

**Université Assane Seck de Ziguinchor**  
**UFR Sciences et Technologies**  
**Département Informatique**



**Mémoire de fin d'études**

Pour l'obtention du diplôme de Master

Mention : Informatique

Spécialité : Génie logiciel

**La dématérialisation de l'état civil :  
La signature électronique**

**Présenté par :**

M. Serigne NDOUR

Soutenance le 03 Août 2024

**Sous la direction de :**

Pr. Ibrahima DIOP

**Membres du jury :**

- Pr. Youssou FAYE (**Président du jury**)
- Dr. El Hadji Malick NDOYE (**Rapporteur**)
- Pr. Youssou DIENG (**Examineur**)
- Pr. Ibrahima DIOP (**Encadreur**)

Année académique : 2023-2024



# RÉSUMÉ

La signature électronique de documents administratifs est devenue une pratique courante dans de nombreux pays en raison de sa commodité et de sa sécurité. Mais cette pratique est très peu utilisée au Sénégal. Et pourtant elle est reconnue par la législation du Sénégal au niveau de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques. En plus elle a beaucoup d'avantages pour tous les services administratifs comme l'état civil. Cette solution de signature électronique permettra aux municipalités d'offrir des services beaucoup plus efficaces. Et par conséquent permettre aux usagers de faire des demandes d'actes d'état civil en ligne.

La signature électronique utilise des techniques cryptographiques pour garantir que le document est authentique et n'a pas été modifié après la signature. Ainsi pour l'utilisation de cette solution de signature électronique l'État du Sénégal a mis en place une architecture de gestion de clés. Cette architecture est basée sur les certificats électroniques et les autorités de certification. Ainsi nous avons une identification de toutes les municipalités qui ont adoptés la signature électronique pour signer des actes d'état civil.

La signature électronique étant un moyen numérique d'authentifier et de valider des documents. Elle a la même fonction qu'une signature manuscrite. Ainsi pour parachever la dématérialisation de la procédure de demander d'un acte d'état civil en permettant à l'officier d'état civil de pouvoir signer un acte d'état civil sans pour autant l'imprimer et ensuite apposer une signature autographe. Nous avons développé un module de signature électronique pour signer les actes d'état civil au format numérique mais pour faire la vérification de l'acte électronique après sa signature.

# DÉDICACES

À mes défunts parents que leur âme repose en paix, ma famille aimante et dévouée, qui m'a soutenu tout au long de ce parcours académique. Votre encouragement constant et votre soutien inconditionnel m'ont donné la force de persévérer. Je vous dédie ce mémoire avec tout mon amour et ma gratitude.

À mes amis et camarades de classe, qui ont partagé cette aventure avec moi. Vos encouragements, nos discussions enrichissantes et notre soutien mutuel ont rendu ce parcours plus agréable. Cette dédicace est pour vous, mes chers amis.

À toutes les personnes qui ont participé à cette étude, je vous suis reconnaissant(e) de votre contribution précieuse. Votre participation a été essentielle pour la réalisation de ce mémoire.

# REMERCIEMENTS

Je tiens à remercier particulièrement **Pr. Ibrahima DIOP** pour le suivi de mon mémoire et toute l'aide qu'il a su m'apporter au cours de ce travail. J'ai eu le privilège de bénéficier de vos conseils et de votre savoir-faire. Votre sérieux, votre compétence et votre sens du devoir m'ont profondément marqué. Ce travail est pour moi l'occasion de vous témoigner ma profonde gratitude.

Veillez trouver ici l'expression de ma respectueuse considération et ma profonde admiration pour toutes vos qualités scientifiques et humaines.

Je remercie chaleureusement les membres de mon jury, pour avoir consacré une partie de leur temps afin de juger mon travail, **Pr. Youssou FAYE** pour avoir accepté de présider mon mémoire, **Pr. Youssou DIENG** pour avoir accepté d'être l'examineur de ce travail et **Dr. El Hadji Malick NDOYE** pour m'avoir fait l'honneur d'y participer.

Enfin je remercie à toutes les personnes qui ont participé à cette étude en tant que participants ou répondants.

# SOMMAIRE

RÉSUMÉ.....	i
DÉDICACES .....	ii
REMERCIEMENTS.....	iii
SOMMAIRE .....	iv
LISTE DES FIGURES.....	viii
LISTE DES SIGLES ET ABRÉVIATIONS .....	x
<b>Introduction .....</b>	<b>1</b>
<b>Chapitre 1 : Contexte du Mémoire.....</b>	<b>2</b>
<b>Introduction .....</b>	<b>2</b>
<b>I.    La gestion de l'état civil en papier .....</b>	<b>2</b>
<b>II.   L'archivage numérique des actes d'état civil en papier .....</b>	<b>3</b>
<b>III.  La dématérialisation partielle des procédures de l'état civil.....</b>	<b>4</b>
III.1  Les limites .....	4
III.1.1  La signature manuscrite.....	5
III.1.2  L'archivage papier.....	6
III.2  La dématérialisation des procédures et documents, la signature électronique.....	6
III.3  Les vulnérabilités de la signature numérisé et la signature numérique.....	7
<b>IV.   Problématique du sujet.....</b>	<b>7</b>
<b>V.    Objectifs .....</b>	<b>8</b>
<b>Conclusion.....</b>	<b>9</b>
<b>Chapitre 2 : La Signature Électronique.....</b>	<b>10</b>
<b>Introduction .....</b>	<b>10</b>

<b>I.</b>	<b>Définition et caractéristiques.....</b>	<b>10</b>
<b>II.</b>	<b>Similarité avec la signature manuscrite .....</b>	<b>11</b>
<b>III.</b>	<b>Cadre légale : reconnaissance de la signature électronique .....</b>	<b>13</b>
<b>IV.</b>	<b>Intérêt à utiliser la signature électronique dans l’administration au Sénégal..</b>	<b>20</b>
IV.1	Politique générale de l’État .....	20
IV.1.1	Signature électronique dans l’administration centrale : projet de l’État du Sénégal sur le numérique – place de la signature numérique .....	21
IV.1.2	Signature électronique dans l’administration local : l la gestion des actes d’état civil : place de la signature électronique .....	22
IV.2	Besoin social et modernisation de l’administration au niveau des municipalités	22
IV.3	La sécurité des documents.....	23
IV.4	Efficacité .....	23
IV.5	Rentabilité .....	24
IV.6	L’archivage numérique .....	24
	<b>Conclusion.....</b>	<b>26</b>
 <b>Chapitre 3 : Méthodes et Approches pour la Signature Électronique.....</b>		<b>28</b>
	<b>Introduction .....</b>	<b>28</b>
<b>I.</b>	<b>La cryptographie .....</b>	<b>28</b>
I.1	La cryptographie symétrique.....	30
I.2	La cryptographie asymétrique .....	32
I.3	La cryptographie hybride .....	34
I.4	Les fonctions de hachages.....	36
<b>II.</b>	<b>La signature électronique : objet technique .....</b>	<b>39</b>
II.1	L’opération de signature.....	39
II.2	La vérification de la signature .....	40
II.3	Les formes et formats de la signature électronique .....	41
II.4	Les certificats et infrastructures de gestion des clés publiques (IGC) .....	43

II.4.1	Les certificats.....	43
II.4.1.1	Notion d'un certificat.....	44
II.4.1.2	Le certificats X509.....	47
II.4.1.3	Types de fichiers des certificats.....	48
II.4.2	Les infrastructures de gestion des clés publiques.....	49
II.4.2.1	L'autorité de certification.....	51
II.4.2.2	Architectures d'infrastructures à clefs publiques.....	52
<b>III.</b>	<b>La signature électronique dans les fichiers PDF .....</b>	<b>54</b>
III.1	Définition et structure d'un fichier PDF.....	55
III.1.1	Définition.....	55
III.1.2	Structure interne des fichiers PDF.....	55
III.1.2.1	Structure de base des fichiers PDF.....	55
III.1.2.2	Fonctionnement de la mise à jour d'un PDF signé.....	57
III.1.2.3	Ajout de la signature électronique dans PDF.....	57
	<b>Conclusion.....</b>	<b>58</b>
	<b>Chapitre 4 : Outils, Implémentation et Présentation du module de signature électronique.....</b>	<b>59</b>
	<b>Introduction .....</b>	<b>59</b>
<b>I.</b>	<b>Outils .....</b>	<b>59</b>
I.1	GroupDocs .....	60
I.1.1	Types de signature supportés.....	60
I.1.2	Limites de l'API GroupDocs.....	61
I.2	L'API IText.....	62
I.2.1	Avantages de l'API IText.....	63
I.2.2	Limites de l'API IText.....	63
I.3	Comparaison entre les deux API.....	63
<b>II.</b>	<b>Implémentation.....</b>	<b>64</b>



II.1	Diagramme de cas d'utilisation.....	64
II.2	Diagrammes de séquence .....	65
II.2.1	Diagramme de séquence signer acte d'état civil .....	65
II.2.2	Diagramme de séquence vérifier signature acte d'état civil.....	66
II.3	KeyStore Explorer.....	66
II.4	Le langage java.....	72
II.4.1	Spring Framework .....	72
II.4.2	L'environnement de développement IntelliJ IDEA.....	74
II.5	Les technologies web utilisées .....	74
II.5.1	Le langage HTML et le moteur de template thymeleaf.....	74
II.5.2	CSS et la librairie Bootstrap .....	75
II.5.3	JavaScript et la librairie JQuery.....	75
<b>III.</b>	<b>Présentation de l'application.....</b>	<b>76</b>
III.1	Page d'accueil .....	76
III.2	Interface de connexion .....	76
III.3	Formulaire de signature électronique .....	78
III.4	Vérification de la signature effectuée.....	80
	<b>Conclusion.....</b>	<b>81</b>
	<b>Conclusion Générale .....</b>	<b>82</b>
	<b>Bibliographie.....</b>	<b>84</b>
	<b>Webographie.....</b>	<b>85</b>

# LISTE DES FIGURES

Fig. 1 : Le parallèle entre les signatures manuscrite et électronique[9].....	13
Fig. 2 : Schéma de fonctionnement de la cryptographie symétrique[24].....	31
Fig. 3 : Interception de la clé secrète par un espion[25, p. 101] .....	32
Fig. 4 : Schéma de fonctionnement de la cryptographie asymétrique[24].....	33
Fig. 5 : Schéma de fonctionnement de la cryptographie hybride[28] .....	36
Fig. 6 : la taille de l’empreinte est constante[11, p. 25] .....	37
Fig. 7 : Le hash est une fonction à sens unique[11, p. 26] .....	38
Fig. 8 : Schéma de fonctionnement des fonctions de hachage[24] .....	38
Fig. 9 : Réalisation cryptographique de la signature numérique[9, p. 21] .....	40
Fig. 10 : Vérification technique de la signature électronique[9, p. 21].....	41
Fig.11 : Formes de signature électronique[10, p. 29].....	41
Fig. 12 : Principe de la création des certificats[22, p. 26] .....	46
Fig. 13 : certificat X509[32, p. 38].....	47
Fig. 14 : Délivrance d’un certificat par une autorité de certification[26, p. 110] .....	52
Fig. 15: Architecture PKI hiérarchique[36] .....	54
Fig. 16 : Structure d'un fichier PDF[37, p. 14].....	56
Fig. 17 : Mise a jour incrémentale d'un PDF[37, p. 15].....	57
Fig. 18 : Visualisation PDF signé numériquement avec un éditeur de texte[41, p. 26].....	58
Fig. 19 : Signature électronique avec signature code-barres[44] .....	61
Fig. 20 : Signature électronique par QR-code[45] .....	61
Fig. 21 : Prix des licences temporaires proposées[46] .....	62
Fig. 22 : Diagramme cas d'utilisation.....	64
Fig. 23:Diagramme séquence signature électronique .....	65
Fig. 24: Diagramme séquence vérification signature électronique .....	66
Fig. 25 : Choix du type de KeyStore et démarrage de la génération de la paire de clés .....	67

Fig. 26 : Choix de l'algorithme, de la taille de la clé et des informations liés au certificat.....	67
Fig. 27 : Information à remplir sur l'autorité de certification.....	68
Fig. 28 : définition de l'alias et du mot de passe .....	68
Fig. 29 : Certificat de l'autorité de certification .....	69
Fig. 30 : étape 1 de la génération du certificat de l'entité réceptrice : Mairie .....	70
Fig. 31 : Saisi information de l'entité réceptrice du certificat .....	70
Fig. 32 : Information liés au certificat.....	71
Fig. 33 : Détails sur le certificat de l'entité réceptrice .....	71
Fig. 34 : Les composants Spring[52] .....	73
Fig. 35 : Page d'accueil de l'application .....	76
Fig. 36 : Procédure de connexion à l'application .....	77
Fig. 37 : Formulaire de connexion .....	77
Fig. 38 : Menu de l'application.....	78
Fig. 39 : Formulaire de signature électronique .....	78
Fig. 40 : Opération de signature réussie .....	79
Fig. 41 : Apparence de la signature.....	80
Fig. 42 : Vérification de la signature électronique .....	80
Fig. 43 : Signature valide .....	81

# LISTE DES SIGLES ET ABRÉVIATIONS

<b>ANEC</b>	Agence Nationale de l'État Civil
<b>FNTC</b>	Fédération Nationale des Tiers de Confiance
<b>CNC</b>	Commission Nationale de Cryptologie
<b>PDF</b>	Portable Document Format
<b>XML</b>	Extensible Markup Language
<b>CSV</b>	Coma Separated Values
<b>UEMOA</b>	Union Économique et Monétaire Ouest Africaine
<b>CEDEAO</b>	Communauté Économique des États de l'Afrique de l'Ouest
<b>OHADA</b>	Organisation pour l'Harmonisation en Afrique du Droit des Affaires
<b>AES</b>	Advanced Encryption Standard
<b>RSA</b>	Rivest Shamir Adelman
<b>HMAC</b>	Hash-Based Message Authentication Code
<b>CMS</b>	Cryptographic Message Syntax
<b>XADES</b>	XML Advanced Electronic Signature
<b>CADES</b>	CMS Advanced Electronic Signature
<b>PADES</b>	PDF Advanced Electronic Signature
<b>PKCS</b>	Public Key Cryptographic Standard
<b>IGC</b>	Infrastructure de Gestion de Clés
<b>PKI</b>	Public Key Infrastructure
<b>AC</b>	Autorité de Certification
<b>ISO</b>	International Organization for Standardization
<b>IETF</b>	Internet Engineering Task Force
<b>CRL</b>	Certificate Revocation List

<b>PGP</b>	Pretty Good Privacy
<b>TLS</b>	Transport Layer Security
<b>AE</b>	Autorité d'Enregistrement
<b>API</b>	Application Programming Interface
<b>LDAP</b>	Lightweight Directory Access Protocol

# Introduction

La pandémie a mis en évidence l'anachronisme que représente la signature papier. Imprimer un document, le signer, le scanner et l'envoyer par mail, voilà une habitude qui appartient au passé et qui ne répond plus aux attentes du bureau à domicile, du travail hybride et globalement de nos sociétés hyperconnectées[1]. Ce processus est en majeure partie, celui que nous retrouvons dans les municipalités. Cette utilisation du support papier pour délivrer des actes d'état civil, qui sont en ce format, donc à l'attente d'une signature à l'encre et au stylo pour leurs validités. Ce qui constitue un handicap majeur pour offrir des services en ligne pour la demande d'un acte d'état civil.

Cependant, avec la dématérialisation des procédures, les mairies, pourront générer des actes d'états civils au format numérique. Dans cette dynamique, la signature électronique s'impose pour parapher les actes d'état civil produits. Ainsi certains points nous interrogent.

