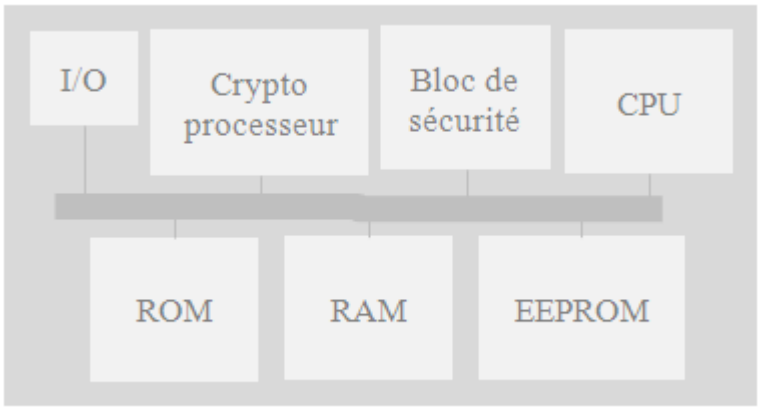


Figure 3.08 : *Architecture interne d'une puce à microprocesseur*

3.7 **Normes**

La force de la carte à puce réside dans son interopérabilité qui peut se résumer en deux principes :

- Tous les lecteurs peuvent lire une carte particulière
- Toutes les cartes peuvent être lues par un lecteur particulier

Les cartes sont très standardisées car elles doivent donc être utilisables avec la gamme la plus large possible de lecteurs dans le monde entier. C'est la raison pour laquelle les caractéristiques des cartes à puce ont été fixées par des règles reconnues universellement qui appartiennent à une famille de standards internationaux. De ce fait, la normalisation ne concerne pas seulement la puce, mais aussi les dimensions physiques de la carte.

Il existe plusieurs organismes qui interviennent dans la normalisation des cartes à puce tels que : l'ETSI (European Telecommunications Standards Institute) pour les téléphones mobiles,

l'EMVCo (Europay Mastercard Visa Consortium) consortium bancaire regroupant Visa, MasterCard et JCB (Japan Card Bureau), l'ECMA (European Computer Manufacturer Association) pour la communication NFC.

Les principaux standards de la carte à puce sont définis par l'ISO. Pour définir une carte à puce, il faut au moins normaliser trois types de paramètres différents :

- Les paramètres physiques qui indiquent la taille de la carte et la position de la puce et de ses contacts.
- Les paramètres électriques qui précisent les tensions d'alimentation et le brochage de la puce sur la carte.
- Les paramètres logiciels qui définissent le mode de dialogue avec la carte, les commandes qu'elle peut interpréter et son comportement face à ces dernières.

Il existe deux normes bien distinctes pour les cartes à puce : les normes des cartes à puce avec contact et celles des cartes à puce sans contact.

3.7.1 Normes des cartes à puce à contact

La norme ISO 7816 fait partie des principales normes des cartes à puce à contact. Elle garantit la compatibilité physique entre les cartes et les lecteurs. La série de normes ISO 7816 s'est focalisée sur les dimensions de la carte, les positionnements des contacts, l'alimentation électrique ainsi que les protocoles de dialogue entre carte et lecteur.

Le tableau ci-dessous donne une liste des principales normes ISO dans le cas des cartes à puce à contact.

Norme	Description
ISO 7816-1	Caractéristiques physiques de la carte
ISO 7816-2	Dimension et position des contacts
ISO 7816-3	Signaux électriques et protocoles de transmission
ISO 7816-4	Commandes de base des cartes à puce pour communiquer avec le lecteur

Tableau 3.01: *Les principales normes ISO de la carte à puce à contact*

3.7.2 Normes des cartes à puce sans contact

La série de normes ISO 10536 définit les aspects physiques des cartes à puce sans contact. Les détails supplémentaires correspondent à la distance de fonctionnement entre le lecteur et la carte. Cependant, la série ISO/IEC 14443 (technologie de carte de proximité) (**Tableau 2.05**) est utilisée pour l'écrasante majorité des déploiements de cartes sans contact.

3.8 **Cycle de vie**

La vie d'une carte à puce est constituée de trois phases :

- Phase amont : le développement du système d'exploitation, la conception de la puce
- Phase de création : fabrication, encartage, initialisation
- Phase de circulation : personnalisation, distribution, utilisation, mort

3.8.1 Phase amont

La première phase consiste au développement du système d'exploitation et à la conception de la puce.

3.8.2 Phase de création

3.8.2.1 Fabrication de la puce

Un programme est inscrit en mémoire ROM définissant les fonctionnalités de base de la carte : il s'agit du système d'exploitation.

3.8.2.2 Encartage

L'encartage est l'assemblage de la puce, du micromodule et du support plastique.

3.8.2.3 Initialisation

L'initialisation est l'inscription en mémoire des données spécifiques propres à l'application dans laquelle la carte va s'insérer. A ce stade, la mémoire va être organisée et répartie suivant les différents besoins. Les zones de travail sont définies et repérées par des indicateurs représentatifs de leur mode de fonctionnement : lecture seule, lecture/écriture, etc.

3.8.3 Phase de circulation

3.8.3.1 Personnalisation

Cette étape, réalisée par l'émetteur, est dédiée à l'adaptation au porteur final de la carte. On distingue :

- La personnalisation électrique : écriture par exemple du nom du porteur, du numéro d'abonné ou de toute autre information pertinente dans la ROM.
- La personnalisation graphique : impression et/ou embossage sur le recto et/ou le verso de tout logo, signe, photographie ou hologramme permettant une identification visuelle rapide de la carte.

3.8.3.2 Distribution

L'opérateur gère la distribution des cartes : remise de la carte (en face à face, par envoi postal, etc.), remise du code PIN, communication éventuelle sur le fonctionnement (le public n'est pas encore habitué à l'utilisation de la carte sans contact par exemple).

3.8.3.3 Utilisation

Traitement des commandes par le masque de la carte avec utilisation et modifications éventuelles des données inscrites dans la carte.

3.8.3.4 Fin de la vie d'une carte

La vie d'une carte prend fin éventuellement lorsqu'il y a invalidation logique, saturation de la mémoire, bris, perte, etc. ou lorsque le système d'exploitation devient non fonctionnel.

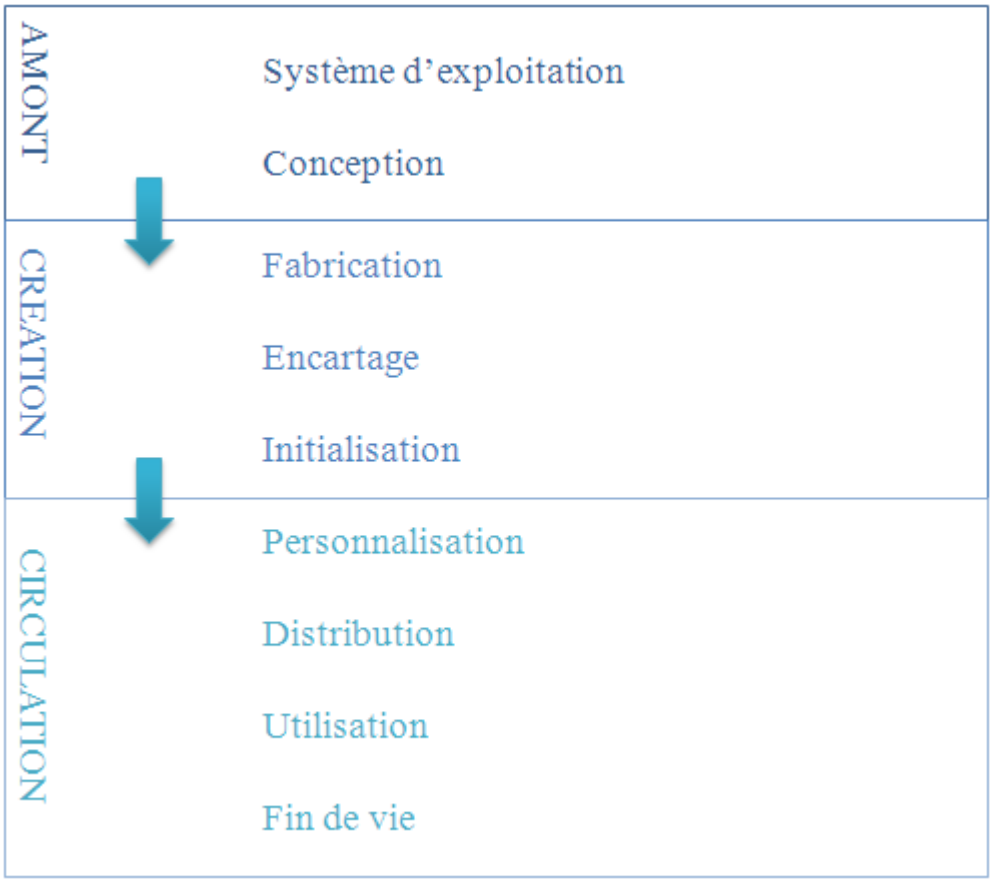


Figure 3.09 : *Cycle de vie d'une carte à puce*

3.9 **Applications**

Les capacités de la puce permettent de l'utiliser dans de nombreuses applications, que ce soit dans les télécommunications, les transports, les banques, etc.

- Télécommunications : cartes SIM insérées dans les téléphones portables.
- Banque : cartes de crédits.
- Entreprise : badges électroniques pour le contrôle d'accès.
- Transport : cartes sans contact pour les transports en commun.
- Santé : carte vitale
- Etc.

La figure **3.10** illustre les livraisons mondiales d'éléments sécurisés par secteur :

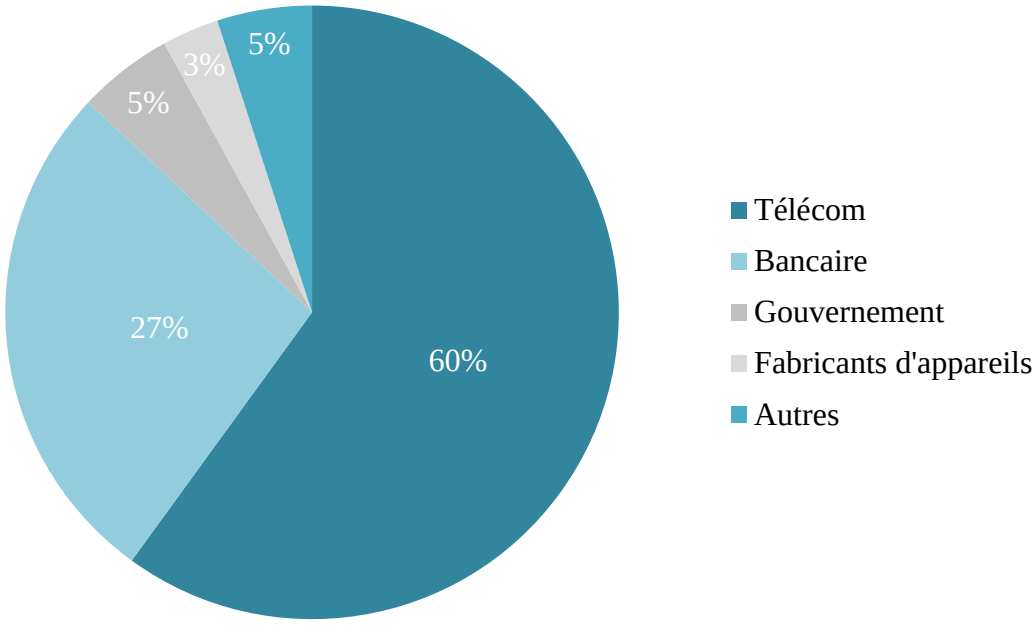


Figure 3.10 : *Eurosmart, avril 2015 : livraisons mondiales d'éléments sécurisés par secteur*

- Télécom : représente les opérateurs de réseau mobile
- Bancaire : représente les banques
- Gouvernement : représente les pouvoirs publics ainsi que les organisations de santé privées
- Fabricants d'appareils : représente les fabricants des téléphones mobiles, des tablettes, des appareils de navigation et autres appareils connectés
- Autres : concerne les transports, cartes d'accès, etc.

La télécommunication est l'un des secteurs dans lequel la puce est la plus répandue. Ce secteur compte pour plus de la moitié de la production totale. En effet, tout ce domaine est centré autour de la téléphonie. Celle-ci peut être d'ordre privé avec l'utilisation des GSM (téléphones portables) mais également d'ordre public à travers l'utilisation de la télécarte dans des cabines extérieures ou publiphones.

Le secteur bancaire représente le second plus grand secteur d'application de la carte à puce. Naturellement quand on retire de l'argent, c'est la carte bleue qui le permet.

Le gouvernement est le troisième plus gros consommateur de cartes à puce à travers des projets existants comme le projet français de carte Vitale ou les projets de cartes d'identité nationales étudiés actuellement par plusieurs pays.