Pourquoi adopter la signature électronique pour signer les actes d'état civil ?

Qu'est-ce que la signature électronique ?

Quelle est le statut juridique de la signature électronique au Sénégal ?

Quelle solution utilisée pour intégrer la signature électronique pour la signature des actes d'état civil ?

Notre va travail s'étayer en quatre chapitres.

Au premier chapitre nous allons parler du contexte général de notre travail de mémoire.

Au deuxième chapitre nous aborderons la notion de la signature électronique, son caractère juridique au Sénégal mais aussi ses opportunités.

Au troisième chapitre nous allons décrire les procédés et mécanismes cryptographiques utilisées pour la signature électronique.

Au quatrième et dernier chapitre nous décrirons les outils et technologies utilisés et présenterons notre module de signature électronique.

# Chapitre 1 : Contexte du Mémoire

## Introduction

Le service d'état civil joue un rôle essentiel à la fois pour chaque individu mais également pour l'État, les administrations publiques et tous les organismes qui ont besoin de connaître la situation juridique des citoyens[2]. Ainsi la gestion efficace et optimale de l'état civil représente un point très important pour la bonne marche d'un État.

Dans cette partie, nous aborderons la gestion de l'état civil au niveau des municipalités qui sont les entités administratives chargées de délivrer des actes d'état civil. Pour ce faire nous l'avons décomposée en quatre sous partie : la gestion de l'état civil en papier, l'archivage numérique des actes d'état civil, la dématérialisation des procédures d'actes d'état civil et ses limites, la problématique du sujet et l'objectif.

### I. La gestion de l'état civil en papier

L'expression « État civil » désigne l'ensemble des éléments relatifs à la personne qui identifient un individu tels que les nom et prénoms, la date et le lieu de sa naissance, sa situation maritale. Par extension c'est l'appellation donnée aux services administratifs d'une commune qui reçoivent les déclarations et qui conservent les registres concernant les naissances, les mariages et les décès [2].

En outre, l'état civil est le moyen permettant à un pays l'enregistrement continu et exhaustif des naissances, des décès et de la situation maritale de leurs habitants. Cependant, pour qu'un acte d'état civil soit délivré, une demande doit être déposée par le ou les individu(s) concerné (s). Les actes d'état civil sont notamment dressés que pour les naissances, les décès ou les mariages survenus dans la commune de l'individu.

Sur le plan individuel, il permet d'identifier une personne dans l'organisation sociale et administrative. Il donne également à l'individu la possibilité d'exercer des droits variés. La copie d'acte de naissance est ainsi utilisée pour les mariages, s'inscrire à l'école, se présenter aux examens et concours, obtenir la carte nationale d'identité.

Comme souligné aux paragraphes précédents, pour obtenir un acte d'état civil nous devons nous déplacer jusqu' aux locaux de la municipalité pour faire la demande. Ensuite, un

agent municipal est chargé de recueillir et d'enregistrer les informations concernées dans un registre et délivre, une copie signée par un officier d'état civil au demandeur.

Ce processus fastidieux représente souvent un handicap. Car les citoyens qui ont besoin d'un acte sont obligés de se déplacer au siège de la municipalité habileté à leur délivrer un acte d'état civil.

Toutefois il faut noter que des initiatives ont été prises dans le cadre du programme national lié à l'archivage numérique et à la digitalisation d'actes d'état civil. Et par conséquent, sur financement de l'Union Européenne[3], l'état du Sénégal, à travers le ministère des collectivités territoriales, du développement et de l'aménagement des territoires, a entamé le projet de numérisation des actes d'état civil.

## **II. L'archivage numérique des actes d'état civil en papier**

L'Agence nationale de l'état civil (ANEC) compte digitaliser ses services, un objectif pour l'atteinte duquel elle prévoit un renforcement de capacités de ses agents et une révision des textes en vue de garantir un état civil fiable et sécurisé, a déclaré son directeur général, Aliou Ousmane SALL. Il poursuit ensuite par : « Cette politique de digitalisation passe par une transformation des procédures pour permettre aux administrations de bien fonctionner, mais surtout de régler les problèmes d'accessibilité des citoyens aux services d'état civil aussi bien aux Sénégalais de l'extérieur que ceux à l'étranger »[4].

Ainsi il a signé avec la société « Sénégal numérique Sa », une convention de partenariat visant à garantir la souveraineté des données d'état civil. Et la direction de l'état civil a procédé à la numérisation de 15 millions d'actes en perspective de la mise en place d'un Registre national de l'état civil qui sera logé au Data center de Diamniadio[5].

Ces actions concrètes posées rentrent dans le cadre de la modernisation du système d'état civil et le processus de dématérialisation des procédures de l'état civil.



### **III. La dématérialisation partielle des procédures de l'état civil**

Aujourd'hui, la dématérialisation des procédures est une nécessité, pour les entreprises et les administrations, pour pouvoir fournir des services de qualité à leurs clients et administrés.

En effet, le temps, la distance géographique, les activités, etc. contraignent la présence des usagers sur les locaux des structures en question pour chercher un document administratif comme par exemple : l'acte de naissance, l'acte de mariage, etc.

Or pour obtenir un acte d'état civil, les personnes concernées sont obligées de se déplacer au niveau de la mairie. Et en conséquence, créer une file d'attente sur place, et ceci pourrait pénaliser certains citoyens qui en ont besoin en urgence. Fort de ce constat, certaines municipalités ont montré leur volonté de faire évoluer les choses. Cette évolutivité va optimiser le processus et rendre l'obtention de ces documents beaucoup plus facile et beaucoup plus accessible au public. Pour y parvenir, adopter une solution numérique est inévitable. Ainsi, certaines mairies ont procédé à la dématérialisation de certaines fonctionnalités comme la génération automatique d'acte de naissance, d'acte de mariage, etc.

Cependant cette dématérialisation partielle, la numérisation des actes papiers sont moins efficaces car elles permettent aux usagers de faire une demande d'un acte d'état civil. Cette contrainte est liée à l'utilisation de la signature autographe pour signer les actes.

#### **III.1 Les limites**

La réalité de la situation actuelle est que, lors des procédures de demande de ces actes au travers leurs services de dématérialisation, certaines tâches sont jusqu'à présent effectuées de manière classique. Parmi ces tâches, nous pouvons citer principalement la signature des actes, qui constitue en quelque sorte l'élément le plus essentiel d'un document de ce genre. Ainsi nous considérons que cette dématérialisation est partielle puisqu'elle ne concerne pas toutes les étapes de la chaîne métier qui interviennent dans ce processus.

Or la dématérialisation de l'information suppose trois conditions essentielles[6] :

- les processus doivent être prévus pour traiter de bout en bout l'information dématérialisée : c'est donc une question d'organisation ;

- la confiance dans l'information ainsi dématérialisée doit être équivalente à celle de l'information « papier » : la sécurité est donc une préoccupation majeure, qu'elle concerne la création, la circulation ou la reconnaissance de l'information sa « non-répudiation »;
- enfin, l'information doit être restituée de façon absolument intègre lorsque l'on en a besoin : l'archivage fait donc lui aussi partie de la problématique.

Un service dématérialisé, qui n'intègre pas la signature numérique, reste très limité. En plus elle nous empêche d'exploiter amplement les atouts que nous procure la dématérialisation sur certains aspects. Et c'est ce que nous retrouvons dans nos municipalités, ce qui oblige à se maintenir dans les pratiques usuelles.

### **III.1.1 La signature manuscrite**

Depuis toujours, le document papier est notre support privilégié dès lors qu'il est nécessaire de conserver le témoignage d'un accord entre plusieurs parties. Traditionnellement, et à défaut de pouvoir en protéger l'intégrité, l'usage de sceaux ou de signatures, permet de garantir l'authenticité de tels documents[7].

Mais entretemps les choses ont changé et les documents numériques sont apparus avec le développement de l'informatique. Du moment que la dématérialisation permet de produire les documents au format numérique, la signature classique que nous utilisons, pour signer les documents au format papier, ne sera plus adaptée. Et c'est là que la signature électronique est venue pour se substituer de la signature manuscrite sur les documents électroniques.

Mais, jusqu'à présent, beaucoup d'administrations comme les municipalités, continuent à signer les actes d'états civils de manière classique en faisant recours à l'impression papier.

Beaucoup de services de dématérialisation de procédure ne font pas usage de la signature électronique. Et au cas où il y a génération de documents lors de la procédure, pour leurs validités, ces documents jouissent d'un droit d'authentification. Mais pour authentifier un document, il faut obligatoirement y apposer sa signature. Et comme les documents à signer sont générés de façon numérique, pour les signer, il va falloir, tout d'abord les imprimer pour pouvoir passer à l'opération de signature. De ce fait, bien que les services (de demande d'un acte de naissance, d'un acte de mariage ou bien de tous autres documents) soient dématérialisés,

l'impression des documents est pratiquement inévitable, et s'impose dès lors qu'une signature doit être apposée pour sa validité.

La municipalité a besoin parfois de garder certains documents pour preuve et pour ce, elle est obligée d'archiver la version papier qui est signée.

### **III.1.2 L'archivage papier**

Comme l'impression papier et la signature classique, l'archivage du papier est aussi inévitable au niveau des mairies, avec le système de dématérialisation partielle des procédures de demandes d'actes d'états civils. Et tant que nous n'intégrons pas la signature numérique, va perdurer. Et cette dématérialisation ne leur permettra pas de profiter de l'archivage numérique beaucoup plus efficace que l'archivage classique.

Ainsi pour lever ces contraintes afin rendre des services de hautes qualités à la population, la solution est, par-dessus la dématérialisation, l'intégration de la signature électronique.

## **III.2 La dématérialisation des procédures et documents, la signature électronique**

La signature électronique est avant tout une fonctionnalité majeure des services de dématérialisation, et les gains qui sont à en attendre sont tous ceux issus de cette disparition des flux papier au profit de flux entièrement électroniques. Cet outil au service de la productivité, tant pour l'expéditeur que pour le destinataire est une solution très efficace pour les municipalités dans la gestion de l'état civil. En effet, elle contribue à [8]:

- **faciliter l'envoi et l'échange des documents**, qui peuvent se faire, par un ordinateur ou un smartphone ;
- **accélérer la procédure de signature** : les documents peuvent être signés en quelques secondes. Ils peuvent être aussi parafés simultanément par les parties, plutôt que successivement comme c'est le cas pour le papier ;
- **suivre en temps réel l'avancement des dossiers** : on peut voir qui a signé et si besoin relancer, ceux qui n'ont pas encore signé ;
- **sécuriser les données dématérialisées** : le tiers de confiance est garant de l'intégrité de vos données ;

- **faire des économies sur l'achat de papier**, d'encre et d'impression des documents à signer ainsi que sur les frais d'envoi ou, le cas échéant de déplacement ;
- **automatiser vos processus** : des traitements ou des actions peuvent être lancées une fois le document signé.

### **III.3 Les vulnérabilités de la signature numérisé et la signature numérique**

La signature numérisée est un moyen rapide pour attacher un document électronique une signature. Cependant elle est vulnérable car très facilement détachable du document auquel elle est apposée. En plus elle ne permet d'identifier le signataire. Pour le cas d'un copier-coller, n'importe qui pourrait donc utiliser une signature et valider des documents. Ainsi prouver aussi la source du document peut être très difficile. Et juridiquement la validité de cette signature est à revoir car au niveau de l'article 42 de la loi sur les transactions le législateur précise que : une signature électronique créée par un dispositif sécurisé que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat numérique est admise comme signature au même titre que la signature autographe.

Comme n'importe quel système de sécurité, la signature électronique possède son lot de vulnérabilités qui font qu'elle est reniée par certaines structures ne la jugeant pas suffisamment fiable. La plus grande vulnérabilité de la signature électronique reste son système de cryptographie, et notamment la clé privée. En effet, cette clé privée doit, en principe, rester la propriété exclusive de l'expéditeur. Dans la pratique, toutefois, cela implique certaines restrictions : notamment, le stockage de la clé privée.

Ces points, aussi importants, sont abordés au chapitre suivant. Ils représentent des arguments solides et valables pour que les municipalités adoptent la signature électronique pour signer les actes d'états civils qu'elles délivrent.

## **IV. Problématique du sujet**

Les citoyens éprouvent d'énormes difficultés pour accéder aux services d'état civil. Ceci est dû le plus souvent par la résidence des usagers qui est souvent éloignée de l'emplacement de la structure municipale qui a la prérogative à délivrer à l'utilisateur l'acte demandé. Et avec le développement rapide du numérique, nous avons un changement de paradigme de la société.

Ainsi pour offrir des services d'état civil qui répondent aux attentes des citoyens, les municipalités doivent passer à la digitalisation des procédures d'obtention d'un acte d'état civil avec l'intégration de la signature électronique dans ce processus.

Aujourd'hui, comme nous l'avons évoqué dans les parties précédentes, beaucoup de municipalités ont commencé à générer les actes d'état civil à travers des formulaires. Cependant pour l'authenticité des documents, elles sont obligées de les imprimer pour qu'une signature soit apposée. Ce processus, générer électroniquement un document ensuite l'imprimer pour le signé, est onéreux et permet pas d'avoir un service de haute qualité qui réponde l'attente de la population. Or les véritables gains issus de l'usage de la signature électronique viennent de la refonte en profondeur des processus métier liés à la génération, au traitement et à la conservation des documents.

## V. Objectifs

L'objectif de ce travail est d'abord d'examiner l'état actuel du numérique dans la gestion de l'état civil, les dispositions juridiques pour l'intégration de la signature électronique dans la dématérialisation des procédures d'état civil. Mais aussi faire une description des aspects techniques qui sous-tendent la signature électronique. Et en fin mettre en place une implémentation pour simuler la signature électronique d'un acte d'état civil.

Ainsi pour renouveler la gestion papier et modifier la méthode d'authentification des actes d'état civil, nous sommes fixées pour objectif de développer des fonctionnalités, à travers une application web, permettant de signer électroniquement un acte d'état civil produit au format numérique et par conséquent changer le processus de signature.

L'application va permettre :

- à partir d'un formulaire, de la clé privée, du certificat du signataire effectuer la signature électronique d'un acte d'état civil ;
- la signature sera matérialisée dans l'acte sous la forme de texte ou sous la forme de QR code pour une meilleure expérience utilisateur et une facilitation lors de la vérification ;

- la vérification est faite à travers une application mobile ou bien à partir d'un formulaire.

## **Conclusion**

Dans cette partie, après avoir donné les détails sur les méthodes utilisées actuellement lors du processus de demande d'un acte d'état civil et montré les limites de celles-ci, nous avons annoncé la problématique sur laquelle repose ce travail de mémoire.

# Chapitre 2 : La Signature Électronique

## Introduction

Dans cette partie, nous allons définir la notion de signature électronique. Ensuite nous parlerons du statut juridique de la signature électronique au Sénégal mais aussi des opportunités de celle-ci.

### I. Définition et caractéristiques

La signature électronique est une réalité multiforme et il est impossible d'en donner une unique définition. Procédé technique à valeur juridique, garant de l'engagement d'une personne mais aussi vecteur de sécurité informatique, il est indispensable de passer par plusieurs angles de vue pour se l'approprier pleinement[9, p. 18]. La signature électronique est un procédé permettant à une personne d'apposer son accord sur un document électronique. Le procédé de la signature électronique est un processus qui fait intervenir plusieurs acteurs, du signataire à l'État en passant par les tiers de confiance.