Les fabricants d'appareils occupent une infime partie du marché. L'intégration de la puce NFC dans les Smartphones et les tablettes est encore actuellement un projet en phase de test et de lancement.

Le transport est l'une des applications qui a permis aux cartes à puce sans contact de connaitre une popularité croissante. Les cartes à puce et les billets intégrés sont largement utilisés par les opérateurs de transports publics à travers le monde.

3.10 **Conclusion**

Ce chapitre a été consacré à l'étude des cartes à puce. Ce sont des objets miniaturisés dotés de mémoire servant de stockage de données ou de véritables microordinateurs pouvant héberger une application. La technologie RFID a permis la naissance des cartes à puce sans contact qui coexistent actuellement avec les cartes à puce à contact. La majorité de ces cartes sans contact respectent la norme ISO 14443 donc fonctionnant à une fréquence de 13.56 MHz. Les cartes à puce sont omniprésentes dans notre vie quotidienne et ces applications facilitent notre mode de vie raison pour laquelle elles sont de plus en plus souhaitées dans de nombreux secteurs d'activité.

CHAPITRE 4
CONCEPTION ET REALISATION

4.1 Description du projet

4.1.1 Présentation du projet

La dématérialisation des documents d'identité est aujourd'hui une étape importante et incontournable au sein d'une organisation ou d'une administration. Cette nouvelle démarche devra permettre à ces dernières d'entrer dans l'ère du « zéro papier » en utilisant des moyens à base d'électronique, d'informatique et de télécommunication. Ce projet permettra de substituer tout support papier d'identité qui encombre des espaces importants, complique les tâches administratives et accroit le risque de violation d'intégrité. C'est afin de répondre à ce besoin qu'est apparue l'idée de concevoir et réaliser une application informatique pour la dématérialisation des documents d'identité « papier ».

4.1.2 Spécification des besoins fonctionnels

Les besoins fonctionnels servent à présenter les actions que doit effectuer le système en réponse à une demande présentée par un utilisateur. Le futur système doit permettre à ce dernier de :

- Créer et modifier un compte administrateur
- S'authentifier
- Créer l'identité d'une personne à partir d'une saisie ou d'une reconnaissance des caractères effectuée sur les documents papier scannés
- Afficher, rechercher et supprimer l'identité d'une personne stockée dans la base de données
- Voir l'historique des évènements
- Imprimer l'identité d'une personne
- Inscrire l'identité d'une personne sur une carte à puce RFID
- Lire l'identité d'une personne stockée sur une carte à puce RFID
- Produire des documents électroniques d'identité à partir d'informations stockées dans la base de données
- Créer des dossiers de classement arborescents
- Stocker et gérer un important volume de documents

- Rechercher facilement un document
- Consulter un document
- Supprimer un document
- Permettre l'exportation de documents numériques vers une plateforme dédiée en vue de back up et d'archivage électronique
- Assurer l'intégrité des documents
- Se connecter à un serveur de base de données distant
- Consulter des statistiques
- Consulter une aide en ligne

4.1.3 Spécification des besoins non fonctionnels

Les besoins non fonctionnels présentent les exigences internes pour le système et cachées vis à vis des utilisateurs.

- Compatibilité avec n'importe quel système d'exploitation tout en étant facile à manipuler
- La sécurité des données doit être prise en compte : sécuriser les données revient à appliquer une stratégie d'identification et d'authentification accrue au sein du système
- L'accès à la base de données doit être rapide
- L'application doit se connecter sans difficulté à un lecteur RFID
- Temps de réponse minimale

4.1.4 Objectif du projet

En tenant compte de ces besoins, l'objectif est de réaliser un SI (Système d'Information) permettant de gérer les identités de personnes. Mais cela ne se limite pas seulement à un SI ; un système de GED devrait aussi être pris en compte. Le SI permettra de collecter, stocker, traiter et diffuser de l'information tandis que l'application de GED se focalisera sur la gestion des documents électroniques créés à partir de cette information. Comme les documents générés par le système de GED sont des documents d'identité numériques, donc nécessitant un système informatique qui assure une conservation sécurisée et qui garantit l'intégrité de ces derniers, un SAE est donc nécessaire pour notre système. Le système envisagé se résume donc à un ensemble SI – GED lié à un SAE.

La figure **4.01** montre un aperçu de notre système :

Le SI de l'ensemble SI – GED prend en entrée soit des informations brutes intégrées au système par saisie, soit des documents papier scannés qui seront traités par une reconnaissance de

caractères afin d'en extraire les informations utiles. Celles-ci doivent ensuite être stockées dans une base de données pour un usage ultérieur. La GED prend à son tour son rôle en extrayant de la base de données les informations utiles pour pouvoir créer un fichier XML et un document électronique au format PDF. Ce dernier fera l'objet de tout traitement attendu d'un système de GED. Le fichier électronique au format XML sera acheminé au travers d'un réseau au SAE. Celui-ci pourra générer à partir de ce fichier XML un document électronique sécurisé au format PDF et assurera son rôle dans l'archivage électronique. Une fonctionnalité importante du système SI – GED sera de stocker des informations sur une carte à puce RFID.

Deux types de documents sont donc produits de cette chaine de traitement effectué par notre système : les documents électroniques sauvegardés au sein de l'administration et les cartes à puce RFID délivrés aux porteurs.

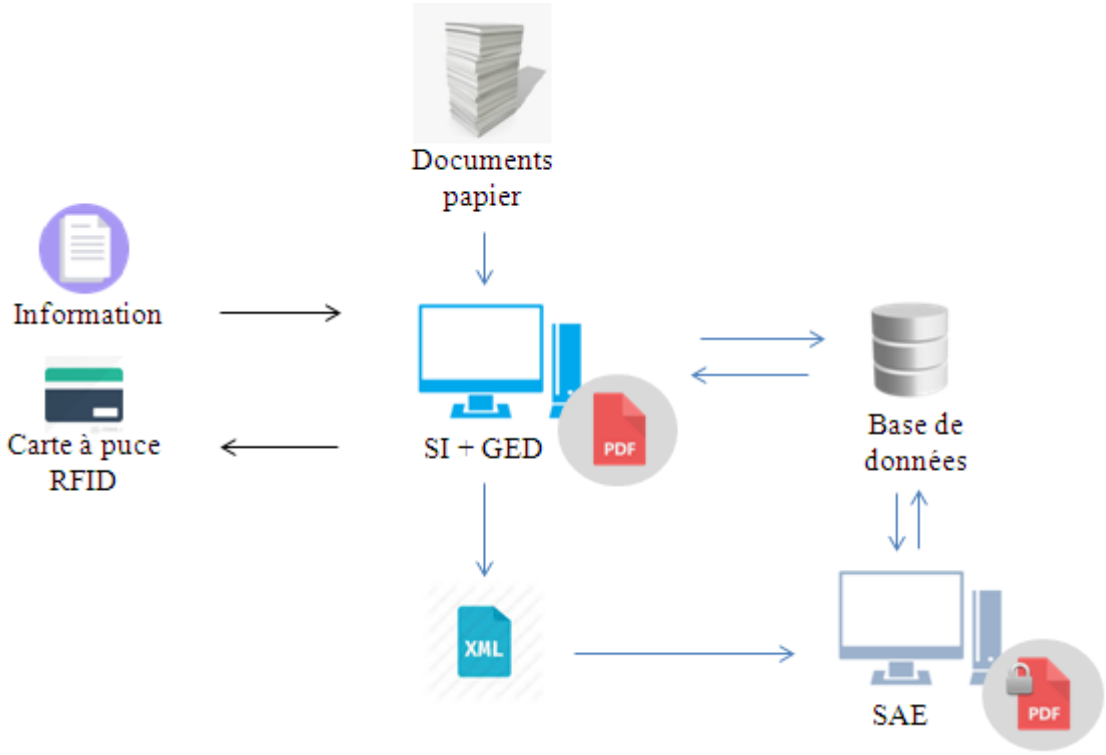


Figure 4.01 : *Aperçu du système*

4.2 **Outils de travail**

Cette partie détaille les différents outils utilisés aussi bien logiciels que matériels pour la réalisation du projet.

4.2.1 Technologie de communication sans fil

La technologie de communication sans fil utilisée pour l'échange de données entre le lecteur et la carte à puce est la NFC. Cette technologie est présente, via une puce, dans des cartes de transport, de paiement, dans des ordinateurs, des Smartphones, etc.

Google Wallet, par exemple, est un système de paiement par téléphone mobile proposé par Google permettant de payer via NFC : on lui confie les identifiants bancaires, qui sont échangées avec la borne chez le commerçant.

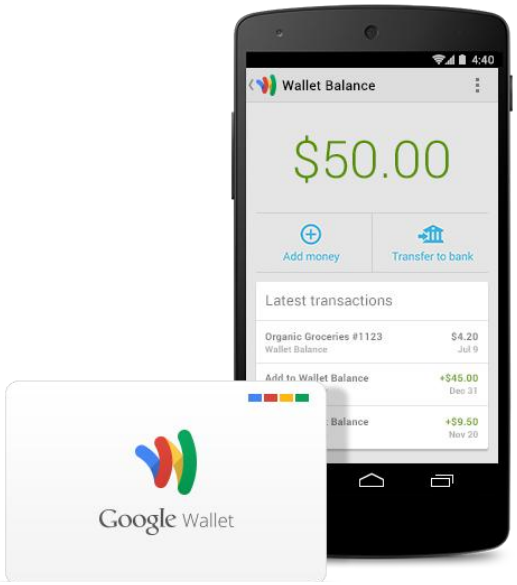


Figure 4.02 : *Google Wallet Card et application Google Wallet*

4.2.2 Matériels

4.2.2.1 Arduino

Arduino sera utilisé pour servir de lecteur de carte RFID.

Arduino est une simple carte électronique, open source, de petit format, supportant un microcontrôleur entouré de minimum de composants nécessaires à son fonctionnement (quartz, condensateur, etc.). Cette carte supporte sur sa périphérie une rangée de connecteurs dans lesquels peuvent s'enficher des cartes d'interface appelées « shield » et elle est équipée en plus d'un connecteur USB permettant de la raccorder à un PC pour pouvoir écrire le programme destiné à la piloter. [28]

Arduino existe en plusieurs versions et on utilisera la version UNO. Arduino seul ne pourra servir de lecteur de carte RFID, il est nécessaire d'y ajouter un shield RFID. Notre choix s'est porté sur le MFRC522.

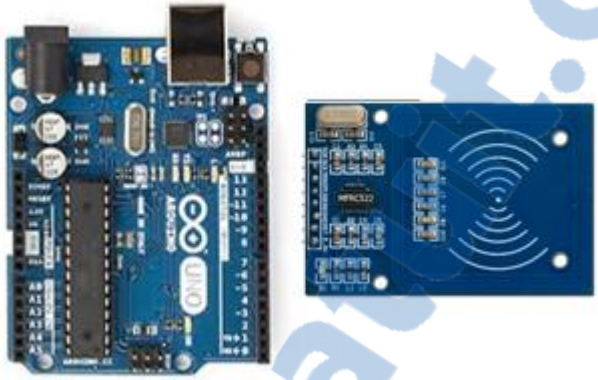


Figure 4.03 : *Arduino UNO et le MFRC522*

4.2.2.2 Carte à puce

Le type de carte à puce utilisé dans notre projet est la carte à puce sans contact MIFARE S50. Cette carte est munie d'une micro puce permettant de stocker des informations et qui produit une action lorsqu'elle est dans le champ d'action d'un lecteur de carte.

Figure 4.04 : *La carte à puce sans contact RFID*

4.2.2.3 Ordinateurs

Deux ordinateurs sont utilisés. L'un, doté d'un système d'exploitation Linux, est utilisé comme serveur de base de données, et l'autre, doté d'un système d'exploitation Windows, sert de station de développement. Ce dernier est aussi utilisé pour héberger et exécuter l'application.
Les caractéristiques de chacun de ces ordinateurs sont détaillées dans le tableau ci-dessous :

	Ordinateur 1	Ordinateur 2
OS	Debian	Windows XP
Processeur	AMD A8-6500 4 x 3.5MHz	Pentium (R) Dual Core CPU E5800 @ 3.20 GHz
RAM	8 GB	2 GB
Disque dur	1 TB	500 GB

Tableau 4.01: *Caractéristiques techniques des PC utilisés lors du projet*

4.2.3 Logiciels

4.2.3.1 NetBeans

L'application qui fait office d'IHM (Interface Homme Machine), sera développée en Java. Pour la programmation, nous avons décidé d'utiliser NetBeans.
NetBeans IDE est un logiciel de développement open source pour le développement de programmes sur Java, C, C++, PHP, JavaScript, etc. Conçu en Java, Netbeans est disponible sous Windows, Linux, Mac OS X ou sous une version indépendante des systèmes d'exploitation requérant une machine virtuelle Java. L'environnement fournit aux développeurs les outils nécessaires pour créer des applications d'internet professionnelles, de bureau, mobile, etc. Un JDK (Java Development Kit) est requis pour les développements en Java.