Elle correspond techniquement aux données électroniques jointes ou associées à un document que le signataire utilise pour signer [4, p. 87]. La signature électronique ne doit pas être confondue avec la signature numérisée (par exemple la signature manuscrite scannée) ! Si la signature électronique n'est pas « un but en soi », elle est aussi un élément constitutif indispensable des transactions électroniques réalisées par Internet et de la validité juridique des documents nativement électroniques.

La signature électronique permet de garantir l'identité d'un signataire, l'intégrité et la provenance d'un document et, plus largement, l'établissement de la confiance dans les échanges numériques[9, p. 8]. Elle représente en quelque sorte la transposition de la signature manuscrite dans le monde numérique. Sauf qu'elle est attachée aux documents d'une façon qui n'est pas familier au grand public. Et elle est aujourd'hui le seul procédé informatique permettant de donner la même valeur juridique à un écrit électronique qu'à un écrit traditionnellement papier[10, p. 3].

Bien au-delà de l'acte technique désormais largement répandu, la signature électronique est un acte fort qui scelle un accord, affirme une position ou encore garantit une conformité à

la réglementation ; dans tous les cas, c'est un acte qui revêt une importance pour la personne physique ou morale qui signe. De fait, nous devons l'étudier sous différents angles pour pouvoir l'utiliser efficacement et bénéficier de ses apports pour signer convenable des documents administratifs au niveau des mairies.

Dans ce contexte, la signature électronique remplit deux rôles majeurs, qui tendent à établir les conditions de la confiance dans les échanges numériques et donc à rendre possible la dématérialisation [9, p. 9]:

- la signature électronique d'un document (acte de naissance par exemple) confère à celui-ci une **valeur juridique équivalente** à celle d'un document papier signé de manière manuscrite, en marquant l'engagement de la personne qui a apposé la signature ;
- des fonctions connexes à la signature électronique (cachet, horodatage...) servent à offrir des conditions **de sécurité technique** en garantissant sa provenance, son intégrité, ou encore la date de sa réalisation.

Cependant, pour jouer ce rôle, la signature électronique doit avoir des caractéristiques bien définies. Et voici ci-dessous, une description détaillée, des caractéristiques fondamentales de la signature électronique :

- **authentique** : l'identité du signataire est vérifiée par un procédé d'authentification, l'identité du signataire doit pouvoir être retrouvée de manière certaine ;
- **infalsifiable** : une personne ne peut pas se faire passer pour un autre, on ne peut pas "imiter" la signature de quelqu'un d'autre ;
- **non réutilisable** : la signature fait partie du document signé et ne peut être déplacée sur un autre document, on ne peut pas "copier/coller" la signature d'un document à un autre ;
- **inaltérable** : une fois que le document est signé, on ne peut plus le modifier, un document signé est inaltérable, ou du moins, toute altération, si minime soit-elle, doit pouvoir être détectée ;
- **irrévocable** : La personne qui a signé ne peut le nier, la personne qui a signé ne peut le contester.

## II. Similarité avec la signature manuscrite



Lorsque nous réalisons une signature, nous utilisons pratiquement quatre éléments essentiels autant pour la signature manuscrite que pour la signature électronique. Si l'un de ces éléments fait défaut, le processus ne pourra pas se dérouler. Donc avant d'entamer de signer quoique ce soit, il faut effectivement se procurer ces fondamentaux. Faisons d'abord une description succincte de ces éléments et pour ce faire nous s'appuyons sur un document produit par la FNTC<sup>1</sup>.

La réalisation d'une signature manuscrite nécessite quatre éléments[11, p. 162] :

- **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente ;
- **un document à signer**, qui peut être de natures diverses tant pour le fond (contrat, lettre, formulaire . . .) que pour la forme (simple papier, papier sécurisé. . .) ;
- **un instrument d'écriture** (plume, stylo . . .) ;
- **un geste**, que le signataire est le seul à savoir réaliser avec l'instrument d'écriture : la signature à proprement parler.

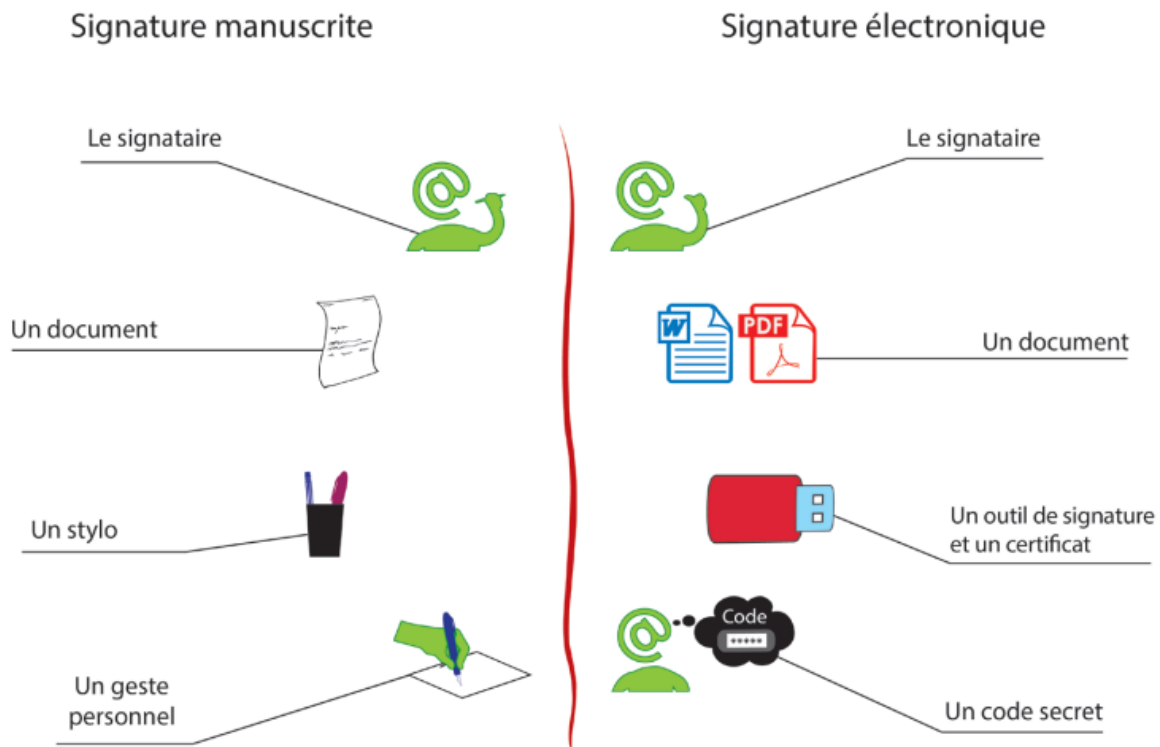
La réalisation de la signature électronique s'effectue aussi comme la signature manuscrite avec quatre éléments, dans un parallèle quasiment parfait avec cette dernière.

- **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente, muni d'un terminal informatique pour réaliser l'opération de signature ;
- **un document à signer**, qui peut être de natures diverses tant pour le fond (lettre, formulaire . . .) que pour la forme (document issu d'un traitement de texte, fichier PDF, fichier image, données informatiques au format XML, CSV ou autres . . .) ;
- **un instrument de signature** (la carte à puce, la clé USB ou le magasin logiciel support du certificat) ;
- **un secret**, que le signataire est le seul à connaître : le code de déblocage de sa clé privée sur le support du certificat.

Voici ci-dessous une figure illustrant ce parallélisme entre ces deux actes de signature.

---

<sup>1</sup> Fédération nationale des tiers de confiance



*Fig. 1 : Le parallèle entre les signatures manuscrite et électronique[9]*

Imaginons qu'on nous soumet un document administratif, le réflexe premier qui nous tient c'est de vérifier s'il est apposé une signature sur ce dernier. Si le document a été signé, c'est en ce moment-là que nous accordons de la valeur au document et une nécessité de l'exploiter. Au cas contraire, nous avons un doute sur le document en tant que tel, mais aussi manquer de confiance envers la personne, la structure, ou l'entité qui a produit le document en question. Donc la signature établit une confiance entre deux parties qui partagent des documents.

La signature étant une marque d'engagement qui confère une valeur juridique au document sur lequel elle est apposée, connaître et bien comprendre, le cadre juridique qui s'applique à la signature électronique dans son pays est primordial pour les acteurs concernés.

### **III. Cadre légale : reconnaissance de la signature électronique**

Les réseaux informatiques ouverts tels que l'Internet ont été techniquement optimisés pour assurer le transport de données. Dans cette optique les aspects juridiques n'étaient pas

encore pris en compte. Or, Internet ayant vocation à devenir la plate-forme universelle d'échange de produits et de services, la réglementation devient primordiale. « *La mise en œuvre de la signature électronique dans un projet répond nécessairement à un besoin juridique. Dans le cas inverse, il faudrait, en amont, s'interroger sur l'utilité de la mise en œuvre de la signature* » [11, p. 164].

Dans cette perspective, il est indispensable d'organiser les échanges électroniques par la mise en place de garanties spécifiques sur le plan juridique. Ainsi selon [12] : « *L'adaptation du droit au numérique apparaît comme une nécessité résultant de l'essor considérable du numérique. Le numérique offre beaucoup d'opportunités, mais engendre beaucoup de contraintes d'ordre juridique. Une assez appréciable adaptation du droit au numérique est opérée par le législateur malien et les législateurs de certaines communautés sous régionales telles que l'UEMOA, la CEDEAO et l'OHADA. Cette adaptation est justifiée par la nécessité de donner aux acteurs les moyens de tirer profit du numérique avec une sécurisation juridique du cyberspace. Toutefois, elle doit être poursuivie afin de suivre l'évolution rapide du numérique* ».

Comme évoqué sur la loi sur les transactions électroniques au Sénégal au niveau de l'exposition des motifs : avec le développement des réseaux informatiques, le nombre de transactions électroniques est en constante augmentation. À titre indicatif, les transactions électroniques portent sur la production, la promotion, la vente, la distribution de produits et les échanges par des réseaux de télécommunications ou informatiques (interrogation à distance, envoi d'une facture, etc.). Les aspects juridiques ont été trop souvent considérés comme un frein à leur développement.

Pour relever ce défi, le Sénégal, dans le cadre de la réglementation des échanges électroniques, mis en place un cadre normatif pour l'utilisation en toute sécurité des documents électroniques et de la signature électronique. Sur cette même logique le législateur précise que : l'objet de la loi sur les transactions électroniques vise à assurer la sécurité et le cadre juridique.

Le Sénégal a établi, plusieurs dispositions traitant la question liée aux documents numériques et à la signature électronique, au travers des lois votés par l'assemblée nationale mais aussi des décrets d'application.

- **LOI n° 2008-08 du 25 janvier 2008 sur les transactions électroniques**

Sur cette loi, le législateur reconnaît de l'importance de l'informatique mais surtout les transactions électroniques et le potentiel qu'ils représentaient. De ce fort constat, il fixe dans le premier article de cette loi le principe :

---

---

**Article premier.** - Sauf dispositions contraires, la communication par voie électronique ne peut être limitée que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, les besoins de la défense nationale, les exigences de service public et les contraintes techniques inhérentes au moyen de communication.

---

---

Les documents électroniques ne pouvaient pas constituer à l'établissement de preuves susceptibles d'être présentées en justice. Et ceci représentait une insécurité sur les acteurs qui intervenaient sur ce secteur d'activité. Pour lever cette contrainte, et définir le cadre légal de la « preuve par écrit » de façon que les documents numériques puissent être recevables comme preuve. Le législateur précise au niveau de l'article 27 de cette loi que :

---

---

**Art. 27.** – L'écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

---

---

Ainsi, il est précisé d'emblée que la preuve peut être établie sur tout support et transmise par tout moyen. Et cela donne la possibilité aux documents électroniques d'être admises dans le droit de la preuve au Sénégal.

Les documents électroniques, sont admis en tant que preuve en justice mais, sont soumises à des contraintes comme mentionné au niveau de l'article 37 de cette loi.

---

---

**Art. 37.** – L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier et a la même force probante que celui-ci, sous réserve que puisse être dûment identifiée dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

---

---

Jusqu'ici, les dispositions que nous avons citées, sont focalisées plus particulièrement sur les documents électroniques. Maintenant voyons les dispositions prises pour la signature

électronique. Sur la base de ces dernières, nous pourrions utiliser la signature électronique pour signer des documents numériques sans encourir aucun risque. Sur ce point, le législateur définit que :

---

---

**Art. 41.** – La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée.

L'acte authentique peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret.

---

---

Pour beaucoup plus de précision sur la question de l'acceptation de la signature électronique dans le droit sénégalais, il donne la signature électronique la même valeur que la signature manuscrite comme indiqué ci-dessous :

---

---

**Art. 42.** – Sans préjudice des dispositions en vigueur, une signature électronique créée par un dispositif sécurisé que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat numérique est admise comme signature au même titre que la signature autographe.

Nul ne peut être contraint de signer électroniquement.

---

---

En fin, sur cette question de la signature électronique, le législateur exhorte l'utilisation de la signature électronique dans les conditions indiquées au niveau de l'article suivant :

---

---

**Art. 54.** – Le message signé électroniquement sur la base d'un certificat numérique, dont l'heure et la date sont certifiées par le prestataire, constitue un envoi recommandé.

---

---

En se basant sur ces dispositions, toute personne physique ou morale peut produire des actes commerciaux ou administratifs pourvue qu'elle respecte les conditions établies au niveau des articles cités ci-dessus.

En plus de cette loi sur les transactions électroniques le parlement du Sénégal a voté aussi une loi sur la cryptologie qui est une science qui sous-tend la signature électronique.

- **LOI N° 2008 - 41 DU 20 AOUT 2008 SUR LA CRYPTOLOGIE**

Par la suite, le Sénégal a adopté cette loi en 2008 sur la cryptologie pour prendre en compte certains aspects fondamentaux notamment, la fourniture, le transfert et les conditions d'homologation liées à l'importation ou l'exportation de moyens ou de « prestations de cryptologie »<sup>1</sup>.

- **Dispositions générales**

« L'objectif de ce projet de loi, qui comprend huit chapitres, est donc de définir les conditions générales d'utilisation, de fourniture, d'importation et d'exportation des moyens et des prestations de cryptologie ». Au travers cette loi, des dispositions ont été prises pour obliger à toute personne ou entité prétendant fournir un service de cryptologie de se conformer aux règles juridiques appliquées à cette technologie.

Dans les dispositions établies par cette loi, le législateur a rappelé d'abord l'objet de l'adoption de cette dernière : « *La présente loi a pour objet de fixer les règles applicables aux moyens, modalités et systèmes de cryptologie* ».

- **Commission nationale de cryptologie**

Pour le suivi et le contrôle de l'activité des personnes ou des organismes qui offrent un service de « moyens de cryptologie »<sup>2</sup>, le Sénégal a instancié une commission nationale de cryptologie : « *Il est créé une Commission nationale de cryptologie rattachée au Secrétariat Général de la Présidence de la République* ». Cette commission a plusieurs missions à accomplir dans le cadre de la sécurité des systèmes d'informations mais aussi de l'utilisation de ces moyens cryptologiques.

La Commission nationale de cryptologie est chargée de statuer sur :

- ✓ toute question relative au développement des moyens ou prestations de cryptologie au Sénégal ;
- ✓ les projets de textes législatifs et réglementaires en matière de cryptologie ;

---

<sup>1</sup> Prestation visant à transformer à l'aide de codes secrets des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet ;

<sup>2</sup> L'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer

- ✓ les normes techniques adoptées dans le domaine de la sécurité des systèmes d'information en général et celui de la cryptologie en particulier.