4.2.3.2 JMerise

JMerise est un logiciel gratuit dédié à la modélisation des modèles conceptuels de données pour Merise. Il génére automatiquement le modèle physique de données et les scripts SQL pour différents systèmes de gestion de base de données.

4.2.3.3 Mysql

MySQL est un SGBDR (Système de Gestion de Bases de Données Relationnelles), c'est-à-dire un logiciel qui permet de gérer des bases de données, et donc de gérer de grosses quantités d'informations, qui utilise le langage SQL. C'est l'un des SGBDR les plus utilisés.

4.2.4 Langages informatiques

4.2.4.1 Java

Le langage Java est un langage de programmation informatique orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au SunWorld. Java est un ensemble de classes et d'interfaces défini par Sun et les acteurs du domaine des bases de données. L'idée de départ de Java était de développer un langage avec lequel on puisse développer les logiciels pour l'électronique grand public, tel que PDA, lecteurs CD-ROM, etc.
Le choix de ce langage est dû aux multiples avantages tel que :

- La simplicité : Java est un langage simple.
- La portabilité : Java est disponible sur de multiples plateformes. Cela inclut tous les systèmes d'exploitation d'ordinateurs ainsi que les serveurs de type Unix et Windows.
- La gratuité : la machine virtuelle Java est à la portée de tout le monde ; elle est gratuite. En outre, de multitudes API (Application Programming Interface) sont dédiées à Java tout en étant de même gratuites.
- L'orienté objet : il très est utile pour le développement d'une application car il permet la réutilisation des objets entre les différents services. [29] [30]

4.2.4.2 SQL

SQL est un langage informatique normalisé servant à exploiter des bases de données relationnelles. La partie langage de manipulation de données de SQL permet de rechercher, d'ajouter, de modifier ou de supprimer des données dans les bases de données relationnelles.

4.2.4.3 Langage Arduino

Le langage Arduino est basé sur les langages C/C++. C'est un véritable métalangage orienté pour la programmation microcontrôleur qui offre des fonctions de syntaxe très simple mais très

puissantes. La plupart des librairies utiles sont également disponibles pour la communication série avec le PC, l'utilisation d'afficheur LCD standard, de servomoteurs ou encore de moteurs pas-à-pas.

4.3 **Conception**

Un système d'information (SI) est l'ensemble des moyens humains, matériels et immatériels mis en œuvre afin de gérer l'information au sein d'une organisation ou d'une entreprise. Un système d'information possède quatre fonctions essentielles :

- la collecte d'information
- la mémorisation de l'information
- le traitement des données stockées
- la diffusion de l'information vers les autres éléments du système ou vers l'environnement extérieur au système

Dans tout SI, la modélisation conceptuelle des données est une phase très importante. Il s'agit de la phase d'analyse du système d'information dont la principale finalité est de déterminer le futur contenu de la base de données. Dans ce contexte, les méthodes de conception des systèmes d'information impliquent la construction de modèles conceptuels et de traitements de données. La construction de ces modèles se fait en utilisant des formalismes divers. Cette phase de conception nécessite l'utilisation de méthode permettant d'obtenir un modèle sur lequel on va s'appuyer. Il existe plusieurs méthodes d'analyse évolués et puissantes dont la méthode MERISE.

4.3.1 Présentation de MERISE

MERISE (Méthode d'Etude et de Réalisation Informatique pour les Systèmes d'Entreprise) est une méthode de conception, de développement et de réalisation de projets informatiques. Le but de cette méthode est d'arriver à concevoir un système d'information. La méthode MERISE est basée sur le principe de séparation des données et des traitements.

La conception d'un système d'information se fait par étapes, afin d'aboutir à un système d'information fonctionnel reflétant une réalité physique. Cette succession d'étapes est appelée cycle d'abstraction. Il se décompose en trois couches : conceptuelle, logique et physique, chacune correspondant à une modélisation des données et des traitements.

4.3.2 Modèle conceptuel de données

Le modèle conceptuel de données (MCD) a pour objectif d'identifier et de décrire les données utilisées par le SI. Il définit également les relations entre ces données. La construction de ce modèle nécessite la connaissance des différents détails se rapportant au système envisagé. Pour aboutir au MCD, il est nécessaire de déterminer :

- les différentes entités entrant en jeu dans le système
- les relations qui existent entre ces entités et les cardinalités associées
- les propriétés de chaque entité

Ainsi, le MCD établi pour notre base de données est le suivant :

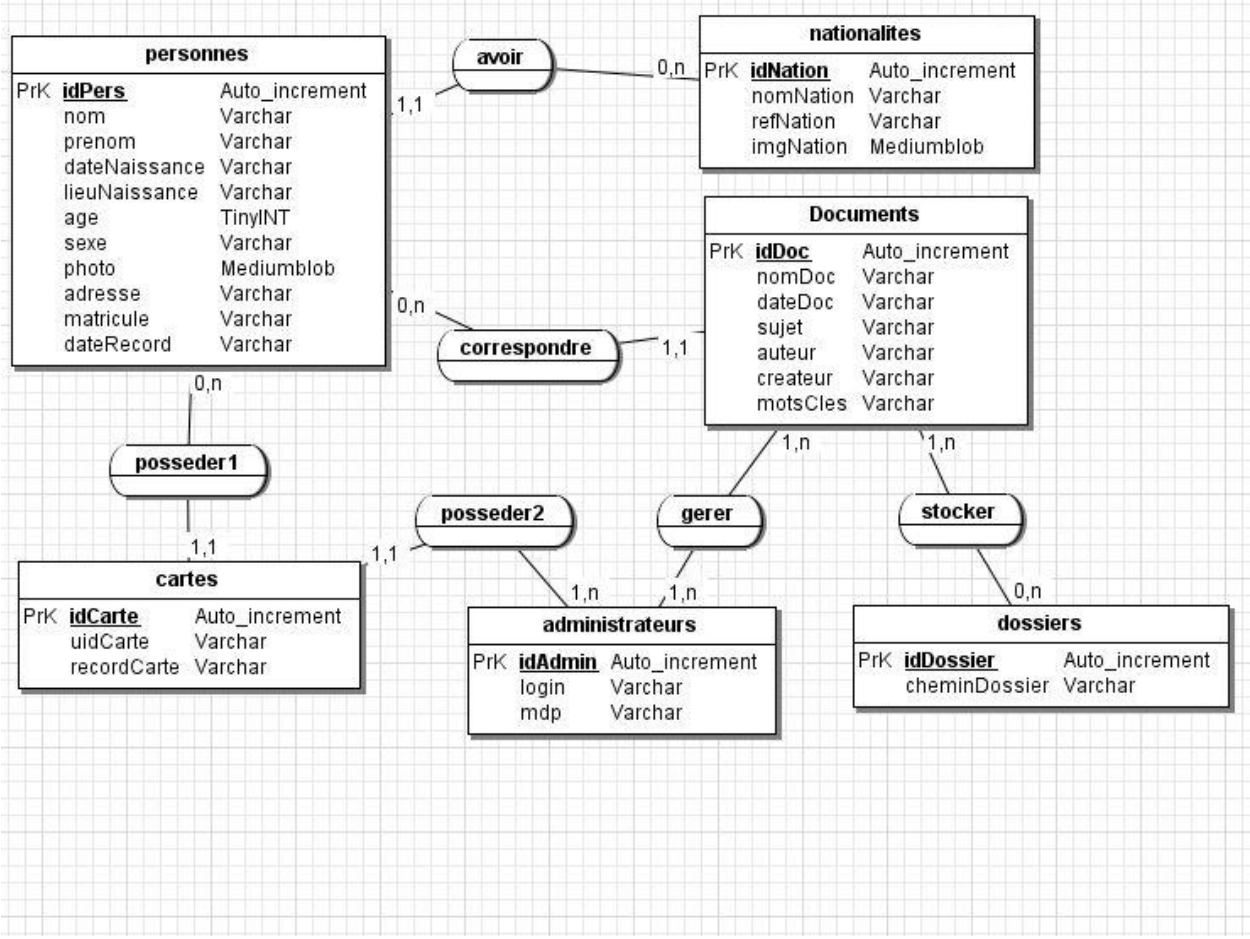


Figure 4.05 : *MCD de la base de données*

Le MCD a ses limites. Il ne connaît pas la notion de table, tandis qu'une base de données, constituée par un ensemble de tables, ne connaît pas le concept des entités reliées entre elles par des relations portant des cardinalités. Pour cela, il existe un autre modèle, le modèle logique des données (MLD), qui utilise le formalisme des tables logiques.

4.3.3 Modèle logique de données

Le MLD représente les informations du MCD à l'aide d'un formalisme différent qui est adapté aux structures d'une base de données. Le MLD s'obtient par application des règles de passage du MCD au MLD :

- les entités deviennent des tables.
- l'identifiant d'une entité devient la clé primaire de la table associée à cette entité.
- les propriétés d'une entité deviennent des attributs de la table.
- dans le cas de l'association (0,1) ou (1,1) à (0, n) ou (1, n) :

– L'entité qui est du côté de la cardinalité (0,1) ou (1,1) reçoit comme attribut l'identifiant de l'autre entité.

– Les propriétés de l'association deviennent des attributs de l'entité qui est du côté de la cardinalité (0,1) ou (1,1).

- dans le cas de l'association (0, n) ou (1, n) à (0, n) ou (1, n) :

– L'association devient une table

– Les identifiants des entités participant à l'association forment ensemble la clé de la table issue de l'association.

– Les propriétés de l'association deviennent les attributs de la table issue de l'association.

En appliquant ces règles, on obtient le MLD suivant :

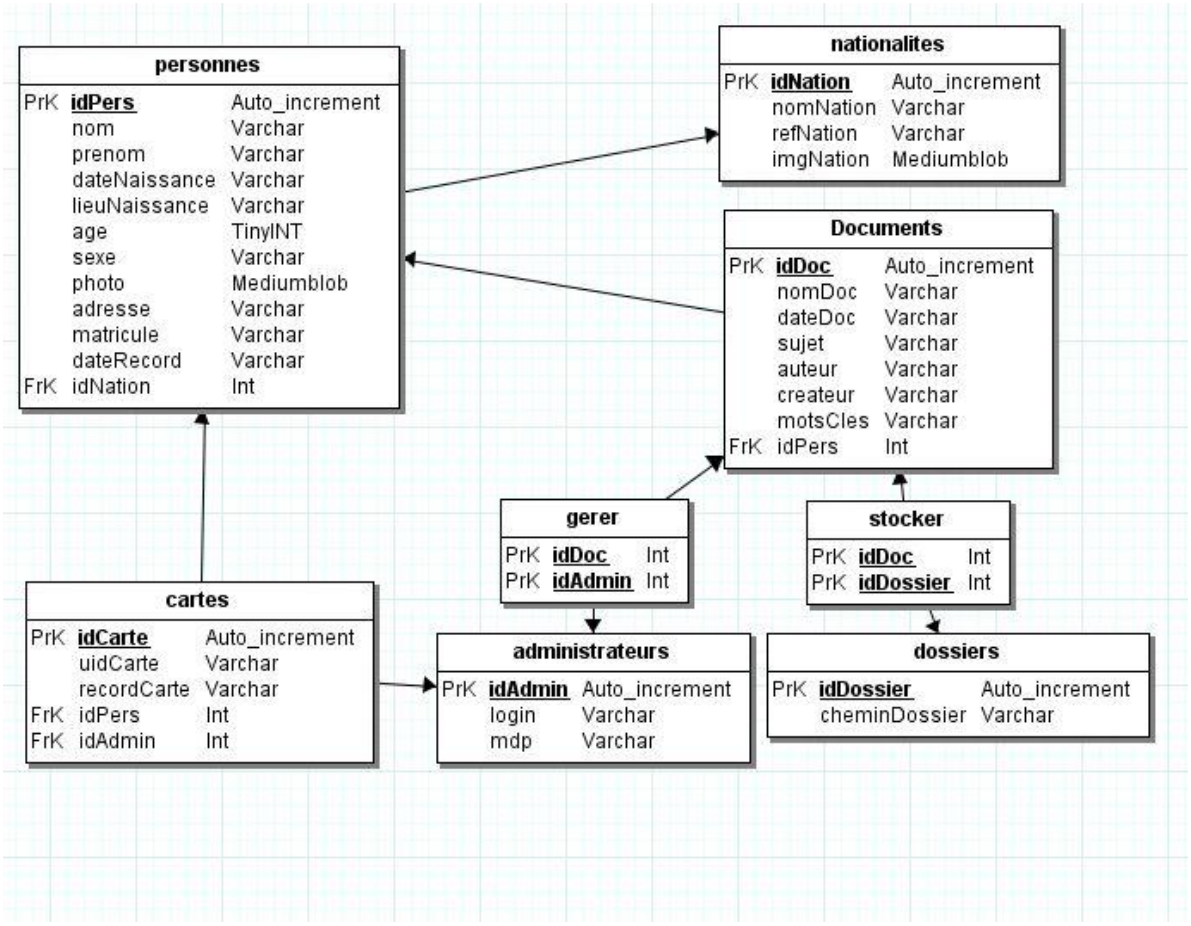


Figure 4.06 : *MLD établi à partir du MCD*

4.3.4 Modèle physique de données

Le modèle physique de données (MPD) est la traduction du MLD dans une structure de données spécifique au système de gestion de bases de données (SGBD) utilisé. Le langage de définition de données généralement utilisé étant le SQL, il s'agit donc de la traduction du MLD en script SQL.

4.4 Réalisation

Cette partie est consacrée à la réalisation de l'application et présente les différentes fonctionnalités qui ont été développées et testées.

4.4.1 Présentation générale de l'application

Notre application porte le nom de « Smart Identity » (Identité intelligente). Elle constitue un système basé sur une architecture client/serveur. Elle est développée en Java et est caractérisée par sa portabilité, dans le sens où elle s'adapte aux différents systèmes d'exploitation autre que

Windows à condition que ceux-ci soient équipés de la machine virtuelle Java. Elle tient son nom du fait que les documents d'identité numériques générés soient intelligents : ils sont classés automatiquement sans l'intervention de l'utilisateur en exploitant les métadonnées qui y sont incorporées ; ces dernières sont elles-mêmes générées automatiquement.

Les cartes d'identité numériques constituent, elles aussi, des objets intelligents. Elles peuvent servir à de multiples applications : la clé d'accès à notre application en est une ; nous assistons ainsi à un niveau d'authentification élevé combinant l'utilisation classique des mots de passe et l'utilisation de la carte. Elles peuvent aussi être utilisées, par exemple, pour l'accès à un local d'une entreprise.

L'identité est intelligente dans le sens où elle va conduire à une révolution en termes de création et de disponibilité de services et entrainer un important changement dans notre façon d'agir sur notre environnement.

L'application est conçue pour collecter et traiter les données organisées suivant le MCD que nous avons établi : l'ensemble des informations est stocké dans une base de données unique, assurant ainsi la centralisation des données.

En lançant l'application, la fenêtre d'authentification est la première interface vue par l'utilisateur. L'authentification sert à restreindre l'accès à l'application.

La figure ci-dessous présente cette fenêtre. L'action demandée étant d'utiliser une carte et de saisir ensuite le mot de passe pour accéder à l'application.

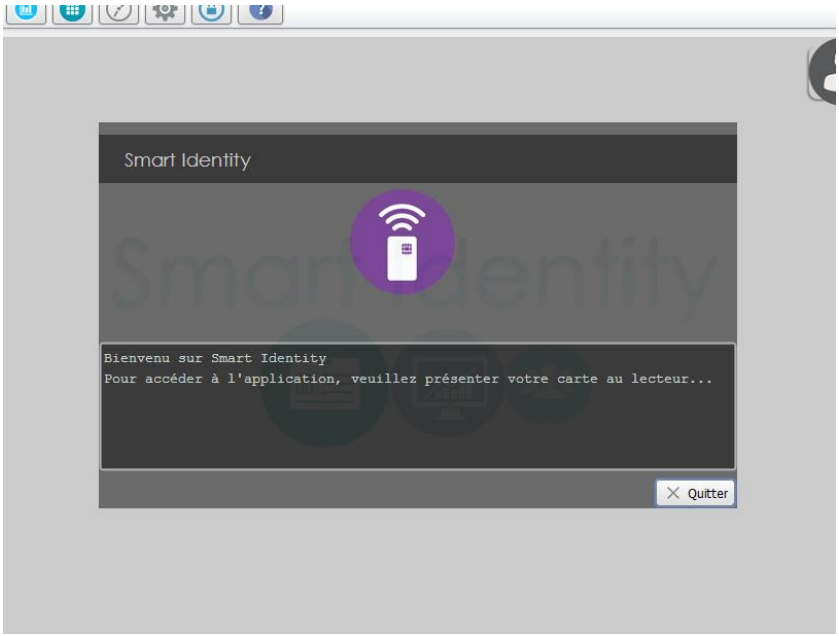


Figure 4.07 : *Fenêtre d'authentification de l'application*

Après l'authentification, on accède directement à la fenêtre principale : elle est composée d'une barre de menus, d'une barre d'outils, d'un espace de travail sur lequel se trouve une étiquette désignant le nom de l'administrateur et d'une horloge.

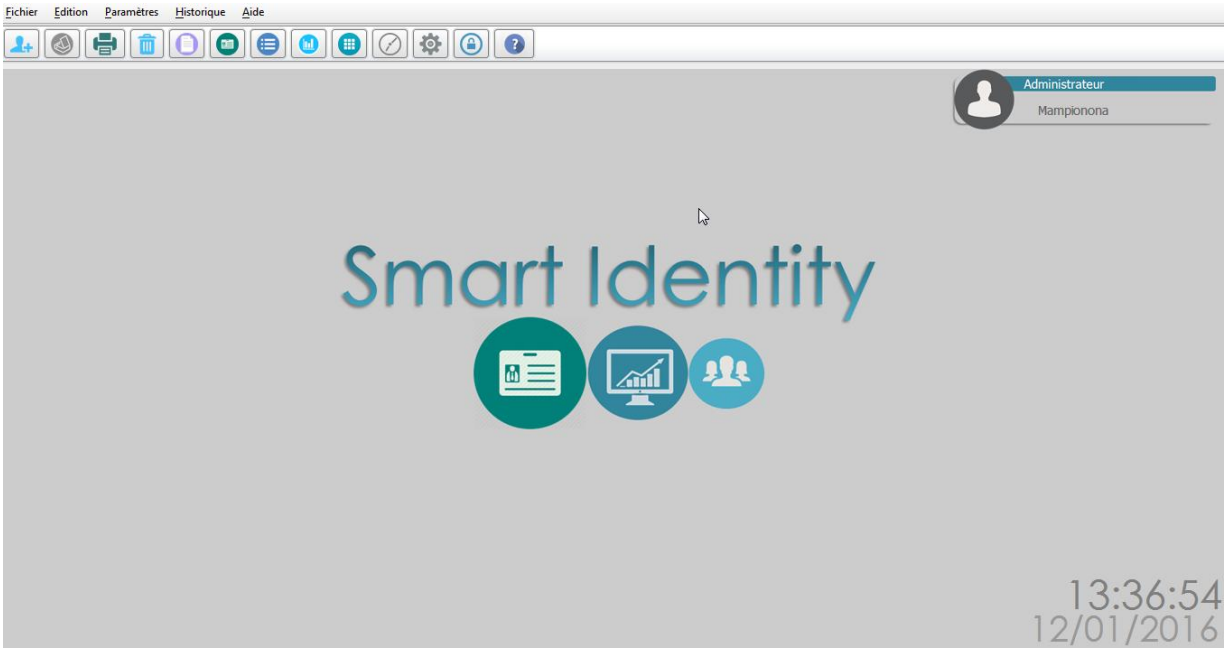


Figure 4.08 : *Fenêtre principale de l'application*

A partir de la fenêtre principale, l'utilisateur peut avoir accès aux différentes fonctionnalités offertes par l'application.

4.4.2 Fonctionnalités de base

Dans l'interface présentée ci-dessous, l'utilisateur peut configurer l'application en cliquant sur les options proposées :

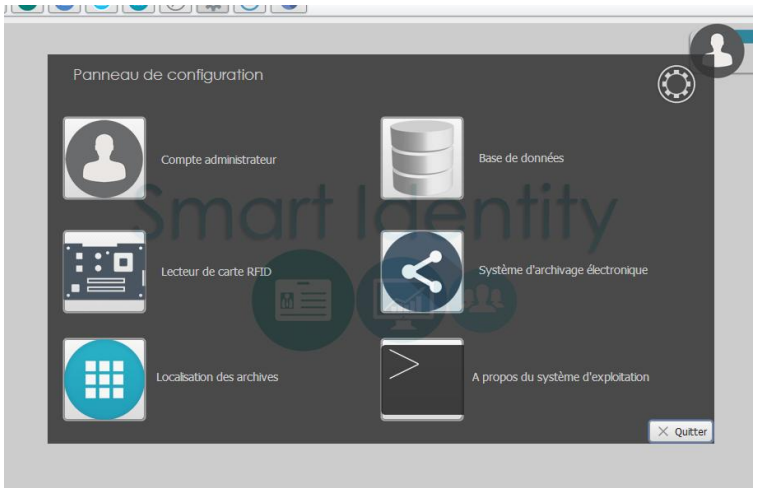


Figure 4.09 : *Panneau de configuration de l'application*

- Compte administrateur : permet de créer ou de modifier le login et/ou le mot de passe de l'administrateur.
- Base de données : permet de définir les paramètres indispensables pour la connexion à la base de données tels que l'adresse IP, le nom d'utilisateur et le mot de passe.
- Lecteur de carte RFID : permet de configurer les différents éléments nécessaires pour l'utilisation du lecteur de carte à puce RFID entre autres, le port de communication et la vitesse de communication.
- Système d'archivage électronique : dans cette option, il faut déterminer l'adresse IP de la machine sur laquelle est exécutée le SAE puis le port utilisé pour pouvoir effectuer un partage de documents.
- Localisation des archives : permet de paramétrer le chemin du répertoire où seront stockés les documents générés par l'administrateur.
- A propos du système d'exploitation : ne contient aucun élément configurable. Il ne fournit que des détails sur le système d'exploitation sur lequel est installée l'application.

Afin d'enregistrer les informations concernant une personne, on utilise l'interface ci-dessous. Après avoir rempli tous les champs, on valide les données et on les enregistre dans la base de données.

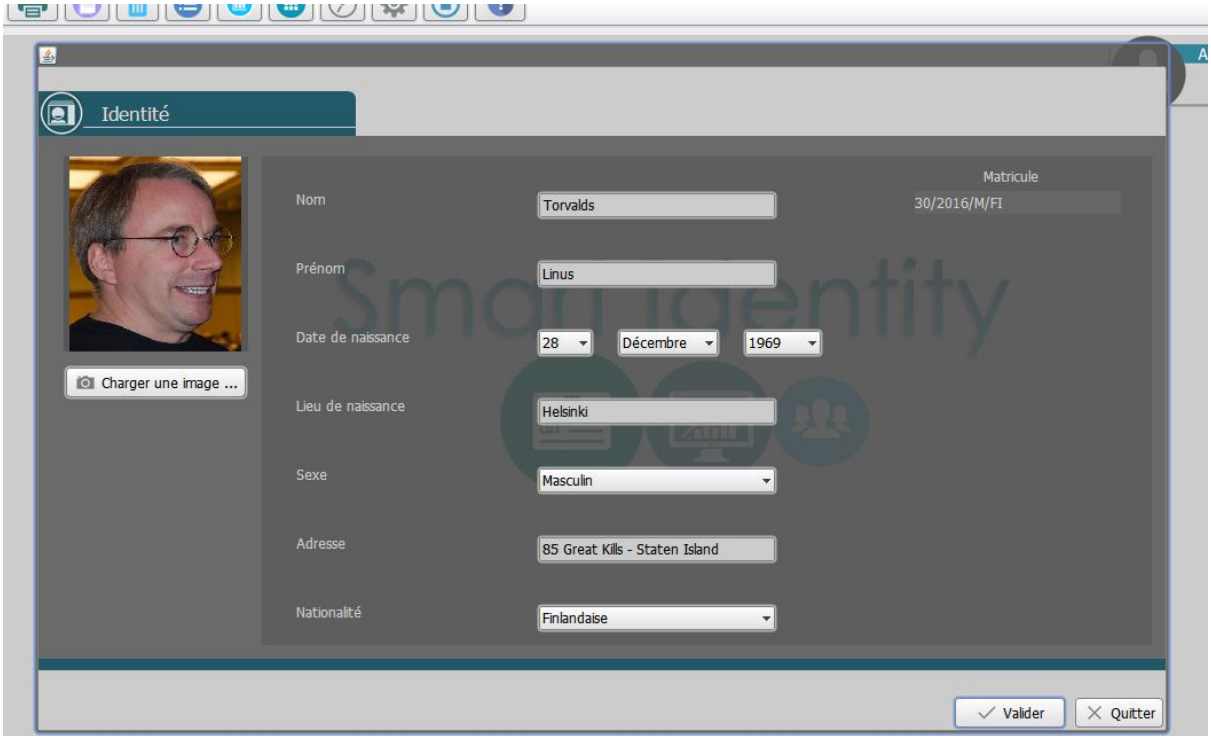


Figure 4.10 : *Interface permettant le recueil d'informations par saisie*

L'interface suivante peut être utilisée dans le cas où le recueil d'informations se fait à partir d'un document papier scanné. L'identité d'une personne est générée automatiquement suite à une reconnaissance de caractères effectuée sur un scan. Dans le cas où des erreurs sont produites dû à une imperfection du document numérisé, il est possible d'éditer les champs erronés. S'il est vraiment impossible de faire une reconnaissance de caractères, l'utilisateur devra recueillir les informations par saisie.