Elle est compétente pour :

- ✓ recevoir les déclarations prévues à l'article 14 de la présente loi ;
- ✓ délivrer des autorisations prévues à l'article 15 de la présente loi ;
- ✓ délivrer des agréments aux « prestataires de services de cryptologie » conformément à l'article 16 de la présente loi ;
- ✓ demander la communication des descriptions des caractéristiques techniques des moyens de cryptologie ;
- ✓ mener des enquêtes et procéder à des contrôles sur les prestataires de services de cryptologie ainsi que sur les produits fournis ;
- ✓ prononcer des sanctions administratives à l'encontre des contrevenants aux dispositions de la présente loi ;
- ✓ défendre les intérêts du Sénégal dans les instances et organismes régionaux et internationaux traitant de la cryptologie.

Le législateur, au travers cette loi, a élaboré aussi les dispositions qui régissent l'utilisation des moyens et prestations de cryptologie.

- **Régimes juridiques des moyens et prestations de cryptologie**

Cette loi a défini également les régimes juridiques des moyens de cryptologie. Elle donne la liberté d'utilisation des moyens et prestations de cryptologie aux personnes physiques ou morales qui en veulent : « *L'utilisation des moyens et prestations de cryptologie est libre.*[13]»

Toutefois, lorsque les moyens ou des prestations de cryptologie permettent d'assurer des fonctions de confidentialité, le principe de libre utilisation ne s'applique que s'ils s'appuient sur des « conventions secrètes »<sup>1</sup> gérées par un organisme agréé conformément à l'article 16 de

---

<sup>1</sup> Accord de volontés portant sur des clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;

la présente loi. La fourniture, l'importation et l'exportation des « moyens de cryptologie » assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont également libres.

Les prestataires de services de cryptologie doivent soumettre à la commission nationale de cryptologie les détails sur les moyens de cryptologie utilisés comme il est indiqué au niveau de l'article 14 de cette loi. *« Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un service de cryptologie tient à la disposition de la Commission nationale de cryptologie une description des caractéristiques techniques de ce moyen de cryptologie. »*

- **Les prestataires de services de cryptologie**

Comme ils gèrent les questions secrètes liées aux échanges de données des personnes ou organismes qui ont confiance en leur service, des dispositions ont été prises pour encadrer leur activité. Tout d'abord, les prestataires de services de cryptologie ont l'obligation de se déclarer auprès de la commission nationale pour que cette dernière puisse approuver leur statut de prestataires de services de cryptologie. Au cas échéant, ces services jouissent d'une légalité. Et sur ce point, la loi, au niveau de l'article 16 et 17, dit : *« Les organismes exerçant des prestations de cryptologie doivent être agréés par la Commission nationale de cryptologie. Les conditions de délivrance de l'agrément aux organismes exerçant des prestations de cryptologie ainsi que leurs obligations sont définies par décret. »*

Ils sont responsables de toutes atteintes d'intégrité aux données. Et sur ce le législateur : *« Les prestataires de services de cryptologie à des fins de confidentialité sont responsables du préjudice causé dans le cadre desdites prestations aux personnes leur confiant la gestion de leurs conventions secrètes, en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions. »*

Les prestataires de services de cryptologie sont responsables vis-à-vis des personnes qui se sont raisonnablement fiées à leur produit, du préjudice résultant de leur faute intentionnelle ou de leur négligence. » Donc tout ceux envisagent de fournir des services en ce sens doivent scrupuleusement tenir en compte de cela.

À défaut du respect des dispositions émanant de cette loi, des sanctions ont été prévues en l'encontre de ces prestataires de services de cryptologie. Ces sanctions sont de la prérogative de la commission nationale de cryptologie. Les sanctions administratives prévues sur cette loi sont définies comme suit :



- Lorsqu'un prestataire de services de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujéti en application de la présente loi, la commission nationale de cryptologie peut, après audition de l'intéressé, prononcer :
  - ✓ l'interdiction d'utiliser ou de mettre en circulation le moyen de cryptologie concerné ;
  - ✓ le retrait provisoire de l'autorisation accordée, pour une durée de trois (3) mois ;
  - ✓ le retrait définitif de l'autorisation ;
  - ✓ des amendes dont le montant est fixé en fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements.

Maintenant que nous avons évoqué la signature électronique de façon définitoire, mais aussi son rôle sur un document. Et en fin, expliciter les caractéristiques sur lesquelles elle s'est fondée, nous présentons, les intérêts des collectivités locales sur l'utilisation de la signature électronique.

## **IV. Intérêt à utiliser la signature électronique dans l'administration au Sénégal**

Sans la signature électronique, nous ne pouvons pas bénéficier de tous les atouts de la dématérialisation. Ainsi, la Comité Ouest Africain d'Organisation et de Normalisation Bancaire et Financière énonce que : La signature électronique permet de parachever le processus de dématérialisation des documents en garantissant l'authentification de l'auteur du message, son intégrité et sa non répudiation. En effet, sans celle-ci, pour signer un document, qui doit constituer un élément lors d'une procédure dématérialisée, nous sommes obligés d'avoir le document physique concerné pour pouvoir apposer notre signature. Et ceci implique le retour aux pratiques classiques, comme je l'ai souligné au niveau des points précédents.

Nous avons plusieurs aspects qui constituent un intérêt pour les municipalités à adopter la signature électronique pour signer les actes (de naissance, de mariage, etc.).

### **IV.1 Politique générale de l'État**

#### **IV.1.1 Signature électronique dans l'administration centrale : projet de l'État du Sénégal sur le numérique – place de la signature numérique**

L'État, dans le cadre du plan Sénégal émergent, a adopté en 2016 la stratégie numérique 2025. La Stratégie Sénégal Numérique 2025 est un projet du ministère de l'Économie numérique et des Télécommunications. Les objectifs stratégiques de ce projet reposent sur plusieurs axes stratégiques fondamentaux. Et parmi les axes stratégiques de ce projet, nous avons[14, p. 6] :

- **le cadre juridique et institutionnel** : Il s'agit la mise en niveau du cadre juridique du secteur des télécommunications et des TIC et améliorer la cohérence et l'efficacité de la gouvernance institutionnelle ;
- **Une administration connectée au service du citoyen et des entreprises** : Afin d'améliorer l'efficacité et la synergie dans les services publics, l'administration sera connectée pour mieux satisfaire les usagers, avec la dématérialisation des procédures administratives, plus de productivité avec une réduction des coûts et des délais des transactions et opérations administratives. L'objectif étant de rapprocher l'administration des usagers dans leurs localités respectives.

De plus, l'État du Sénégal engagera la numérisation des grands registres (des personnes physiques, des personnes morales et du patrimoine géoréférencé) et l'implémentation des projets numériques emblématiques (référentiel biométrique des personnes physiques, cadastre numérique national, plan d'adressage national), pour donner une véritable impulsion à la dématérialisation intégrale de l'administration publique[14, p. 33].

L'administration électronique a marqué des progrès appréciables, avec des initiatives portées sur l'informatisation des procédures administratives. Le lancement de quelques téléprocédures d'utilité publique reconnue telles que : Télédac (permis de construire), Etax (Téléprocédures fiscales) et Campusen (orientation des nouveaux bacheliers) ; cela indique la nouvelle approche d'un citoyen perçu comme un « client » des services de l'État. Il faut souligner l'impact grandissant des processus de dématérialisation dans le domaine de la douane et du commerce extérieur avec les applications ORBUS et GAINDE[14, p. 16].

- **la confiance numérique** : Ce point s'active au renforcement du cyber sécurité nationale et assurer la coordination des interventions dans le domaine du cyber sécurité. Pour mieux

promouvoir l'usage des transactions numériques sécurisées, vulgariser la signature électronique et instaurer la confiance numérique dans le cyberspace, 10.000 certificats électroniques seront également délivrés par an[14, p. 28]. Ce point prend en compte donc la signature électronique qui assure l'intégrité l'authentification des documents électroniques.

#### **IV.1.2 Signature électronique dans l'administration local : l la gestion des actes d'état civil : place de la signature électronique**

La dématérialisation vise à permettre aux citoyens de faire leurs démarches administratives en ligne d'une part, et d'autre part aux administrations de traiter informatiquement les demandes. Elle contribue ainsi à la promotion d'une administration électronique, accessible, efficace et sécurisée au service du citoyen[15].

Cependant dans l'administration locale comme les municipalités, l'automatisation des procédures pour la demande d'actes d'état civil n'existe pratiquement pas. Par exemple pour l'obtention d'un acte d'état civil, il n'y a pas de téléprocédures pour faire la demande à distance. Toutefois certaines mairies ont commencé la génération automatique d'acte d'état civil ce qui constitue un pas vers la dématérialisation des procédures pour l'obtention de ces documents.

Cela montre que l'État du Sénégal est dans une dynamique de transformation vers le numérique. Ces projets rentrent dans le cadre l'amélioration de l'efficacité du fonctionnement de l'administration et de la qualité du service public rendu aux usagers. De ce fait, c'est aussi aux mairies, qui représentent l'administration locale, vont élargir cette politique de l'état au niveau des collectivités territoriales.

#### **IV.2 Besoin social et modernisation de l'administration au niveau des municipalités**

La population fonce de plus en plus à l'usage intensif des réseaux d'information et de la technologie de l'information. Ce qui fait que, l'utilisation de services dématérialisés peut être beaucoup plus efficace et rentable, dans le cadre de leur activités. Encore que, les usagers, qui font des demandes de documents administratifs au niveau des mairies, ont parfois besoins de déposer ces documents dans d'autres structures. Au cas échéant, les dépôts se font souvent en

ligne donc l'obligation d'avoir le document numérique s'impose. Ainsi, remettre aux usagers des documents nativement électronique est la meilleure approche pour rendre un service de qualité au public cible.

Vu cette dynamique de la société, les mairies, pour une bonne gouvernance locale, devons être à jour sur des questions qui impactent sur les activités de leur population surtout en matière de technologie de l'information. Et la signature électronique pour authentifier un document administratif est une des modernités que toutes les administrations de manière générale, doivent intégrer dans leur système d'information.

### **IV.3 La sécurité des documents**

Avec le développement des échanges numériques le recours à des produits de sécurité s'impose pour garantir la fiabilité et préserver la confidentialité. Des produits de sécurité ont été élaborés en parallèle, contre les intrusions, les virus...mais aussi pour garantir, en messagerie électronique, la fiabilité des messages[16].

Ainsi, la signature électronique assure la sécurité des données que nous partageons sur internet et au niveau de l'informatique de manière générale. Elle repose sur l'utilisation de clés publiques et privées et des procédés cryptographiques complexes afin de garantir un niveau de sécurité et une confiance maximale de l'utilisateur. En matière de signatures, l'authenticité et la sécurité sont des priorités. Grâce au cryptage, nous avons la garantie que le document reste inchangé après sa signature.

Et avec une signature numérique, nous sommes à chaque fois sûr de signer l'intégralité des documents. Il n'y a aucun risque que certaines pages soient ajoutées ou supprimées par la suite. En réalité, l'aspect sécurité constitue le centre névralgique sur l'utilisation de la signature électronique dans les transactions électroniques. D'ailleurs, en se référant sur les objectifs de la signature électronique, nous voyons que la sécurité fait partie des finalités de la mise en place d'une solution de signature électronique.

### **IV.4 Efficacité**

La signature électronique est beaucoup plus rapide que la signature manuscrite : quelques secondes suffisent pour signer des documents. Par ailleurs, il est plus rapide de transmettre des

documents par voie numérique, par e-mail ou via des services de partage de fichiers[17]. Ceci permettra aux municipalités d'effectuer un gain de temps.

La technologie de signature électronique apporte plus de flexibilité et de souplesse lors de la signature des documents par rapport à la signature manuscrite classique. Quel que soit l'endroit où vous vous trouvez et même en déplacement, vous pouvez aisément formaliser vos accords instantanément[18].

En plus, et pour rendre beaucoup plus flexible le travail des agents et de son personnel de façon générale, les mairies pourront adopter le télétravail. Et la pandémie du covid-19 a montré que nous devons l'intégrer dans nos activités.

## **IV.5 Rentabilité**

Les administrations recherchent toujours des astuces pour la réduction de leurs dépenses. Cependant au niveau les mairies, les cartouches d'encre et le papier d'impression ont un coût non négligeable. Avec l'utilisation de la signature électronique, ils pourront éviter ces dépenses.

## **IV.6 L'archivage numérique**

Avec la dématérialisation, la majeure partie des documents produits et échangés dans le cadre de l'activité des entreprises et des administrations sont nativement sous format électronique.

Le cycle de vie de ces documents inclut leur création, leurs évolutions, leur validation, éventuellement leur signature, leur envoi aux destinataires . . . mais ne s'arrête pas une fois le document transmis. La plupart d'entre eux revêtent une importance sur le long terme, de par[11, p. 235] :

- leur valeur juridique (contrats, commandes, factures, fiches de paie, ordres de mission, traces applicatives . . .) ;
- leur contenu technique et informationnel (spécifications, brevets . . .) ;
- leur valeur patrimoniale (articles, notes professionnelles . . .).

Ainsi, même à l'issue de son utilité immédiate au sein du projet qui a motivé sa création, un document doit être conservé dans des conditions qui permettront de le retrouver a posteriori,

éventuellement de nombreuses années plus tard, dans le cadre de besoins qui sont ou non prévisibles lors de sa génération.

En résumé, la signature électronique offre ces possibilités aux municipalités :

- la possibilité de signer un document sans l'imprimer, et par conséquent effectuer une économie de papier ;
- la possibilité d'envoyer le document par email économie de timbre ;
- la possibilité de signer un document sans se rencontrer, En effet, elle permet à deux parties concernées de donner leurs accords sans se rencontrer physiquement, ainsi elle offre une réduction considérable des déplacements ;
- la possibilité de conserver le document au format numérique, en effet la conservation du document au format numérique nous permet de consulter nos documents sur n'importe quel appareil, et procure la simplification et suppression de l'archivage papier ;
- ... ;

Les véritables gains issus de l'usage de la signature électronique viennent de la refonte en profondeur des processus métier liés à la génération, au traitement et à la conservation des documents.

Voici un tableau récapitulatif montrant les bénéfices qui peuvent être induits par l'usage de la signature électronique.

**Tableau 1:** *Récapitulation des opportunités de la signature électronique*

Opportunités	Description
<b>Gain de temps et d'efficacité</b>	<ul style="list-style-type: none"> <li>● Simplification des démarches administratives ;</li> <li>● Vérification de l'authenticité des documents ;</li> <li>● Diminution des manipulations administratives : amélioration du suivi des dossiers ;</li> <li>● Traçabilité.</li> </ul>
<b>Gain de place</b>	<ul style="list-style-type: none"> <li>● Réduction de l'espace dévolu au stockage et à l'archivage ;</li> <li>● Diminution de l'utilisation du papier.</li> </ul>
<b>Accessibilité</b>	Possibilité d'accéder aux documents en tout temps et en tous lieux à condition de bénéficier d'une connexion Internet.

<b>Collaboration</b>	<ul style="list-style-type: none"> <li>• Partage de document ;</li> <li>• Procédure de classement simplifiée ;</li> <li>• Facilite les interactions entre collègues ;</li> <li>• Dynamise les flux.</li> </ul>
<b>Réduction des risques de perte de dossiers</b>	Réduction du risque de perte des dossiers, notamment des originaux et de destruction des dossiers (feu/inondation/vol).

## Conclusion

En résumé, au regard des disposition des juridiques des lois sur la cryptologie et les transactions électroniques et, de leurs décrets d'applications, le Sénégal a bâti un arsenal juridique solide pour la mise en œuvre des techniques cryptographiques comme la signature électronique.