Figure 4.11 : *Interface permettant de générer une identité à partir d'un scan*

On peut afficher la liste de toutes les personnes enregistrées dans la base de données via l'interface de la figure ci-dessous. Il est possible de consulter les informations concernant une personne et cela, en cliquant sur la ligne correspondante du tableau. Dans le cas où la liste est encombrée, un champ de recherche est disponible afin de trouver une personne plus rapidement.

Cette interface offre plusieurs services à l'utilisateur :

- Création de document au format PDF et au format XML
- Possibilité de rayer l'identité d'une personne de la base de données
- Possibilité d'effectuer une impression s'il est vraiment nécessaire

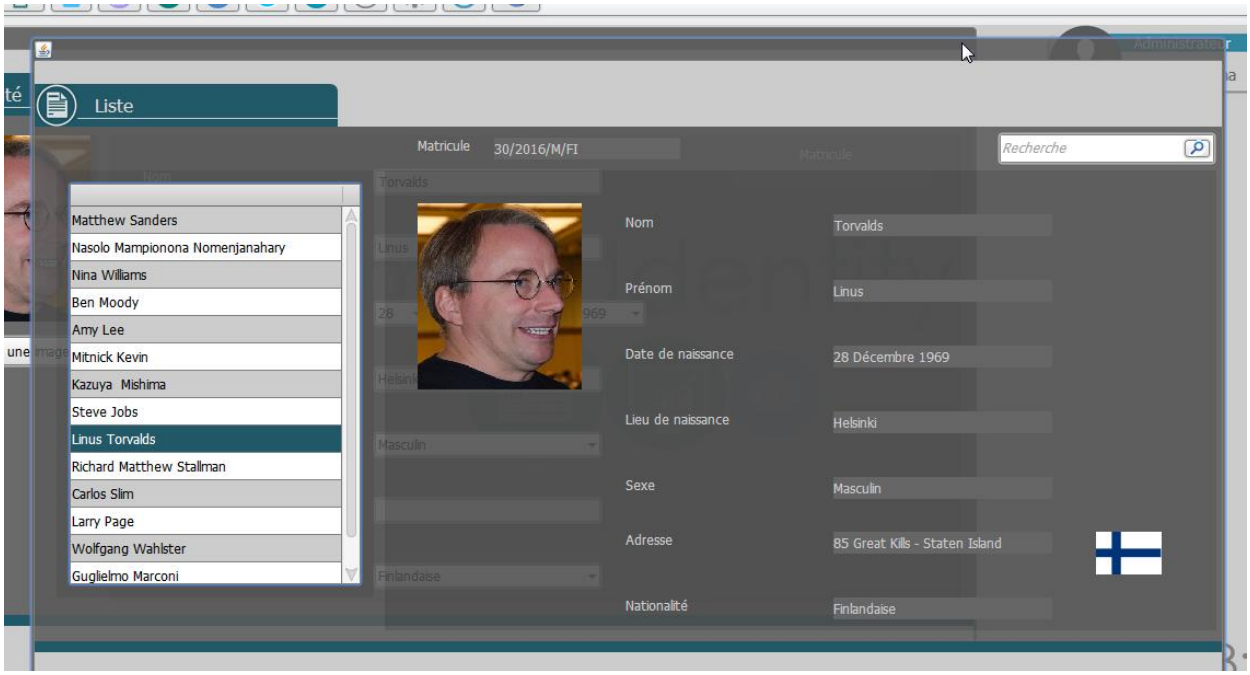


Figure 4.12 : *Interface : liste des personnes ajoutées*

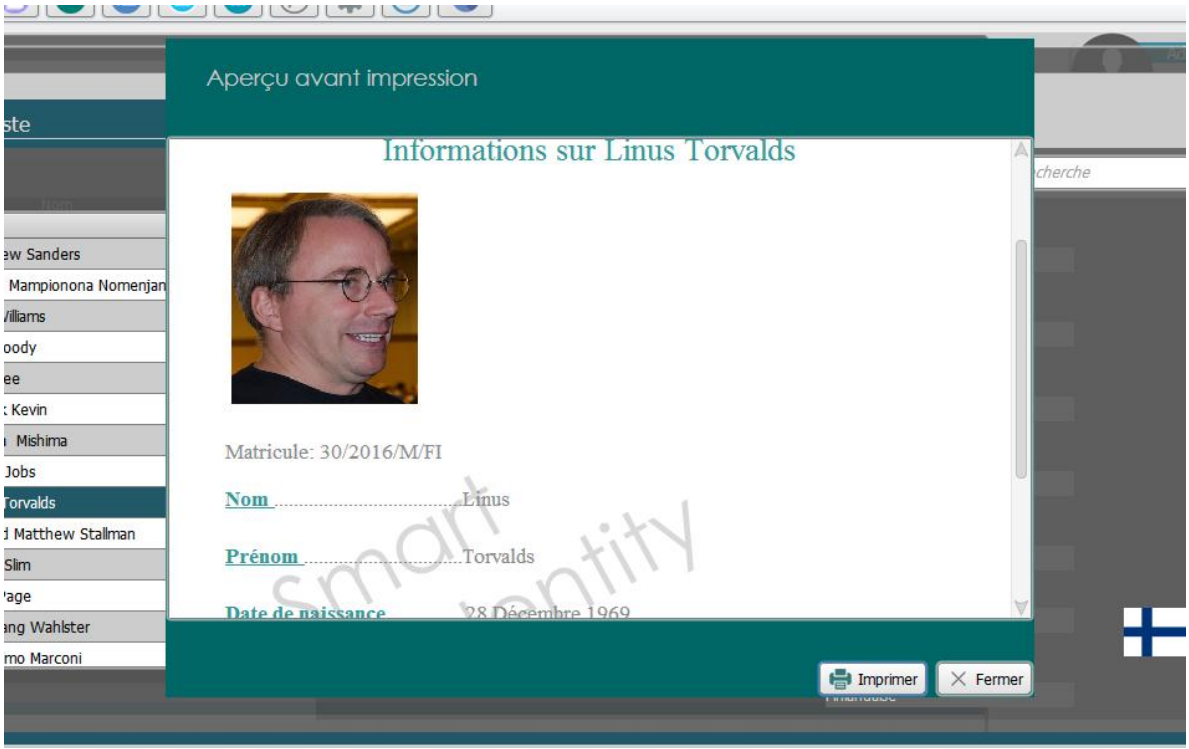


Figure 4.13 : *Fenêtre de visualisation pour une impression*

Les documents numériques créés au format PDF seront stockés sur le disque dur. Si l'utilisateur crée un document pour la première fois, il sera invité à spécifier le chemin vers lequel a lieu le stockage.

Dans le but d'assurer une pérennité et une intégrité des documents numériques générés, et en vue de back up, un fichier XML sera exporté, au travers d'un réseau, vers une application jouant le rôle de coffre-fort électronique (SAE) (**Figure 4.15**). Ce fichier XML est une source d'information permettant la génération d'un document numérique sécurisé au format PDF. Le SAE se présente sous forme d'une fenêtre principale qui contient un ensemble d'onglets permettant à l'utilisateur de naviguer entre les différents services offerts. L'application contient plusieurs interfaces dont la principale est l'interface de gestion des archives.

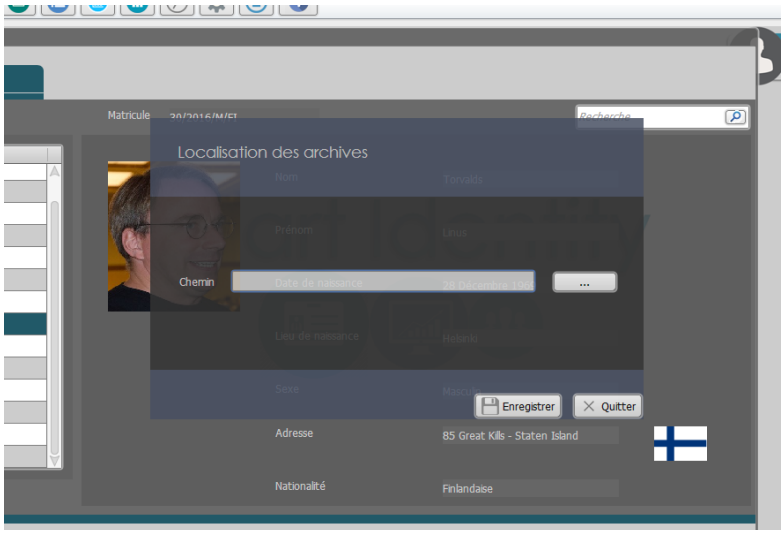


Figure 4.14 : *Une fenêtre permettant de paramétrer le chemin d'accès aux archives*

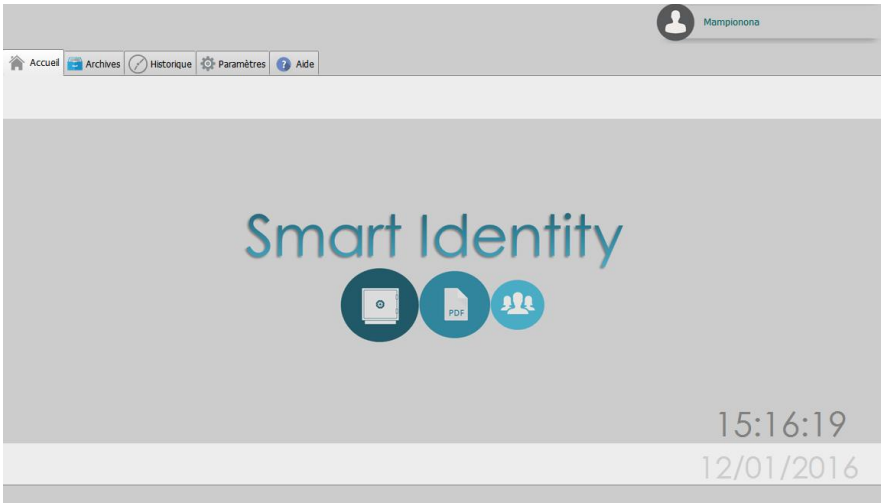


Figure 4.15 : *Interface d'accueil du SAE*

L'interface suivante affiche tous les documents créés par l'utilisateur. Celle-ci présente une arborescence permettant de les classer selon un plan de classement et une table affichant les détails sur chacun des documents créés (nom du document, taille, date de création, chemin d'accès).

Un champ de recherche est disponible pour effectuer une recherche rapide. La consultation du document est également possible via cette interface sous la condition qu'une application de lecture de fichier PDF est préinstallée sur la machine.

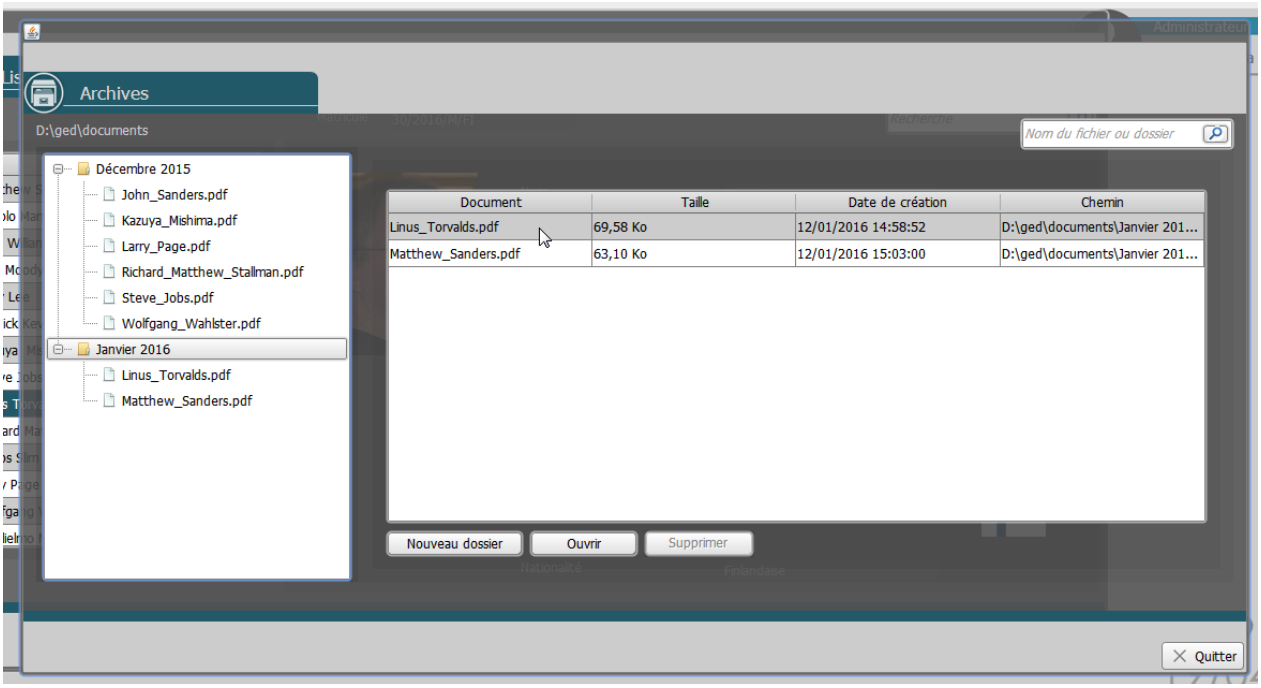


Figure 4.16 : *L'interface de GED*

La fenêtre suivante sert à gérer les cartes RFID. Elle est connectée à un lecteur RFID et permet de réaliser les fonctions lecture/écriture sur une carte présentée à proximité de celui-ci. Dans la partie supérieure, on retrouve des champs permettant de récupérer les données lors de la lecture d'une carte. La partie inférieure affiche la liste des porteurs et non porteurs de cartes et permet de faire une opération d'écriture sur la carte en sélectionnant une ligne du tableau.