Cependant par rapport à l'évolution rapide des technologies et des mutations fréquents qui agitent la société de l'information et de la connaissance, la mise à jour de ces dispositions juridiques est fondamentale.

Au Sénégal, des projets de dématérialisation de procédures ont été réalisés dans plusieurs domaines comme par exemple le service « teledac » pour le retrait de diplôme de baccalauréat. Malgré ces efforts fournis en matière de dématérialisation de procédures, on n'arrive pas jusqu'à présent à régler les problèmes d'accessibilité aux services d'état civil.

Ainsi pour recommandations, nous devons revoir le système juridique qui encadre les systèmes cryptographiques au Sénégal. Ensuite exposer les procédures à suivre pour se doter de ces outils.

Par ailleurs nous devons aussi mettre en place une écosystème puissant et efficace qui permettrait l'intégration facile de la signature électronique, même pour les structures qui ont des revenus moins.

Cela étant fait nous pourrons passer à la dématérialisation complète de procédures comme le retrait des attestions des étudiants, des diplômes de baccalauréat, etc.

Pour accélérer et favoriser le développement de nouvelles applications et e-services autour des transactions électroniques, la sécurité devient alors une priorité[19]. Ainsi, plusieurs mécanismes et techniques ont été mise en place pour satisfaire ce besoin capital. C'est d'ailleurs ces techniques qui sous-tendent et rendent possible la signature électronique.



# Chapitre 3 : Méthodes et Approches pour la Signature Électronique

## Introduction

Dans cette partie, nous décrirons les mécanismes et procédés de chiffrements. Nous allons aussi aborder les fonctions de hachage et les infrastructures de gestion de clés basés sur les certificats et les autorités de certification. Nous verrons aussi la signature électronique de documents électroniques au format PDF.

### I. La cryptographie

Le mot **cryptographie** est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe « **crypter** » est parfois utilisé mais on lui préférera le verbe « **chiffrer** ». La cryptologie est essentiellement basée sur l'arithmétique. Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour [20, p. 91] :

- les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé **cryptogramme** par opposition au message initial, appelé **message en clair** ;
- faire en sorte que le destinataire saura les déchiffrer. Le fait de coder un message de telle façon à le rendre secret s'appelle **chiffrement**. La méthode inverse, consistant à retrouver le message original, est appelée **déchiffrement**.

La cryptographie est la pratique de la protection des informations par l'utilisation d'algorithmes codés, de hachages et de signatures. Les informations peuvent être au repos (comme un fichier sur un disque dur), en transit (comme une communication électronique échangée entre deux ou plusieurs parties), ou en cours d'utilisation (lors de l'utilisation de données)[21].

L'objectif fondamental de la cryptographie est de permettre à deux personnes, appelées traditionnellement Alice et Bob de communiquer à travers un canal peu sûr de telle sorte qu'un opposant, Oscar, qui a accès aux informations qui circulent sur le canal de communication, ne puisse ni comprendre et/ou modifier ce qui est échangé, ni se faire passer pour Alice ou Bob. Le canal peut être par exemple une ligne téléphonique ou tout autre réseau de communication.

Les communications échangées entre Alice et Bob sont sujettes à un certain nombre de menaces. La cryptographie apporte des fonctionnalités permettant de répondre à ces menaces, résumées dans l'ensemble confidentialité, authentification, intégrité, non-répudiation :

- **Confidentialité** des informations stockées ou manipulées par le biais des algorithmes de chiffrement. La confidentialité consiste à garantir que seules ont accès aux informations les personnes autorisées à les connaître ou, en d'autres termes, à empêcher l'accès aux informations à ceux qui n'en sont pas les destinataires. Ils peuvent lire les messages chiffrés transmis sur le canal mais ne doivent pas pouvoir accéder à leurs contenus ;
- **Authentification** des protagonistes d'une communication. L'authentification a pour but de valider l'identité d'une personne ou de détecter une usurpation d'identité, afin d'avoir la garantie que la personne est bien celle qu'elle prétend être. Le terme « authentification » est également utilisé pour désigner la vérification de l'origine de données reçues (aussi appelée « preuve d'origine »). Par exemple, Alice peut s'authentifier en prouvant à Bob qu'elle connaît un secret  $S$  qu'elle est la seule à connaître ;
- **Intégrité** des informations stockées ou manipulées. L'intégrité a pour but de vérifier que le message n'a pas subi d'altérations lors de son parcours. Cette vérification concerne par exemple une potentielle modification ou substitution volontaire et malicieuse de l'information provoquée par un tiers lors du transfert sur un canal de communication. Ces modifications sont en général masquées par le tiers pour être difficilement détectables ;
- **Non-répudiation** des informations. C'est une protection entre les protagonistes d'un échange, et non plus contre un tiers. Si Alice envoie un message  $M$ , elle ne doit pas pouvoir prétendre ensuite devant Bob qu'elle ne l'a pas fait, ou alors qu'elle a envoyé  $M_2$  et que le message a été mal compris et réciproquement. Techniquement, il s'agit souvent d'une combinaison d'authentification et d'intégrité prouvable à un tiers, par

exemple un magistrat. C'est pour cela que des algorithmes asymétriques sont aujourd'hui indispensables[22, p. 4].

Ces quatre services sont les principales propriétés de sécurité nécessaires dans les communications sécurisées.

Sur la base de ces objectifs, elle permettra d'inventer des « coffres-forts » numériques que l'utilisateur peut laisser traîner sans problème sur le « cloud » ouvert à tous les espions. Ensuite, remplacer tous les procédés autrefois mis en œuvre sur papier par leurs équivalents numériques[23].

La cryptographie utilise un certain nombre d'algorithmes cryptographiques pour atteindre un ou plusieurs de ces objectifs de sécurité de l'information. Ces outils comprennent des algorithmes de chiffrement, des algorithmes de signature numérique, des fonctions de hachages.

Par ailleurs, la mise en place d'une solution de signature électronique devient chaotique au cas nous ne maîtrisons pas les notions de base de cryptographie. Nous allons maintenant aborder les trois grandes familles : la cryptographie symétrique, la cryptographie asymétrique et les fonctions de hachages.

## **I.1 La cryptographie symétrique**

La cryptographie symétrique, ou cryptographie à « clé secrète »<sup>1</sup>, sert à garantir la confidentialité des données par le mécanisme appelé « chiffrement »[11, p. 32]. Donc la cryptographie symétrique s'appuie sur le mécanisme de chiffrement symétrique.

Le chiffrement est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire. Le déchiffrement est l'opération qui permet de restaurer le message original à partir du message chiffré[24].

---

<sup>1</sup> Clé non publiée mais utilisée uniquement en cryptographie symétrique et nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de déchiffrement.

Un système symétrique peut être vu comme un coffre-fort, ou comme une boîte munie d'un cadenas. Alice introduit son message dans le coffre, l'envoie à Bob qui l'ouvre avec sa clé. Alice et Bob doivent donc partager la même clé[25, p. 99].

La clé<sup>1</sup> est une donnée particulièrement sensible. C'est sur son secret que repose la confidentialité des messages. Si elle venait à être divulguée, un espion aurait sans problème accès au message. Le transport sécurisé des clés est un élément crucial pour la sécurité du chiffrement symétrique

L'algorithme actuellement recommandé pour le chiffrement symétrique s'appelle AES[11, p. 32].

Le fonctionnement général de la cryptographie symétrique est illustré par la figure 4 :

- l'émetteur d'une donnée secrète génère une clé symétrique ;
- il l'utilise pour chiffrer la donnée secrète ;
- il transmet à son correspondant la donnée secrète chiffrée et la clé symétrique ;
- le correspondant se sert de la clé symétrique pour déchiffrer la donnée secrète et en prendre connaissance.

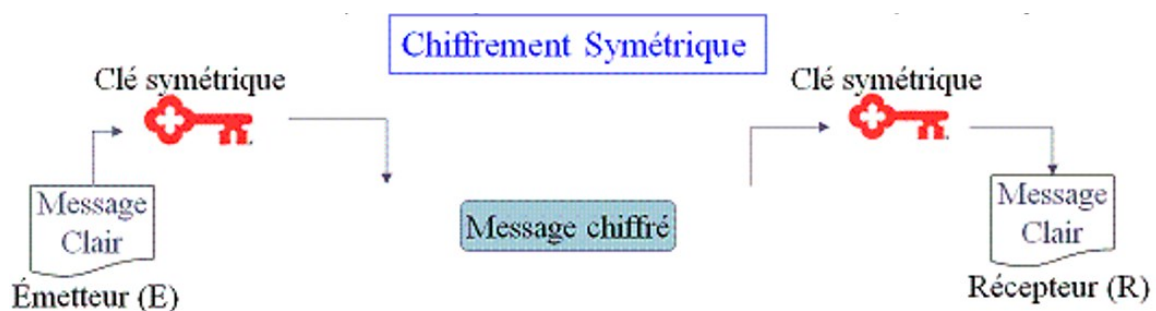


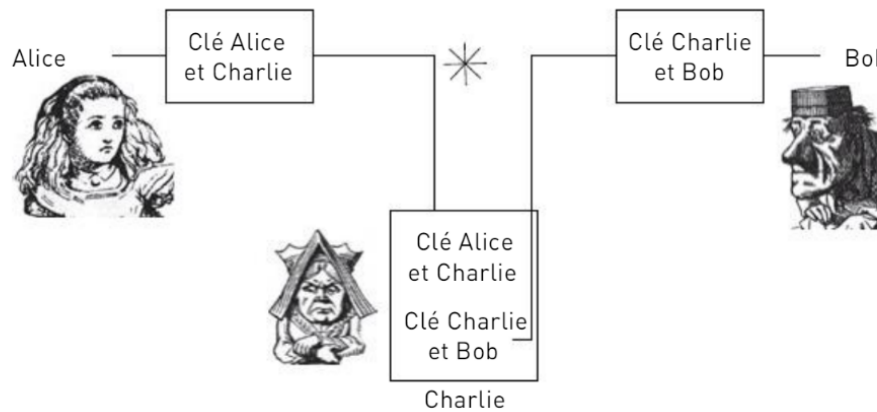
Fig. 2 : Schéma de fonctionnement de la cryptographie symétrique[24]

En plus d'assurer la confidentialité des communications, les systèmes symétriques bénéficient d'une rapidité considérable, ce qui constitue une caractéristique importante sur la performance du système.

---

<sup>1</sup> Ensemble de caractères, de chiffres, avec une longueur spécifiée, destiné à chiffrer, à déchiffrer, à signer et à authentifier une signature

Cependant, le grand problème des systèmes symétriques est la distribution des clés : comme le montre le schéma, les clés doivent être échangées sur un canal sécurisé. En effet, au cas où le canal par lequel la clé secrète transite, n'est pas hautement sécurisé, un espion peut l'intercepter et se faire passer pour l'un des communicateurs.



*Fig. 3 : Interception de la clé secrète par un espion[25, p. 101]*

En fait, Alice, en voulant communiquer avec Bob, Charlie intercepte la clé secrète et se fait passer pour Bob auprès d'Alice et pour Alice auprès de Bob

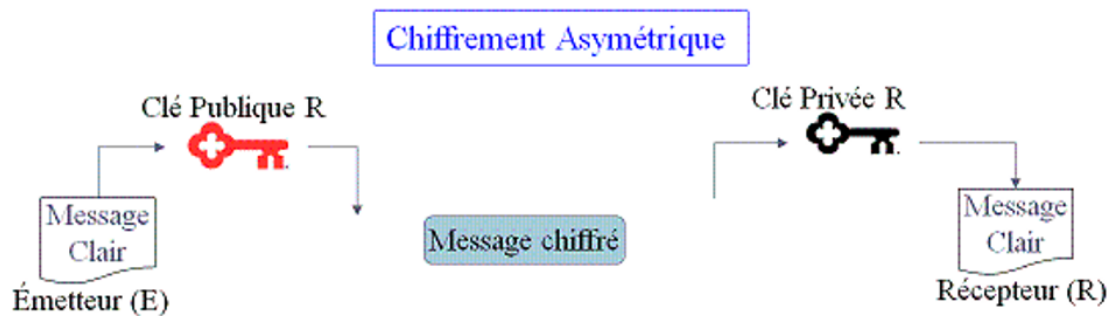
En plus de la cryptographie symétrique, nous avons aussi un autre système de chiffrement qui est la cryptographie asymétrique.

## **I.2 La cryptographie asymétrique**

Un cryptosystème à clé publique, dit aussi « système asymétrique », compte deux clés : l'une publique pour chiffrer le message, l'autre privée pour déchiffrer le message. Il est pratiquement impossible de calculer l'une à partir de l'autre[25, p. 103].

La cryptographie asymétrique ou cryptographie à clé publique fonctionne de façon totalement différente à la cryptographie symétrique. Si l'on peut comparer la cryptographie symétrique à un coffre-fort auquel seules les personnes possédant la clé peuvent accéder, la cryptographie asymétrique pourrait être comparée à une boîte aux lettres dans laquelle on peut déposer des informations, et seule la personne possédant la clé peut accéder au contenu de la boîte. La boîte aux lettres serait la clé publique (donc accessible à tout le monde), alors que la

clé pour ouvrir la boîte serait la clé privée. En effet, dans la cryptographie asymétrique, il y a une clé publique<sup>1</sup> et une clé privée<sup>2</sup>[23, p. 21].



*Fig. 4 : Schéma de fonctionnement de la cryptographie asymétrique [24]*

L'utilité fonctionnelle de la cryptographie asymétrique, illustrée par la figure 6, est la suivante :

- un individu (le « porteur ») doit être capable de faire un calcul que lui seul est capable de réaliser : pour cela, il doit disposer d'un secret ;
- un autre individu (le correspondant) doit être capable de vérifier le calcul pour s'assurer que le porteur dispose de ce secret, mais sans en disposer lui-même.

Ils reposent sur deux données complémentaires, liées mathématiquement et générées conjointement, mais gérées de manière très différente :

- la « clé privée » constitue le secret que le porteur doit conserver confidentiel, et qu'il utilisera pour effectuer l'opération de chiffrement ;
- la « clé publique » est son pendant mathématique, qui permet d'effectuer le calcul inverse, et donc de vérifier que la personne qui a fait le calcul initial possédait bien la clé privée.

La clé publique peut être diffusée largement, et transmise librement à toute personne appelée à l'utiliser. Bien entendu, la connaissance de la clé publique ne permet pas de déduire

<sup>1</sup> Clé utilisée en cryptographie asymétrique publiable et nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement et de déchiffrement

<sup>2</sup> Clé non publiable utilisée en cryptographie asymétrique et associée à une clé publique

la clé privée. La sécurité de la cryptographie asymétrique repose entièrement sur cette propriété mathématique.

Le RSA est sans doute le plus utilisé des procédés à clé publique[26, p. 54].

La cryptographie asymétrique présente quelques avantages :

- plus de clé partagée, avec la crainte que le correspondant trahisse un jour le secret ;
- le nombre de clés nécessaires au fonctionnement du système est réduit ;
- la clé privée est en principe fortement liée à l'identité de son propriétaire[25, p. 105].

Toutefois elle connaît deux limites principales.

Tout d'abord, les données que l'algorithme RSA peut accepter en entrée sont limitées à la taille de la bi-clé<sup>1</sup>.

Si l'on utilise une bi-clé de 2 048 bits, cela veut dire que l'on ne peut pas signer ou chiffrer avec l'algorithme RSA un fichier de plus de 256 caractères . . . Voilà qui risque de mettre fin rapidement à notre intérêt pour RSA . . . Sauf à trouver des solutions !