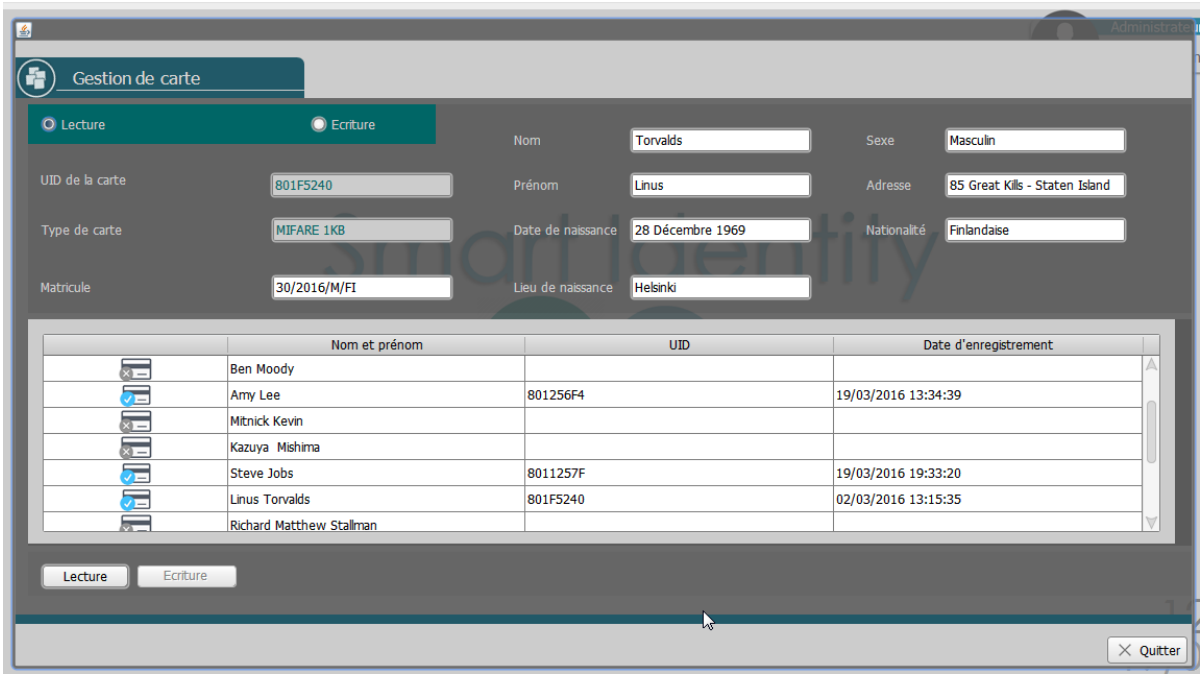


Figure 4.17 : *L'interface de gestion de carte*

Afin d'assurer une meilleure traçabilité des activités de l'utilisateur, un historique est mis à sa disposition. Il possède une vue détaillée des différentes actions entreprises qui sont enregistrées dans un fichier et classées par ordre chronologique.

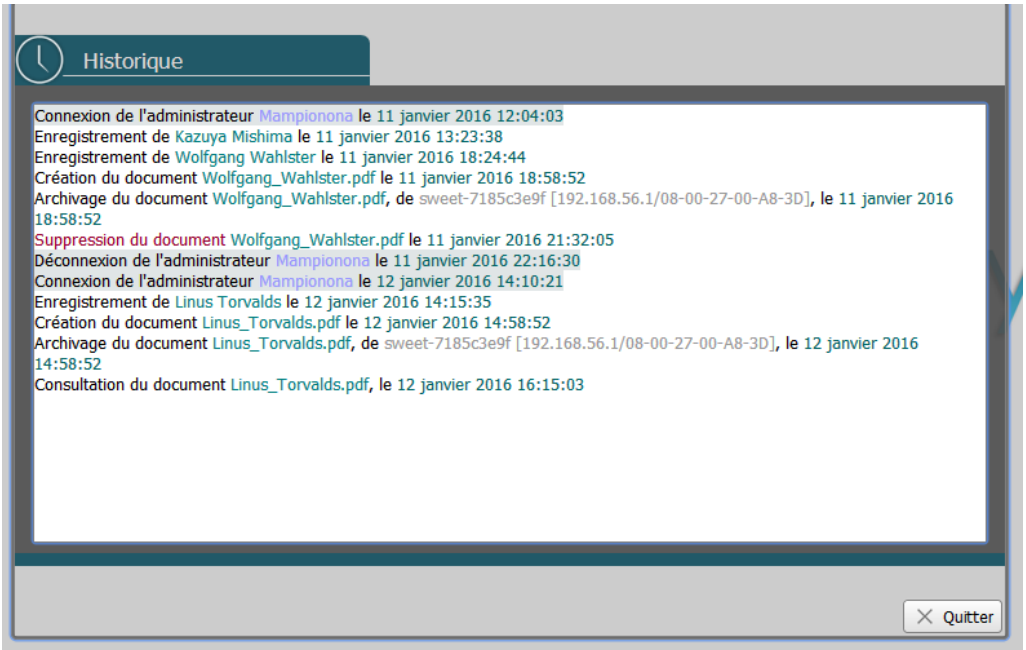


Figure 4.18 : *Historique des évènements*

4.4.3 Fonctionnalités supplémentaires

Lorsqu'il est difficile pour l'utilisateur de manipuler l'application une aide détaillée lui est fournie. L'application propose de même une aide en ligne. En cliquant sur le sous-menu « Aide en ligne », on sera redirigé vers un site web pour encore plus de détails.

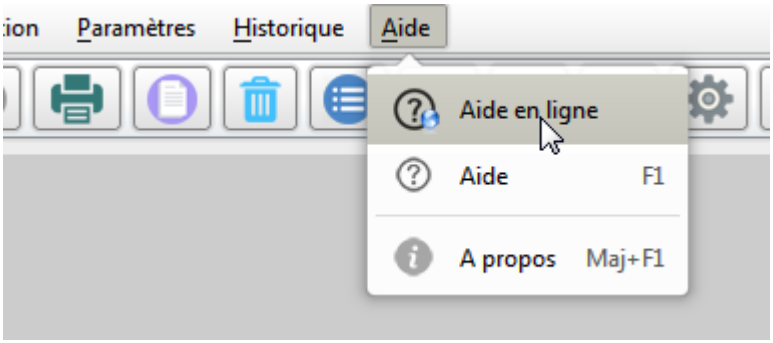
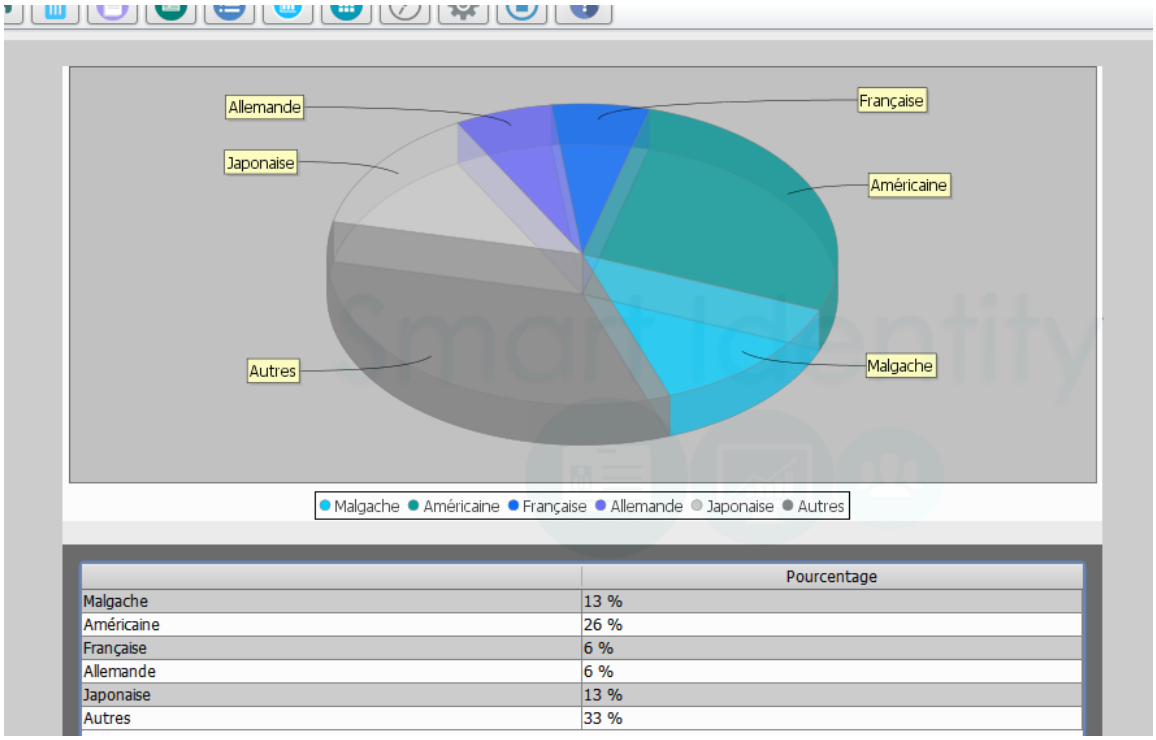


Figure 4.19 : *Sous-menu « Aide en ligne »*

Figure 4.20 : *Site web vers lequel pointe l'aide en ligne*

Une autre fonctionnalité supplémentaire est ajoutée à l'application : les statistiques. Elles constituent un outil incontournable au sein d'une organisation ou d'une entreprise. L'application intègre un outil statistique permettant de représenter les données plus facilement sous une forme graphique.



	Pourcentage
Malgache	13 %
Américaine	26 %
Française	6 %
Allemande	6 %
Japonaise	13 %
Autres	33 %

Figure 4.21 : *Exemple de statistique fournie par l'application*

4.5 Conclusion

Le présent chapitre est une partie déterminante axée sur la réalisation de notre projet. C'est une partie d'études et de conception de l'application. Nous avons décrit en premier lieu les différents besoins auxquels l'application devra répondre ainsi que l'objectif du projet. En second lieu, les différents outils matériels et logiciels ainsi que les langages utilisés pour le développement ont été détaillés. Nous sommes passés ensuite à la conception de la base de données pour finir par une présentation de quelques interfaces décrivant les fonctionnalités attendues de l'application. Après avoir terminé l'intégralité des tests qui se sont déroulés avec succès, nous pouvons affirmer que l'application que nous avons développé fonctionne correctement et est capable de satisfaire la totalité des besoins requis.

CONCLUSION GENERALE

Dans ce mémoire, nous nous sommes intéressés à la notion de dématérialisation, à la technologie RFID et aux cartes à puce. L'objectif de ce mémoire étant de développer une application pour la dématérialisation des documents d'identité, nous nous sommes focalisés sur les deux éléments clés intervenant dans la dématérialisation : la GED et le SAE. Ces deux notions sont en général axées sur la gestion des documents numériques, le cycle de vie de ces derniers a été étudié en détails.

Ensuite, nous avons étudiés la technologie RFID qui est connue aujourd'hui comme la nouvelle tendance en matière d'identification et d'authentification d'objets ou de personnes. Elle se décline en une multitude de technologies différentes, avec divers standards et caractéristiques physiques, dont la technologie NFC. Celle-ci se retrouve dans de nombreuses applications dû à ses caractéristiques particulières.

Par la suite, nous avons étudié les cartes à puce qui sont le fruit d'une véritable évolution du numérique et qui ont de multiples applications, à tel point qu'elles sont devenues omniprésentes dans notre vie quotidienne. Avec ce déploiement à grande échelle et les capacités offertes par la puce électronique, il est difficile de s'en passer lorsqu'on parle de dématérialisation de carte d'identité. Cette technologie est dotée de mémoires informatiques voire de microprocesseur lui permettant de se comporter comme un ordinateur. De ce fait, elle convient parfaitement comme moyen d'identification personnelle. En outre, la technologie RFID, plus précisément la NFC, a permis d'orienter la donne vers les cartes à puce sans contact.