Ensuite, les performances de la cryptographie asymétrique sont assez mauvaises en termes de vitesse de réalisation. Générer des bi-clés est consommateur de ressources, et les utiliser pour effectuer des calculs RSA également. Il faut donc limiter l'usage de la cryptographie asymétrique à des opérations peu nombreuses[11, p. 31].

Le cryptage asymétrique est trop lent, et le cryptage symétrique n'est pas sûr car il faut que l'expéditeur envoie sa clé au destinataire, ce qui est beaucoup trop risqué sur certains réseaux (comme Internet). Pour combler ces limites des deux systèmes de chiffrement, une solution est apportée : l'utilisation conjointe de la cryptographie symétrique et de la cryptographie asymétrique qu'on appelle communément la cryptographie hybride.

### **I.3 La cryptographie hybride**

C'est un mélange des deux types de cryptographie précédents. Un message est chiffré par la méthode symétrique à l'aide d'une clé secrète, puis cette clé est chiffrée à son tour par la

---

<sup>1</sup> Couple clé publique/clé privée utilisé dans des algorithmes de cryptographie asymétrique

méthode asymétrique, puis envoyée au destinataire. Le destinataire commence par déchiffrer la clé et ensuite utiliser cette clé pour déchiffrer le message[27, p. 2].

Dans cette technique, deux mécanismes sont mis en œuvre conjointement pour le chiffrement et le déchiffrement des données.

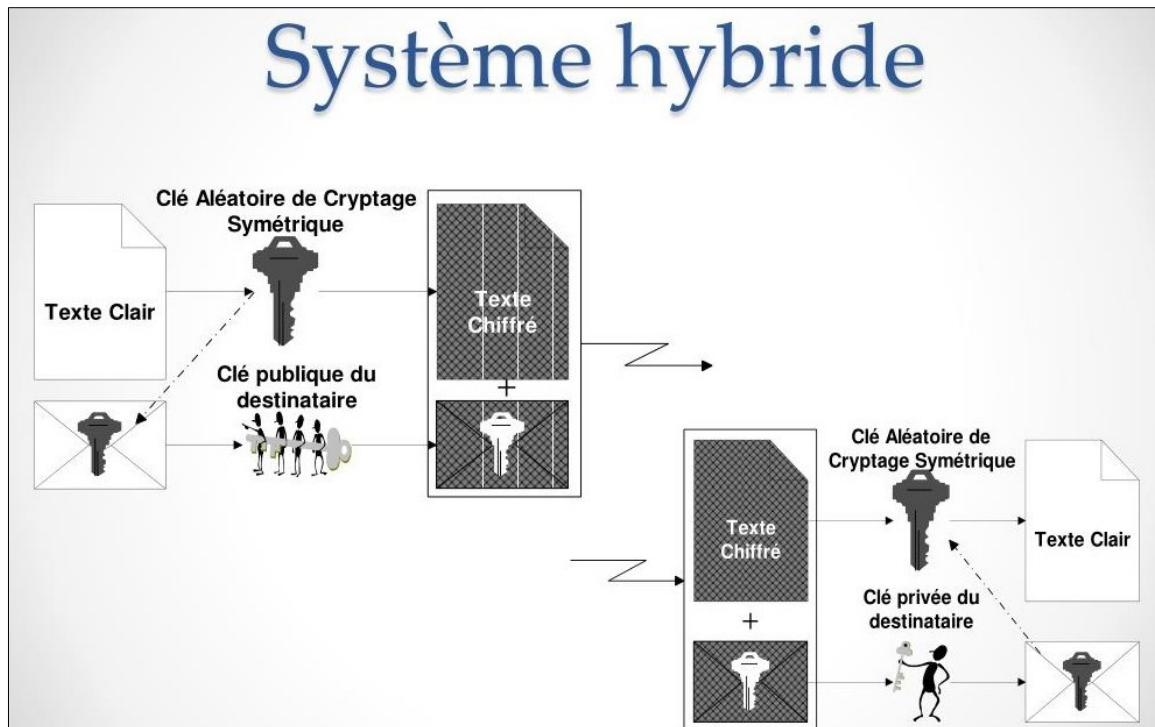
- **L'opération de chiffrement**

- ✓ L'émetteur de la donnée confidentielle génère une clé de chiffrement symétrique, sous la forme d'une suite aléatoire de bits.
- ✓ L'émetteur chiffre les données confidentielles à l'aide de la cryptographie symétrique, en employant l'algorithme AES et la clé qu'il vient de générer.
- ✓ L'émetteur se procure la clé publique du destinataire.
- ✓ L'émetteur chiffre la clé symétrique qu'il a générée lors de la première étape à l'aide de la cryptographie asymétrique, en employant l'algorithme RSA et la clé publique du destinataire.
- ✓ La donnée chiffrée et la clé de déchiffrement elle-même chiffrée sont réunies dans une « enveloppe », que l'émetteur peut transmettre au destinataire.

- **L'opération de déchiffrement**

- ✓ Le destinataire reçoit l'enveloppe chiffrée ; il en extrait la clé chiffrée et les données chiffrées.
- ✓ Le destinataire déchiffre la clé symétrique à l'aide de la cryptographie asymétrique, en employant l'algorithme RSA et sa propre clé privée.
- ✓ Le destinataire déchiffre les données à l'aide de la cryptographie symétrique, en employant l'algorithme AES et la clé symétrique qu'il vient de déchiffrer. Il a alors accès aux données en clair.





*Fig. 5 : Schéma de fonctionnement de la cryptographie hybride [28]*

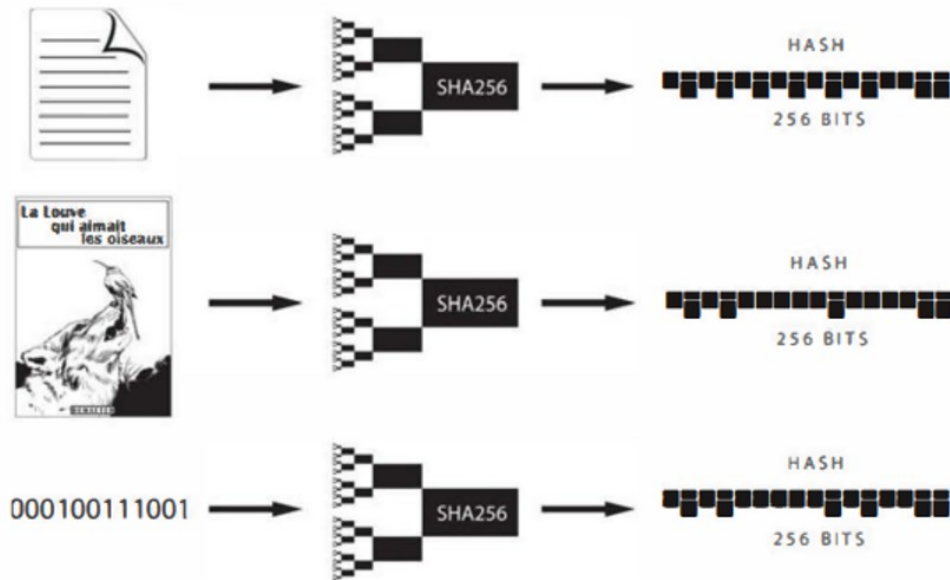
Ainsi, l'utilisation successive des deux types de cryptographies permet [11, p. 147] :

- de résoudre le problème posé par la cryptographie symétrique : celui du partage de la clé secrète entre l'émetteur et le destinataire ;
- de résoudre le problème posé par la cryptographie asymétrique : la taille limitée des données que l'on peut chiffrer. En effet, ici, on ne chiffre qu'une clé, qui est de petite taille.

Après avoir survoler les concepts et fonctionnement de la cryptographie symétrique comme asymétrique, nous précisons que celles-ci n'assurent que la confidentialité des données échangées mais ne garantissent pas l'intégrité des données. C'est ainsi que les fonctions de hachages sont mises en place pour assurer cette fonctionnalité.

## I.4 Les fonctions de hachages

Les fonctions de hachages sont des fonctions à sens unique et « sans collision », générant une sortie de taille fixe (appelée condensat ou empreinte), caractéristique des données fournies en entrée [7]. Les fonctions de hash sont des algorithmes mathématiques qui prennent en entrée une donnée qui peut avoir n'importe quelle taille, et qui rendent en sortie une chaîne d'octets de longueur fixe qui dépend de chacun des bits de l'entrée mais ne permet pas de retrouver l'entrée.

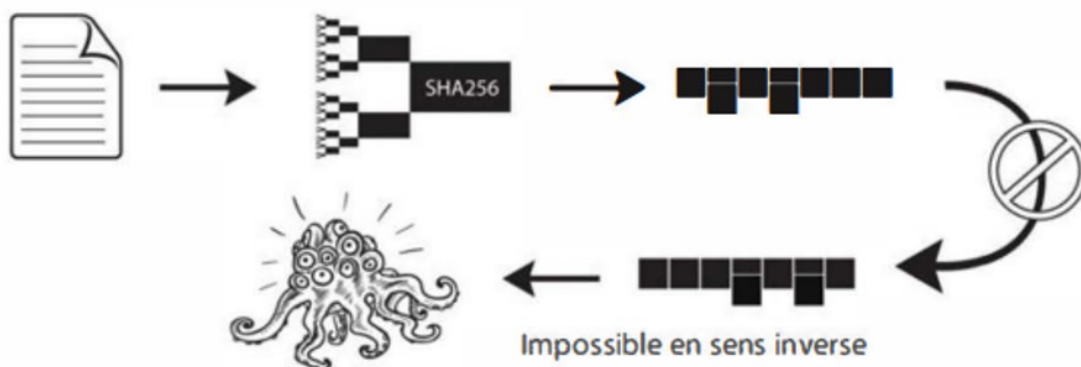


*Fig. 6 : la taille de l'empreinte est constante[11, p. 25]*

La fonction de hachage peut être classée en hachage sans clé et hachage avec clé. La fonction de hachage sans clé n'a pas de clé, telle que MD5, SHA-1, SHA-2 et SHA-3, généralement utilisée pour assurer l'intégrité et l'authentification des données. La fonction de hachage avec clé prend deux entrées : message et clé secrète, et est pratique pour les protocoles de sécurité de la couche transport[29].

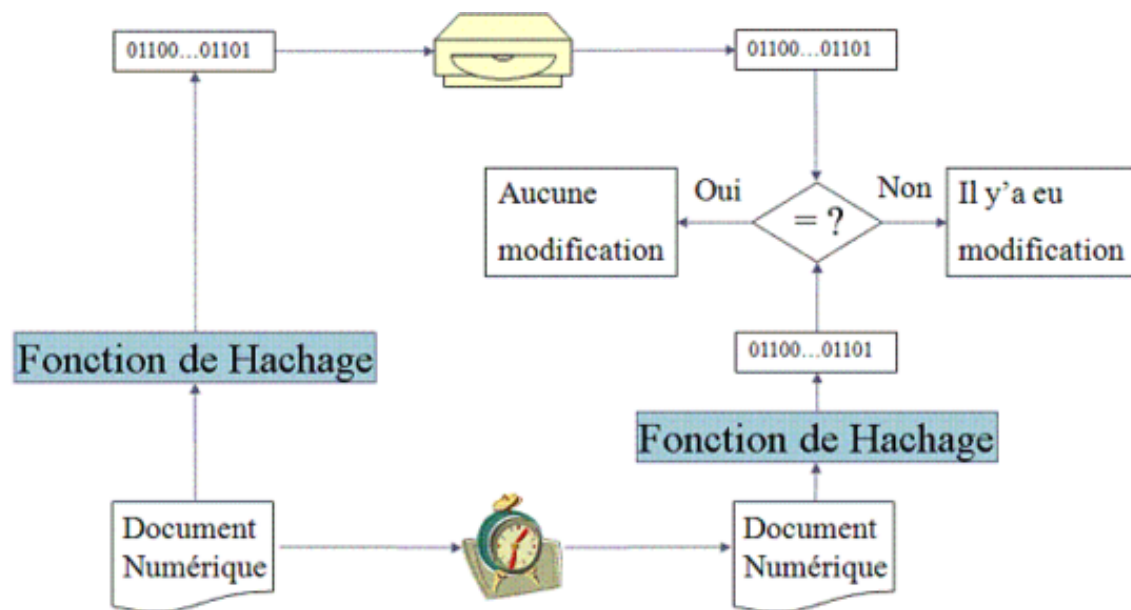
Les fonctions de hachage ont les propriétés suivantes[26, p. 58] :

- l'empreinte d'un message doit être calculable de manière efficace ;
- une fonction de hachage doit être à sens unique. Pour presque toute empreinte, il ne doit pas être possible de trouver un message lui correspondant. Les seules valeurs pour lesquelles cela doit rester possible sont les empreintes de messages déjà calculées ;



*Fig. 7 : Le hash est une fonction à sens unique [11, p. 26]*

- une fonction de hachage doit aussi résister au second antécédent. Pour un message **m** donné ayant pour empreinte **h**, il ne doit pas être possible de trouver un second message **m<sub>1</sub>** ayant la même empreinte que **m** ;
- enfin, une fonction de hachage doit résister aux collisions, ce qui signifie qu'il doit être pratiquement impossible de trouver deux messages ayant la même empreinte.



*Fig. 8 : Schéma de fonctionnement des fonctions de hachage [24]*

Les fonctions de hachage cryptographique sont un élément fondamental de la sécurité de l'information et sont utilisées dans de nombreuses applications et protocoles de sécurité tels que la signature électronique, l' HMAC et la blockchain pour garantir l'intégrité et l'authentification des données [29].

Les fonctions de hachage permettent d'assurer, au niveau des systèmes cryptographiques, l'intégrité des informations échangées.

Parfois, les données échangées sont de très grandes tailles, pour réduire la taille des données, on les applique à une fonction de hachage, ce qui produit une sortie de taille fixe puisse on la chiffre avec le mécanisme de chiffrement choisi.

Pour la mise en œuvre de la signature électronique, les systèmes de cryptographie asymétrique sont utilisés. Dans ce système de cryptographie le partage de la clé publique pose un problème. En effet, **rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est**

associée puisque un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique[20, p. 104].

## **II. La signature électronique : objet technique**

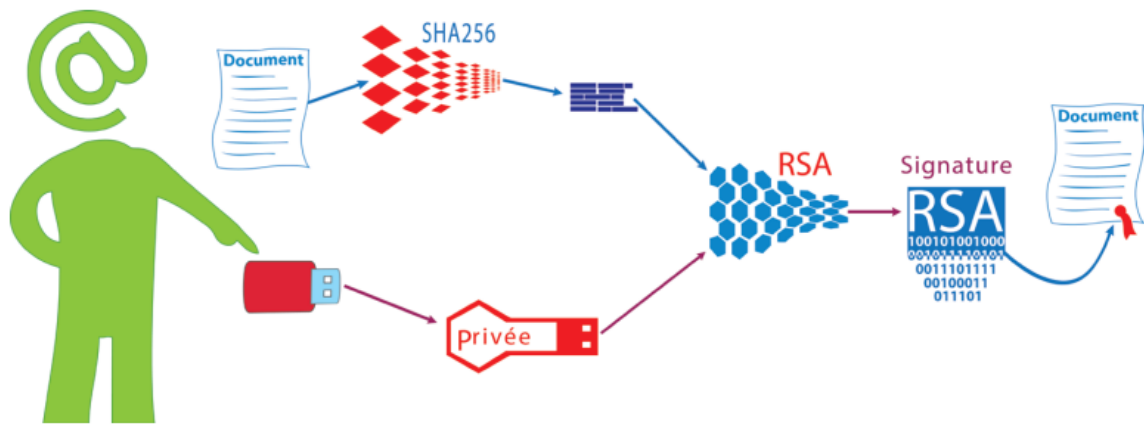
La cryptographie à clé publique rend possible l'utilisation des signatures électroniques. Celles-ci permettent de corroborer l'origine d'un message. Pour signer un message, on utilise une fonction mathématique (fonction de hachage) qui produit un résumé du message. Le résumé obtenu est chiffré à l'aide de la clé privée de l'expéditeur. Le résultat, qui constitue la signature électronique, est annexé au message. Le destinataire du message peut ensuite s'assurer l'origine du message et l'intégrité de l'information[19].

La signature numérique vient s'appuyer sur l'architecture de la cryptographie pour assurer l'aspect de la non-répudiation. Le signataire ne pourra pas désavouer, d'avoir effectué la signature. Au cas échéant des preuves sont fournies pour lui montrer qu'il est responsable de l'acte.

### **II.1 L'opération de signature**

Lorsque l'on clique sur le bouton « signer », les opérations techniques suivantes sont réalisées, conformément à l'illustration ci-dessous :

- le document à signer est haché de manière à en obtenir un condensé(SHA256) ;
- le condensé du document et la clef privée du signataire sont employés pour effectuer un calcul mathématique (RSA) : le résultat de ce calcul est, du point de vue technique, la signature électronique ;
- la signature est jointe au document, ainsi que le certificat du signataire, qui permettra sa vérification.



*Fig. 9 : Réalisation cryptographique de la signature numérique[9, p. 21]*

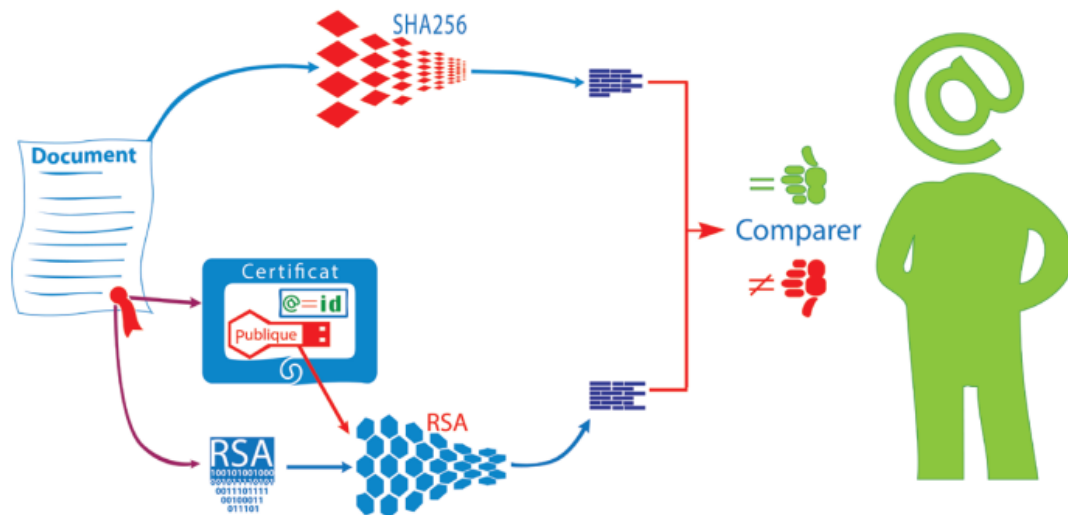
Nous pouvons aussi ajouter des éléments complémentaires dans une signature électronique comme par exemple :

- la chaîne de certification correspondante ;
- un jeton d'horodatage permettant de connaître avec certitude le moment de réalisation de la signature, et ainsi de vérifier la validité du certificat du signataire ;

## **II.2 La vérification de la signature**

La vérification technique d'une signature électronique passe par les opérations suivantes, illustrées dans la figure ci-dessous :

- le destinataire du document signé sépare le document lui-même de sa signature ;
- il extrait du certificat du signataire sa clef publique et s'en sert pour réaliser sur la signature le calcul RSA inverse : il obtient ainsi le condensé du document initialement signé ;
- il réalise à son tour le calcul du condensé du document reçu ;il compare les deux condensés ainsi obtenus : s'ils sont identiques, la signature portait bien sur le document reçu (lien avec le document), et a bien été réalisée par le porteur du certificat (lien avec l'identité du signataire).



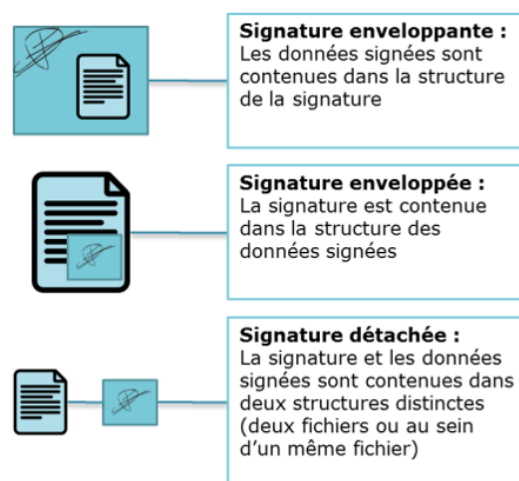
*Fig. 10 : Vérification technique de la signature électronique[9, p. 21]*

À l'issue de cette vérification, un résultat valide donne la certitude que le signataire est bien le porteur du certificat qui a été transmis avec la signature.

La vérification du certificat du signataire constitue aussi une étape très importante lors du processus de vérification de la signature électronique. À ce niveau, nous devons porter la vérification sur la validité du certificat au moment où la signature a été réalisée. Il est donc fondamental de disposer dans la signature de la date de sa réalisation.

### II.3 Les formes et formats de la signature électronique

Tout d'abord, il existe plusieurs formes de signatures différentes[10, p. 29] :



*Fig.11 : Formes de signature électronique[10, p. 29]*

- **enveloppante** : la signature contient les données signées en elle-même ;
- **enveloppée** : la signature est intégrée au document et une seule structure contient le document et la signature ;
- **détachée** : la signature et le document sont deux structures distinctes, et donc potentiellement mis dans deux fichiers différents. Dans ce cas, la signature électronique est un fichier informatique autonome, distinct du fichier d'origine. Ce fichier autonome est appelé "jeton de signature". Cette forme présente néanmoins le désavantage de devoir manipuler et conserver de façon liée deux fichiers au lieu d'un seul pour des signatures enveloppantes ou enveloppées.

Il existe aussi plusieurs formats de signature standardisés. Ces formats standards sont regroupés en trois grandes familles[11, p. 178] :

- **le format XML**

Connu sous le terme générique de XAdES. Il s'agit d'un format de stockage des signatures électroniques qui peut être indépendant des données signées (la signature constitue alors un fichier XML séparé du document signé, qui peut être à n'importe quel format), ou inclus dans le document signé si ce document est lui-même au format XML.

- **le format PKCS#7/CMS**

Connu sous le terme de CADES, permet de former des signatures détachées (la signature est dans un fichier à part, à transmettre en même temps que le document signé) ou opaque, c'est-à-dire que le document est inclus dans une « enveloppe » qui comporte aussi la signature.

Les deux options comportent des avantages et des inconvénients :

- ✓ dans le cas des signatures détachées, pour transmettre un document signé, il faut envoyer les deux fichiers simultanément ; le document initial est lisible avec le logiciel qui lui est nativement associé sans aucune manipulation ;
- ✓ dans le cas des signatures opaques, il faut disposer d'un outil pour extraire de l'enveloppe le document lorsque l'on souhaite le lire : faute de cet outil, l'enveloppe n'est pas exploitable directement, par exemple par un logiciel bureautique.

Le format CADES permet la signature multiple du même document par plusieurs signataires.

- **Le format PDF**

Connu sous le terme de PAdES, il représente le format des signatures électroniques incluses dans les documents PDF. Le format PAdES s'appuie sur le format CAdES.

Il permet la signature multiple du même document par plusieurs signataires, sous la forme de sursignatures : chaque signataire signe non seulement le document, mais aussi les signatures déjà apposées par les signataires précédents. La forme de signature d'un document PDF la plus adaptée est sans doute la forme enveloppée, si l'on souhaite que le destinataire reçoive un seul fichier lisible à partir de son lecteur traditionnel et intégrant la signature.

Pour apporter beaucoup plus de garantie sur la chaîne de communication et assurer davantage la sécurité pour le mécanisme de signature électronique, les certificats et les PKI sont utilisés à cet fin.

## **II.4 Les certificats et infrastructures de gestion des clés publiques (IGC)**

Au niveau du décret d'application de la loi n° 2008-08 du 25 janvier 2008 sur les **transactions électroniques**, le législateur précise que :

- le Sénégal a choisi d'adopter le système de la certification comme moyen privilégié d'authentification électronique des personnes et des documents ;
- l'une des composantes de ce système est la mise en place d'une Autorité de certification ;
- le présent décret apporte les précisions relatives, notamment :
  - ✓ à la gestion d'un système d'accréditation ;
  - ✓ aux conditions de délivrance d'un certificat électronique ;
  - ✓ aux obligations de l'autorité et des organismes de certification.

Donc pour la mise en œuvre d'une solution de signature électronique, s'enquérir des notions et concepts de certificat électronique est fondamental.

### **II.4.1 Les certificats**



### II.4.1.1 Notion d'un certificat

Le certificat est une attestation électronique qui lie des données afférentes à la vérification d'une signature ou de tout autre document numérique, à une personne. Le certificat confirmant l'identité d'une personne ou la conformité d'un document, est un lien entre l'entité physique et l'entité électronique[30].

Le certificat est le document émis et signé par une entité (organisme digne de confiance ou un utilisateur normal), associant une clé publique à des informations relatives au propriétaire du certificat[31].

Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé **autorité de certification**. [20, p. 105].

Ceci permettra de renforcer la confiance des usagers sur l'utilisation de clé publique dans le cadre de la vérification de la signature électronique.

Les certificats portent un certain nombre d'informations qui sont des standards adoptés par tous, mais aussi d'autres informations peuvent être rajoutées en fonction des besoins et de la législation de la zone géographique concernée.

Au Sénégal, c'est la loi sur les transactions électroniques et son décret d'application qui statue sur les certificats électroniques.

Le décret n° 2008-720 du 30 juin 2008 relatif à la **certification électronique** pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les **transactions électroniques** définit d'abord les catégories de certificat que peut émettre l'autorité de certification. Sur ce point, le législateur énumère les classes de certificat.

---

---

**Article 32.** - Les certificats que l'organisme de certification peut émettre sont classés en plusieurs catégories, notamment :

- **les certificats de classe 1** : aucun contrôle de l'identité du détenteur du certificat n'est requis ;
- **les certificats de classe 2** : l'organisme de certification effectue un contrôle sur le dossier de demande de certificat ;

- **les certificats de classe 3** : l'organisme de certification demande une vérification physique avec la présence de l'utilisateur ;
- **les certificats de classe 4** : l'organisme de certification exige la présence de l'utilisateur qui recevra son certificat sur un support physique (carte à puce ou clé USB).

L'Agence de l'informatique de l'État<sup>1</sup> peut décider, en cas de besoin, de créer d'autres catégories de certificats électroniques.

Ensuite, il précise aussi les informations que doit contenir un certificat électronique.

---

---

**Article 33.** - Tout certificat doit contenir les informations suivantes :

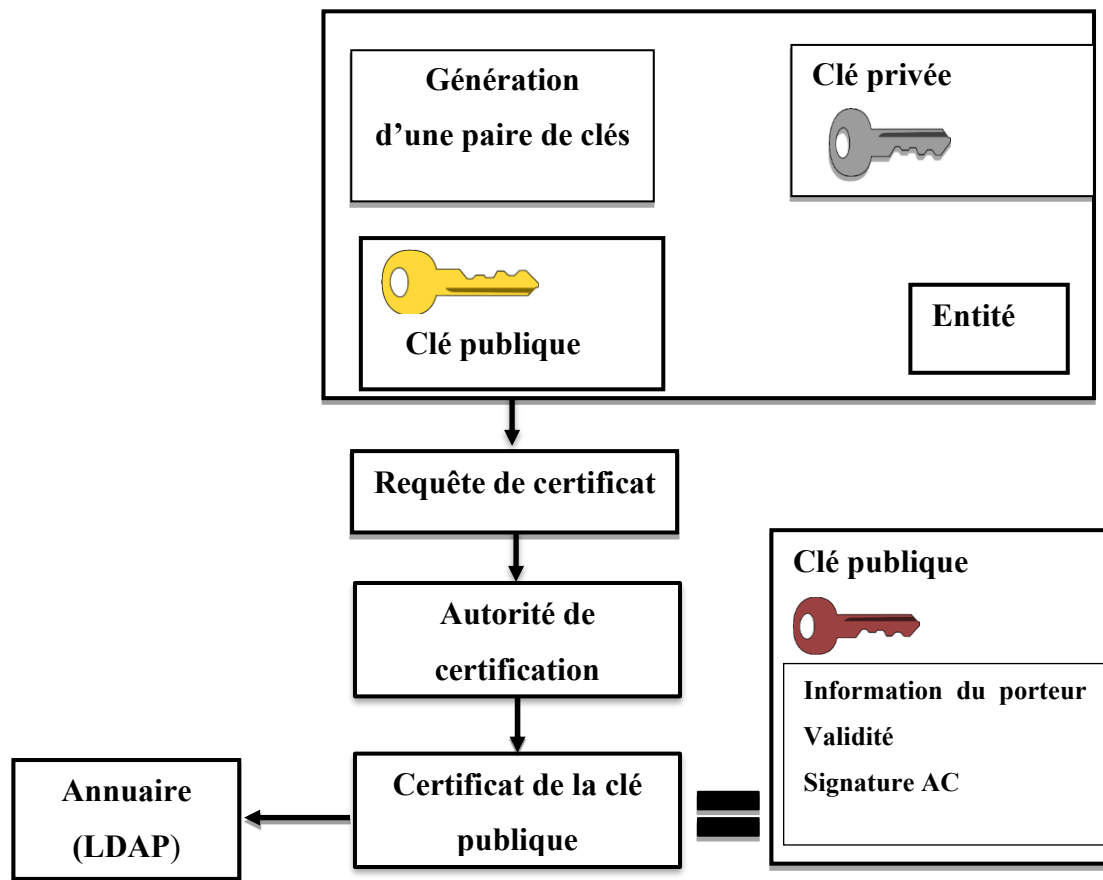
- l'identification de l'organisme de certification ;
- le nom du demandeur ou de son pseudonyme ;
- les données afférentes à la vérification de la signature ;
- la période de validité du certificat ;
- le code d'identification du certificat ;
- la qualité du demandeur du certificat ;
- l'accréditation de l'organisme de certification ;
- les limites à l'utilisation du certificat.

En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de la conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer immédiatement le certificat.

---

<sup>1</sup> L'Agence de l'informatique de l'État (ADIE) désignée actuellement par la société **Sénégal Numérique SA**

**Article 34.** - Toute publication d'un certificat électronique est soumise au consentement de son titulaire.



*Fig. 12 : Principe de la création des certificats[22, p. 26]*

Une entité (par exemple Alice) génère un couple clef publique/clef privée. Alice conserve sa clef privée (soit dans un répertoire accessible par elle seule ou mieux, sur une carte à puce ou une clef USB protégée). Ensuite, il s'agit de rendre sa clef publique disponible pour toute personne désireuse d'effectuer un échange avec elle. Pour cela, Alice va utiliser un tiers de confiance, également appelé une Autorité de Certification (AC), pour créer un certificat. Un certificat est un document numérique qui contient au moins les coordonnées personnelles d'Alice, ainsi que sa clef publique. Ce document est signé par l'AC qui apporte ainsi sa garantie que cette clef publique est bien celle d'Alice. Cette signature sert donc à certifier l'origine du certificat et également son intégrité.