Enfin, nous avons abordé la phase de conception et de réalisation de l'application. Nous avons identifié les différents besoins requis et recensé la totalité des outils utilisés. La phase de conception s'est portée sur la création de la base de données utilisée par notre application. La programmation des interfaces utilisateur a été ensuite entamée. Finalement, une série de tests a été effectuée pour s'assurer du bon fonctionnement des différentes fonctionnalités attendues de notre application. Celle-ci permettra d'une part, de gérer les documents numériques d'identité du côté de l'administration et d'autre part, de fournir une pièce d'identité numérique destinée aux porteurs.

Ainsi, le présent mémoire nous a permis d'exploiter les points forts de diverses technologies de télécommunication et d'informatique afin de permettre à toute organisation ou organisme de dématérialiser ses supports « papier » d'identité.

ANNEXE 1

PDF A/1

PDF A/1 est une version standardisée ISO du PDF, un format propriétaire documenté mis au point par la société Adobe Systems. Son usage est très répandu pour conserver et échanger des documents numériques.

Le principal avantage de ce format est que les fichiers au format PDF/A-1 sont fidèles aux documents originaux : les polices, les images, les objets graphiques et la mise en forme du fichier source sont préservés, quelles que soient l'application et la plate-forme utilisées pour le créer.

C'est donc une version restreinte du format PDF standard.

Les restrictions comportent :

- La non inclusion d'objet dynamique de type audio ou vidéo
- L'interdiction du lancement de code script ou de fichiers exécutables
- L'inclusion de toutes les polices de caractères
- L'interdiction du chiffrement
- L'utilisation obligatoire de métadonnées

Les principales utilisations sont : la GED et le SAE.

ANNEXE 2

CONFIGURATION DU SERVEUR MYSQL SOUS LINUX

Linux est un système d'exploitation comme Windows ou Mac OS X. A la différence de ces derniers, il est libre, c'est à dire que les utilisateurs sont libres de l'utiliser, le modifier et le redistribuer. Différentes distributions de Linux ont été créées pour simplifier la vie des utilisateurs et leur permettre de faire un choix. Nous avons choisi la distribution Debian qui est l'une des distributions les plus populaires. [31]

MySQL est préinstallé sur la distribution Linux que nous avons utilisé. Pour un accès distant au serveur MySQL, les étapes suivantes ont été exécutées :

- Démarrage du serveur MySQL :

/etc/init.d/mysql start

- Modification du fichier my.cnf :

nano /etc/mysql/my.cnf

Le fichier contient une ligne où il faut insérer l'adresse IP du serveur :

bind-address = xxx . xxx. xxx. xxx

- Redémarrage du serveur :

/etc/init.d/mysql restart

- Création d'un utilisateur :

« root » est l'utilisateur par défaut dans MySQL. Il est nécessaire de créer un nouvel utilisateur. La commande permettant de réaliser cette tâche est la suivante :

grant all privileges on smart.* to 'user'@'%' identified by 'password' ;

- Ouverture des ports du firewall :

Il est nécessaire de pouvoir accéder au serveur MySQL à travers le firewall.

/sbin/iptables -a input -i eth0 -p tcp --destination-port 3306 -j accept

Cette commande ouvrira le port 3306 depuis toutes les machines.

ANNEXE 3

PROCEDURES STOCKEES

Les procédures stockées sont des morceaux de code SQL présents dans une base de données et qui peuvent être appelés via une requête SQL.

Les procédures stockées sont précompilées par le serveur, du coup on économise le temps nécessaire à l'analyse et au décodage d'une requête SQL normale. On économise les échanges d'information entre le client et le serveur, ce qui procure une réduction du trafic sur le réseau.

Les procédures stockées sont de deux types : les procédures qui ne retournent rien, et les fonctions, qui retournent une variable.

La syntaxe pour créer une procédure est relativement simple et se présente sous la forme suivante :

```
create procedure nom_de_la_procedure ([paramètres])
```

Une fonction comme une procédure s'exécute sur le serveur de base de données, mais une fonction retourne un résultat. Pour créer une fonction, on utilise la commande suivante :

```
create function nom_de_la_fonction ([paramètres]) returns type_de_retour
```

ANNEXE 4

MFRC 522

Le module utilisé dans notre projet est le Philips MFRC522. Il est monté sur une carte déjà câblée avec une antenne. Il permet la lecture sans contact des puces RFID, intégrées dans une carte, présentée à proximité.

Ses caractéristiques physiques sont détaillées ci-dessous :

- Tension de fonctionnement : 3.3V
- Courant maximale : 30mA
- Fréquence de fonctionnement : 13.56 MHz
- Distance de lecture/écriture : < 10 cm
- Type de communication : SPI
- Débit de transmission de données : 10 Mb/s
- Dimensions : 40 mm x 60 mm
- Température de fonctionnement : -20 à 80 °C

Le tableau ci-dessous montre le brochage du module RFID sur la carte Arduino UNO

Module RFID	Carte Arduino UNO
Vcc	3,3V
RST	Pin 9
GND	GND
MISO	Pin 12
MOSI	Pin 11
SCK	Pin 13
SS	Pin 10
IRQ	-

Tableau A4.1 : *Branchements à réaliser entre le module RFID et la carte Arduino UNO*

Le module MFRC522 utilise une interface SPI. Il s'agit d'un bus de donnée série synchrone qui opère en full duplex. Les circuits communiquent selon un schéma maître-esclave, où le maître s'occupe totalement de la communication. Plusieurs esclaves peuvent coexister sur un bus, la sélection du destinataire se fait par une ligne dédiée entre le maître et l'esclave appelée « Slave Select ».

ANNEXE 5

MIFARE S50

La MIFARE MF1 IC S50 est développée par NXP (anciennement Philips). C'est une carte à puce sans contact opérant avec un débit de transmission de données de 106Kb/s et permettant des échanges de données bien plus importantes. Elle n'est plus considérée comme un simple identifiant ou un système d'authentification quelconque, mais comme une mémoire stockant ses propres informations, à la manière d'un disque dur ou d'une clé USB.

Le fondeur de puces, NXP, a ainsi ajouté des fonctions de sécurité et d'anticollision dans la carte à puce sans contact, telles que :

- Authentification mutuelle carte/lecteur (impliquant de la cryptographie, des clés) ;
- Protection de la mémoire par clé read/write pour éviter le clonage d'une carte ;
- Encryption des transmissions lecteur/carte par mécanisme de clé de session pour éviter toute divulgation de données ;
- Algorithme d'anticollision pour ne lire qu'une carte à la fois.

Ses caractéristiques physiques sont détaillées ci-dessous :

- Capacité de stockage : 1KB
- Fréquence de fonctionnement : 13.56 MHz
- Distance de lecture/écriture : 2.5 à 10 cm
- Débit de transmission de données : 106 Kb/s
- Conservation de données : > 10 ans
- Dimensions : 85,5 mm x 54 mm x 0,80 mm ± 0.04 mm
- Matériau : PVC, waterproof
- Température de fonctionnement : -20 à 80°C
- Normes : ISO 14443, ISO 7816

La puce MIFARE S50 se compose d'une interface radiofréquence, d'une unité de commande numérique et d'une EEPROM de 1KB. L'énergie et les données sont transférées par l'intermédiaire d'une antenne constituée d'une bobine avec un petit nombre de spires, qui est directement reliée à la puce.

Les différents éléments constitutifs de la MIFARE S50 sont :

- Interface Radiofréquence : contient un modem (modulateur démodulateur) et un régulateur de tension.
- Anticollision : permet d'éviter les erreurs de collision engendrées par l'existence de plusieurs cartes dans le champ d'un lecteur.
- Authentication (Authentification) : précédant toute opération de la mémoire, la procédure d'authentification garantit l'accès à un bloc.
- Arithmetic Logic Unit (Unité arithmétique et logique) : effectue des calculs sur des valeurs stockées tel que l'incrémentation ou la décrémentation.
- EEPROM Interface : permet l'interaction entre l'EEPROM et les autres modules.
- Crypto unit (Unité cryptographique) : assure la sécurisation des transactions.
- EEPROM : contient les données.

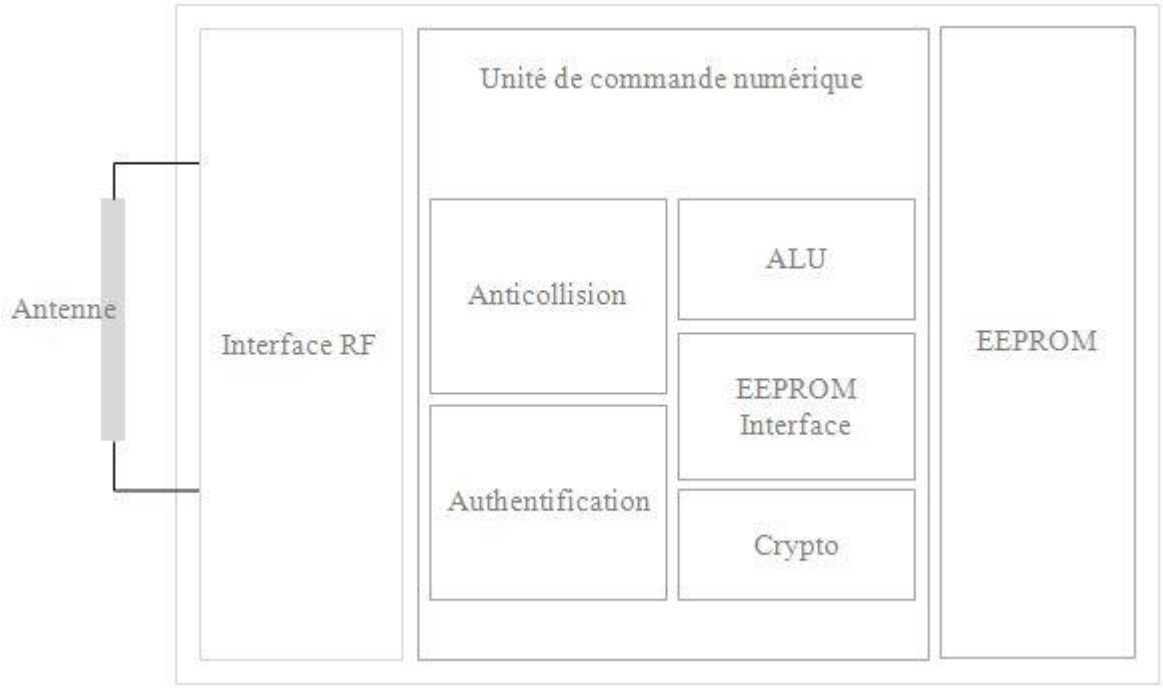


Figure A5.1 : *Architecture interne de la MIFARE S50*

L'EEPROM est organisée en 16 secteurs de 4 blocs chacun : 3 blocs de données (blocs 0 à 2) et 1 bloc de sécurité (bloc 3). Le bloc est le plus petit élément adressable et est codé sur 16 octets. [25]

- Bloc fabricant

Le bloc 0 du premier secteur (secteur 0) est appelé bloc fabricant. Il contient les données du fabricant et ne peut être écrit.

- Bloc de données

A l'exception du secteur 0, tous les secteurs contiennent 3 blocs de données pour la mémorisation des données.

- Bloc de sécurité ou bloc « Trailer »

C'est le dernier bloc de chaque secteur. Il contient : une clé secrète A codé sur 6 octets, des conditions d'accès pour chaque bloc sur 4 octets et une clé secrète B sur 6 octets.

Après authentification, l'une des opérations suivantes peut être exécutée :

- Ecriture de données : écrit les données dans un bloc
- Lecture de données : lit les données stockées dans un bloc
- Décrémentation : opération qui consiste à décrémenter la valeur du contenu d'un bloc et mémorise ensuite le résultat dans un registre de données
- Incrémentation : opération qui consiste à incrémenter la valeur du contenu d'un bloc et mémorise ensuite le résultat dans un registre données

ANNEXE 6

SOCKETS

Un socket est un point de terminaison d'une communication entre un client et un serveur en cours d'exécution sur un réseau donné. Trois informations essentielles sont utilisées dans le concept des sockets : l'adresse IP, le numéro de port et le protocole utilisé (TCP ou UDP).

Une adresse IP est une adresse permettant d'identifier une machine dans un réseau ; elle est souvent représentée sous la notation décimale pointée comme 127.0.0.1.

Le port est un nombre positif pouvant prendre une valeur de 0 à 65535.

TCP et UDP sont deux protocoles servant à échanger des paquets d'information entre deux machines en utilisant leur adresse IP et un numéro de port. [33]

Le schéma suivant présente les algorithmes de fonctionnement des serveurs et clients.

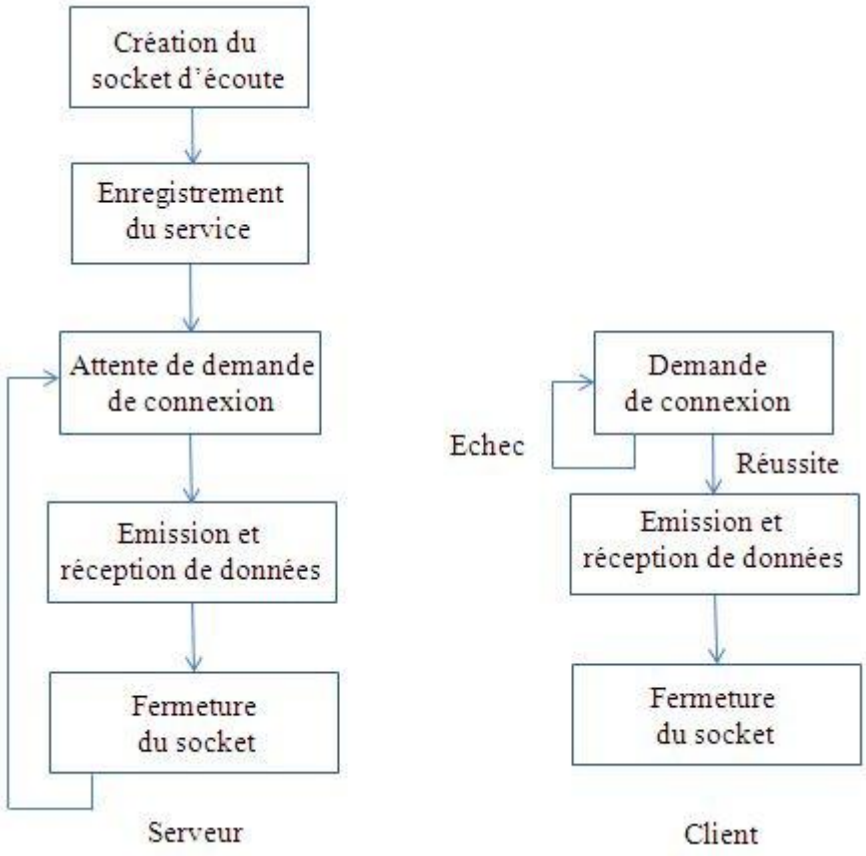


Figure A6.1 : *Organigrammes décrivant le fonctionnement des sockets serveur et client*

- Création du socket d'écoute par le serveur
- Le serveur enregistre son service sous un numéro de port, indiquant le nombre de clients qu'il pourra accepter.
- Il se met ensuite en attente d'une connexion de la part d'un client.
- Un client peut alors établir une connexion en demandant la création d'un socket à destination du serveur pour le port sur lequel le service a été enregistré.
- Le serveur accepte la demande de connexion du client.
- Le client et le serveur peuvent alors échanger les données
- .Après l'échange de données, il y a fermeture des sockets

Nous utilisons dans notre projet les sockets utilisant le protocole TCP.

ANNEXE 7
PROGRAMMATION DE LA CARTE ARDUINO

La programmation d'une carte Arduino nécessite un environnement de développement qui lui est associée. La programmation se fait en utilisant un langage proche du C. Une fois le programme achevé, il sera transféré et mémorisé dans la carte Arduino à travers la liaison USB. La communication entre la carte Arduino et l'ordinateur est une communication série et utilise la librairie Serial. Afin de communiquer avec le module MFRC522, il est nécessaire d'utiliser une bibliothèque dédiée : la « SPI.h ». Elle permet de communiquer avec des périphériques SPI. [32]
La lecture ou l'écriture de données sur la carte RFID (MIFARE S50) se fait à l'aide de la librairie « MFRC522.h ». La figure ci-dessous représente un organigramme qui explique le déroulement des différentes séquences lors d'une opération effectuée sur la carte RFID :

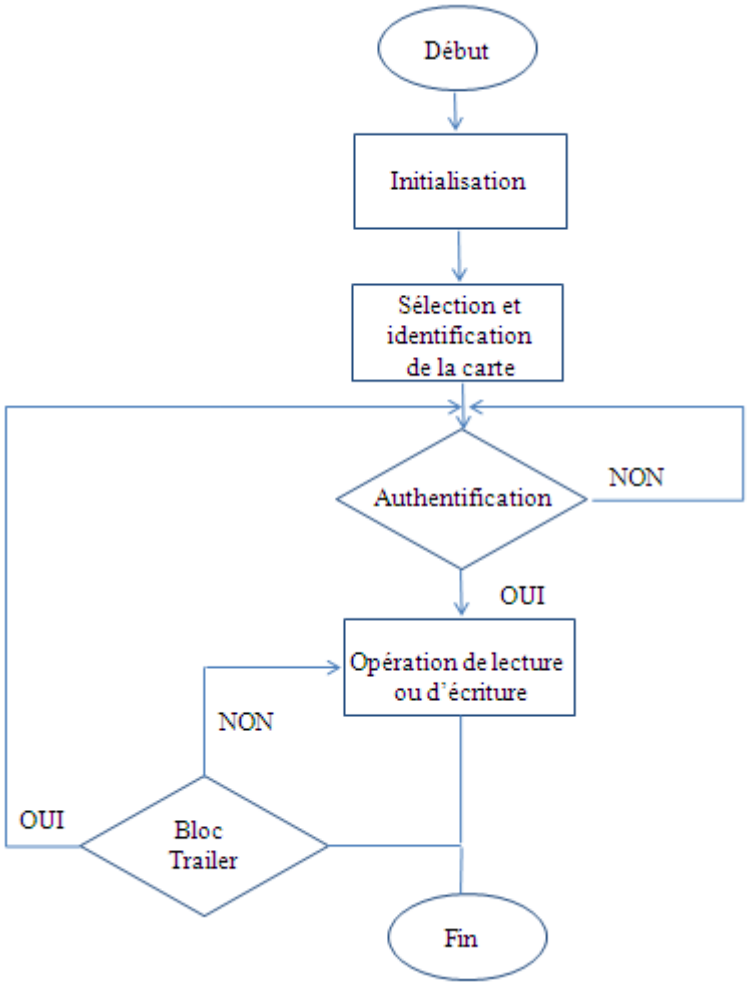


Figure A7.1 : *Organigramme d'une opération effectuée sur la carte RFID*

BIBLIOGRAPHIE

[1] « *Dématérialisation* », *fr.wikipedia.org/wiki/Dématérialisation*, Février 2016

[2] « *GED* », *www.commentcamarche.net/contents/319-ged-gestion-electronique-de-documents*, Avril 2016

[3] ADDPI, « *La maîtrise du flux documentaire* », Janvier 2011, Livre blanc

[4] J.M. Rietsch, M.A.Chabin, E. Caprioli, « *Dématérialisation et archivage électronique : Mise en oeuvre de l'ILM (Information Lifecycle Management)* », Dunod, Décembre 2006

[5] « *CCITT Group 4*», *fileformats.archiveteam.org/wiki/CCITT_Group_4*, Mars 2016

[6] F. Pelletier, « *La GED : générateur de gains à tous les niveaux* », MOS, 1998

[7] « *OCR ? ICR ? IWR ?* », *www.thecrowleycompany.com/ocr-icr-iwr-omg-get-scanned-text/*, Avril 2016

[8] « *Form processing, data capture,…*», *www.cmssoft.co.uk/pages/form_processing.html*, Avril 2016

[9] G. Desbetes, L. Leroy, A.G. Liebert, « *La Gestion électronique des documents : Typologie des systèmes d'information* », Université de Lille, Mars 2008

[10] « *Librairie de sauvegarde* », *fr.wikipedia.org/wiki/Librairie_de_sauvegarde*, Mars 2016

[11] M. Serlet, « *Etat de l'art de l'archivage électronique confronté à sa mise en pratique* », ENSSIB, Juin 2009

[12] S. Rohr, C. Bianchi, F. Chatelan, C. Guanzini, « *Manuel pratique de gestion des documents : Mettre en place les principes de Records management dans les communes vaudoises* », AVA, 2011

[13] E. Micaelli « *Système d'archivage électronique (SAE) : des exigences et des spécifications qui tiennent compte d'un environnement [GED-SAE(PAE)-PGA]* », Achivistes Expert, Mai 2012

[14] « *NFC et RFID* », *www.strategiestm.com/spip.php?page=print&id_article=3208*, Février 2016

[15] T. Igoe, D. Coleman, B. Jepson, « *Beginning NFC: Near Field Communication with Arduino, Android, and PhoneGap* », O'Reilly, Janvier 2014

[16] V. Coskun, K. Ok, B. Ozdenizci, *« Professional NFC Application Development for Android* », Wrox, Avril 2013

[17] E.P. Radonamandimby, « *Ondes radioélectriques* », ESPA Madagascar département Télécommunications, 2013-2014

[18] « *Onde radio* », *fr.wikipedia.org/wiki/Onde_radio*, Février 2016

[19] E. Conil, « *Propagation électromagnétique en milieu complexe : du champ proche au champ lointain* », Institut National Polytechnique de Grenoble, 2005

[20] D. Paret, « *RFID en ultra et super hautes fréquences UHF-SHF : théorie et mise en œuvre* », Dunod, 2008

[21] « *Communication en champ proche* », *fr.wikipedia.org/wiki/Communication_en_champ_proche*, Février 2016

[22] « *Qu'est-ce que la NFC ?* », *www.identivenfc.com/fr/what-is-nfc*, Février 2016

[23] « *Carte à puce* », *fr.wikipedia.org/wiki/Carte_à_puce*, Février 2016

[24] S. Bouzefrane, P. Paradinas, « *Les Cartes à puce* », Hermès, Septembre 2013

[25] C. Tavernier, « *Les Cartes à puce : Théorie et mise en œuvre* », Dunod, Mars 2011

[26] W. Rankel, W. Effing, « *Smart Card Hand Book* », Wiley, Juillet 2010

[27] A. Ratsimbazafy, « *Mémoires* et *Microprocesseur* », ESPA Madagascar département Télécommunications, 2012-2013

[28] C. Tavernier, « *Arduino : Maîtrisez sa programmation et ses cartes d'interface (shields)* », Dunod, Avril 2014

[29] L.E. Randriarijaona, « *Technique de programmation* », ESPA Madagascar département Télécommunications, 2012-2013

[30] L.E. Randriarijaona, « *Programmation orientée objet* », ESPA Madagascar département Télécommunications, 2013-2014

[31] N.M. Ravonimanantsoa, « *Unix et Linux* », ESPA Madagascar département Télécommunications, 2013-2014

[32] « *La librairie SPI* », *www.mon-club-elec.fr/pmwiki_reference_arduino/pmwiki.php?n=Main.LibrairieSPI*, Avril 2016

[33] K.L. Calvert, M.J. Donahoo, « *TCP/IP sockets in Java* », Elsevier, Février 2008

PAGE DE RENSEIGNEMENTS

Nom : NOMENJANAHARY

Prénoms : Nasolo Mampionona

Adresse : Lot AKT IB 20 Manjaka Vontovorona

Numéro de Téléphone : +261 33 82 515 74

E-mail : nmampionona@gmail.com

Titre du mémoire : « DEVELOPPEMENT D'UNE APPLICATION POUR LA DEMATERIALISATION DES DOCUMENTS D'IDENTITE »

Nombre de pages : 87

Nombre de tableaux : 10

Nombre de figures : 50

Directeur de mémoire :

Nom : RADONAMANDIMBY

Prénoms : Edmond Jean Pierre

Téléphone : +261 33 29 777 11

RÉSUMÉ

La dématérialisation est le remplacement du support papier par un support informatique à l'occasion de l'échange ou de la conservation des informations. Elle nécessite la mise en place d'une GED et/ou d'un SAE et induit de nouvelles habitudes de travail. La dématérialisation d'un document papier d'identité ne se limite pas à la production d'un document numérique d'identité. Elle fournit aussi une carte d'identité numérique nécessitant l'utilisation de la technologie RFID associée à celle des cartes à puce. Le développement d'une application informatique pour la dématérialisation des documents papier d'identité a été mis en œuvre afin de faciliter toute tâche administrative dans la gestion de ces documents. En outre, elle offre la possibilité de réduire les risques d'usurpation d'identité en pourvoyant une carte d'identité numérique servant de pièce justificative de l'identité d'un sujet.

Mots clés : Dématérialisation, RFID, cartes à puce.

ABSTRACT

Dematerialization is the replacement of paper by computer media on the occasion of the exchange or the storage of information. It requires the establishment of a EDM and/or ERMS and induces new work habits. Dematerialization of paper identity is not limited to the production of a digital identity document. It also provides a digital identity card that requires the use of RFID technology combined with that of smart cards. The development of a computer application for the dematerialization of documents paper identity has been implemented to facilitate any administrative task in managing these documents. In addition, it offers the possibility to reduce the risk of identity theft by providing a digital identity card serve as confirmation of the identity of a subject.

Keywords: Dematerialization, RFID, smart cards.