La figure ci-dessus montre les étapes de la création d'un certificat. Tout d'abord Alice génère une paire de clef privée/publique. Elle utilise sa clef publique pour demander à une AC la création d'un certificat. L'autorité de certification produit le certificat de la clef publique

d'Alice qui contient la clef publique d'Alice et différentes informations relatives à Alice signées par l'AC. Elle publie également ce certificat dans un annuaire[22, p. 25].

### II.4.1.2 Le certificats X509

Il existe plusieurs formats de certificats. Cependant, comme les certificats sont échangés entre différentes entités pour des services diverses, il serait beaucoup plus commode d'avoir un standard sur lequel les générateurs de certificats vont se baser. Sans cela, il serait impossible d'intégrer ces certificats dans des applications logicielles développées par des différents fournisseurs, pour cette raison, les certificats numériques sont soumis à un standard[32, p. 37]. Ainsi le formats X509, décrit par la norme X.509v3[19], fait l'objet d'une normalisation par l'ISO. Il a été réalisé par l'IETF (Internet Engineering Task Force) et est identifié par un « Distinguished Name » (DN)[32, p. 37].

Un certificat contient des informations sur les usages qui peuvent en être faits et sur son porteur. La description d'un certificat est la suivante[32, p. 38] :

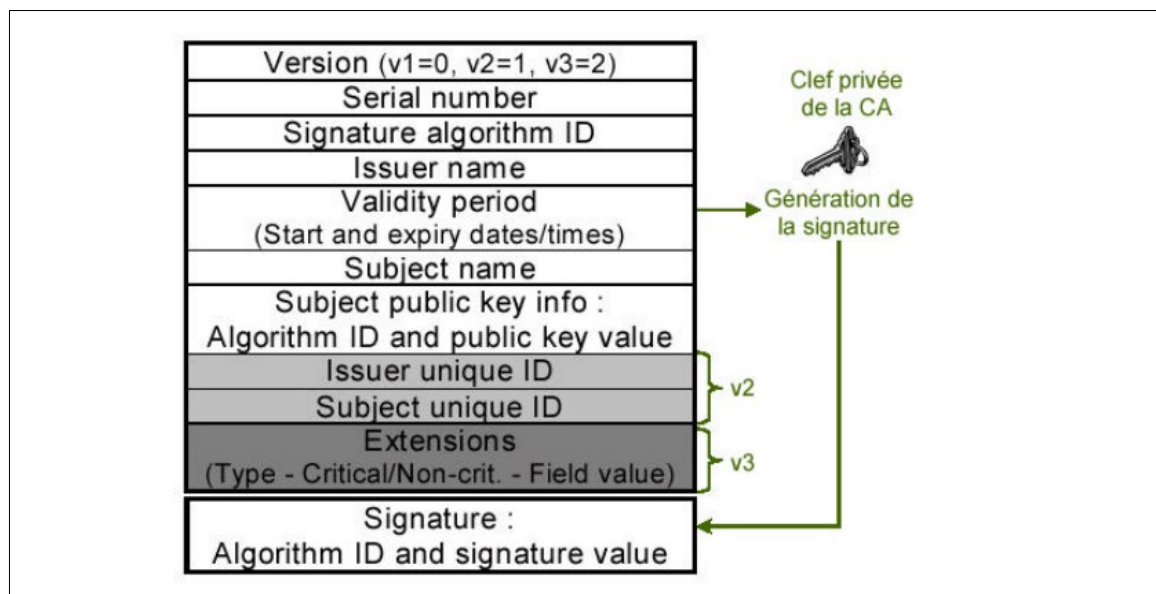


Fig. 13 : certificat X509[32, p. 38]

- ✓ **version** : Ce champ identifie à quelle version de X.509 correspond ce certificat ;
- ✓ **serial number** : Numéro de série du certificat (propre à chaque autorité de certification) ;
- ✓ **signature Algorithm ID** : algorithme utilisé pour signer le certificat ;
- ✓ **issuer Name** : Distinguished Name (DN) de l'autorité de certification qui a émis ce certificat ;

- ✓ **validity period** : C'est une paire de date pendant laquelle le certificat est valide ;
- ✓ **subject Name** : Distinguished Name (DN) du détenteur de la clé publique ;
- ✓ **subject public key info** : Le nom de l'algorithme à clé publique (ex RSA), ainsi que tous les paramètres concernant cette clé, et la clé proprement dite ;
- ✓ **issuer Unique ID/Subject Unique Id** : Extensions optionnelles introduites avec la version 2 de X.509 ;
- ✓ **extensions** : Extensions génériques optionnelles, introduites avec la version 3 de X.509 ;
- ✓ **signature** : Signatures numériques de la CA sur l'ensemble des champs précédents ;

Pour une personne physique. Le DN comporte en général les attributs suivants[11, p. 90] :

- ✓ **Common Name (CN)** : le nom du porteur, composé par la concaténation de son prénom et de son nom ;
- ✓ **Email (E)** : l'adresse e-mail du porteur ;
- ✓ **Country (C)** : Le pays de l'autorité de certification émettrice du certificat ;
- ✓ **Organization (O)** : l'entreprise (ou équivalent) d'appartenance du porteur ;
- ✓ **Organizational Unit (OU, champ multivalué)** : l'entité d'appartenance du porteur. Ou le numéro SIRET de l'entreprise référencée dans le champ O.

### II.4.1.3 Types de fichiers des certificats

Les certificats et les clés sont stockés dans plusieurs types de fichiers. Parmi ces différents types de fichiers nous avons[33] :

- **.pem** un fichier PEM comportant une extension de fichier « .pem ». Le format PEM prend en charge plusieurs certificats numériques, notamment une chaîne de certificat. Si votre organisation utilise ces hiérarchies, utilisez ce format afin de créer des certificats de CA ;
- **.arm** un fichier portant l'extension « .arm » contient une représentation ASCII codée en base 64 d'un certificat. Il inclut sa clé publique, mais pas sa clé privée.
- **.der** un fichier comportant l'extension « .der » contient des données binaires. Ce format peut être utilisé pour un seul certificat uniquement, contrairement à un fichier PEM qui peut contenir plusieurs certificats ;

- **.pfx** un fichier PKCS12 comporte l'extension « .pfx ». Il contient un certificat (d'une autorité de certification ou d'auto-signature) et une clé privée correspondante. Utilisez ce format pour transférer le contenu d'un fichier de clés vers un ordinateur distinct. Par exemple, vous pouvez créer et installer un certificat et une clé privée à l'aide de l'utilitaire de gestion des clés.

La cryptologie à clé publique résout le problème de l'échange discret entre deux correspondants qui communiquent sans s'être préalablement entendus sur une clé secrète commune. Pour transmettre un message confidentiel, il me suffit de connaître la clé publique du destinataire. Et pour cela, je la lui demande et il peut me la communiquer publiquement. Mais cette clé publique que je reçois, est-ce bien la sienne ? N'est-ce pas un intrus qui se fait passer pour mon correspondant ?

Comment puis-je m'en assurer ? Les infrastructures de gestion des clés publiques sont une réponse à ce problème.

## **II.4.2 Les infrastructures de gestion des clés publiques**

Avant d'avancer sur cette question, rappelons d'abord que le Sénégal a adopté ce système depuis 2016.

**Arrêté n° 1038 en date 29 janvier 2016** portant création et fixant les fonctionnement et d'organisation du Comité de Pilotage du projet de mise en place d'une **Infrastructure nationale de Gestion des Clefs publiques (COFIL-PKI)**

**Article Premier.** - Il est créé, auprès de la Commission Nationale Cryptologie, un Comité de pilotage du projet de mise en place d'une Infrastructure nationale de Gestion des Clefs publiques.

Une infrastructure à clé publique (PKI) est un système d'installations, de politiques et de services qui prend en charge l'utilisation de la cryptographie à clé publique pour authentifier les parties impliquées dans une transaction[34].

Les PKI (l'ensemble client/serveur) devraient permettre de traiter les points suivants (d'un point de vue technique et non uniquement marketing) [35]:

- établissement d'une confiance commune à un groupe d'utilisateurs munis de certificats ;
- mise en pratique des politiques de certification ;
- enregistrement des utilisateurs ;
- génération des clés (optionnel) ;
- certification des clés publiques ;
- gestion de la durée de vie des certificats et des clés ;
- archivage des certificats ;
- renouvellement des clés et des certificats ;
- recouvrement des clés de chiffrement (optionnel) ;
- publication et accessibilité des certificats (ce point ne relève pas à strictement parler de la PKI, et est en général assuré par des annuaires) ;
- vérification des certificats et des signatures ;
- révocation des certificats (CRL : Liste de Certificats Révoqués) ;
- gestion des co-certificats ;
- horodatage ;
- journalisation.

En réalité, ces points soulignent le rôle que doit assurer un service d'infrastructure à clés publiques. Pour accomplir cette mission, les infrastructures à clés publiques doivent être bâties sur des architectures solides sécurisés et performantes.

Il existe deux principales familles d'architectures d'infrastructures à clefs publiques[22, p. 55]:

- les architectures hiérarchiques, qui reposent sur différentes AC, distinctes des utilisateurs;
- les architectures non hiérarchiques où chaque utilisateur gère son propre réseau de confiance. Ces architectures, initialement conçues pour la messagerie comme PGP et les systèmes pair-à-pair sécurisés, reposent sur la confiance mutuelle entre les utilisateurs.

Il n'existe pas de norme unique qui définit les composants d'une infrastructure à clé publique, mais une PKI comprend généralement des autorités de certification et des autorités d'enregistrement.

#### II.4.2.1 L'autorité de certification

Dans un échange sécurisé de données électroniques par un protocole tel que TLS, les algorithmes de chiffrement asymétrique sont basés sur le partage de clés publiques entre les différents utilisateurs. L'organisme qui se charge de garantir l'authenticité et la validité des clés partagées par les différents utilisateurs est une Autorité de Certification[27, p. 3].

Les autorités de certification fournissent les services suivants :

- **émission de certificats numériques ;**
- **validation des certificats numériques ;**
- **révocation de certificats numériques ;**
- **distribution de clés publiques.**

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification ; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification[20, p. 105].





Fig. 14 : Délivrance d'un certificat par une autorité de certification[26, p. 110]

Ainsi, la signature présente dans mon certificat est vérifiable par tous mes correspondants avec la clé publique de l'autorité de certification. Ils peuvent alors utiliser en toute confiance la clé publique de mon certificat pour chiffrer des messages à mon intention[26, p. 110].

## II.4.2.2 Architectures d'infrastructures à clefs publiques

Une PKI est une infrastructure formée de certificats et de serveurs pour créer, gérer et mettre à disposition des certificats numériques dont l'authenticité est certifiée par l'autorité de certification représentant cette PKI[22, p. 58].

Une infrastructure de gestion de clefs publiques permet de protéger les clefs publiques (et parfois leurs clefs privées associées) et d'authentifier les entités (personne physique, personne morale, équipement, etc.) qui en sont propriétaires (appelés également détenteurs)[22, p. 55].

### II.4.2.2.1 Rôles des PKI

Pour la mise en œuvre de cette architecture, les certificats et l'autorité de certification sont des éléments primordiaux. Cette architecture assure des fonctions fondamentales pour des échanges électroniques sécurisés[22, p. 56] :

- **création d'une paire de clefs** : la première fonction nécessaire est bien évidemment la création de la paire de clefs, privée et publique, qui sera ensuite utilisée pour sécuriser les échanges. Cette création repose sur des mécanismes de génération d'aléa. Ceux-ci doivent être suffisamment robustes, c'est-à-dire ne doivent pas permettre à un attaquant de déterminer la valeur de la clef privée, que ce soit par attaque de type force brute ou par l'exploitation de biais dans le générateur ;
- **authentification de la clef et génération du certificat** : une fois la paire de clefs générée, il est nécessaire d'authentifier la clef publique, tandis que la clef privée sera protégée de manière à garantir sa confidentialité. Cette authentification est la fonction principale d'une PKI ;
- **remise du certificat au porteur** : cette fonction est la remise au porteur de son certificat. Le cas échéant, cela peut inclure le support contenant la clef privée et le certificat, les codes d'activation, etc.

- **publication des certificats** : ne infrastructure à clefs publiques doit permettre la mise à disposition des certificats disponibles vers l'ensemble des entités participant aux échanges. En fonction des systèmes, cette diffusion peut se faire au travers d'un annuaire en ligne, par messagerie électronique, etc.
- **vérification des certificats** : la fonction de vérification de la validité des certificats est effectuée en exploitant les informations dans le certificat (par exemple les dates de validité), la signature ou les signatures du certificat ainsi que la chaîne de confiance (en fonction de l'architecture de la PKI). Cette fonction est associée à celle de diffusion et de révocation de certificats.
- **révocation d'un certificat** : en cryptographie asymétrique, il est difficile de supprimer les certificats une fois ceux-ci diffusés. D'une part, une PKI ne connaît pas nécessairement l'ensemble des acteurs disposant d'une copie du certificat et, d'autre part, le certificat et la clef publique qu'il contient peuvent être utiles dans le futur, par exemple pour vérifier une signature précédemment apposée sur un document électronique, ou pour déchiffrer un contenu précédemment chiffré. Ainsi les certificats ne sont pas supprimés mais révoqués : l'information reste mais est complétée en indiquant que le certificat ne doit plus être utilisé pour protéger des données. La fonction de révocation inclut l'authentification de l'entité requérant la révocation ainsi que la publication des informations et des éléments associés.

#### II.4.2.2 Les composants d'une PKI

Une PKI met en œuvre plusieurs acteurs s'articulant autour d'un AC et de certificats, éléments principaux de l'architecture. Ces entités sont plus ou moins nombreuses en fonction de l'architecture de la PKI (hiérarchique ou non)[22, p. 57] :

- **le détenteur d'un certificat**, entité qui possède une clef privée et est le sujet d'un certificat numérique contenant la clef publique correspondante. Il peut s'agir d'une personne physique, d'un serveur (Web, annuaire, etc.), d'un équipement réseau, etc. ;
- **l'utilisateur d'un certificat**, qui récupère le certificat et utilise la clef publique qu'il contient dans sa transaction avec le détenteur du certificat ;
- **l'AC (« Certification Authority », CA)** qui contrôle l'identité du détenteur du certificat et signe son certificat pour attester de son authenticité;

- **l'émetteur de CRL** qui met à disposition les CRL. Sa fonction peut être déléguée hors de l'AC à une entité spécialisée.

Les entités suivantes sont propres aux architectures hiérarchiques :

- **l'Autorité d'Enregistrement (AE)** (« Registration Authority », RA) joue le rôle d'intermédiaire entre le détenteur de la clef et l'AC;
- **le dépôt ou annuaire** (« repository ») est connu par son adresse et son protocole d'accès, par exemple LDAP, X.500. Il se charge :
  - ✓ de distribuer les certificats et les CRL ;
  - ✓ d'accepter les certificats et les CRL d'autres AC et de les rendre disponibles aux utilisateurs.
- **l'archive** se charge du stockage sur le long terme des informations pour le compte d'une AC. Ce service permet de régler les litiges en conservant la mémoire des certificats, détenteurs et périodes de validité.

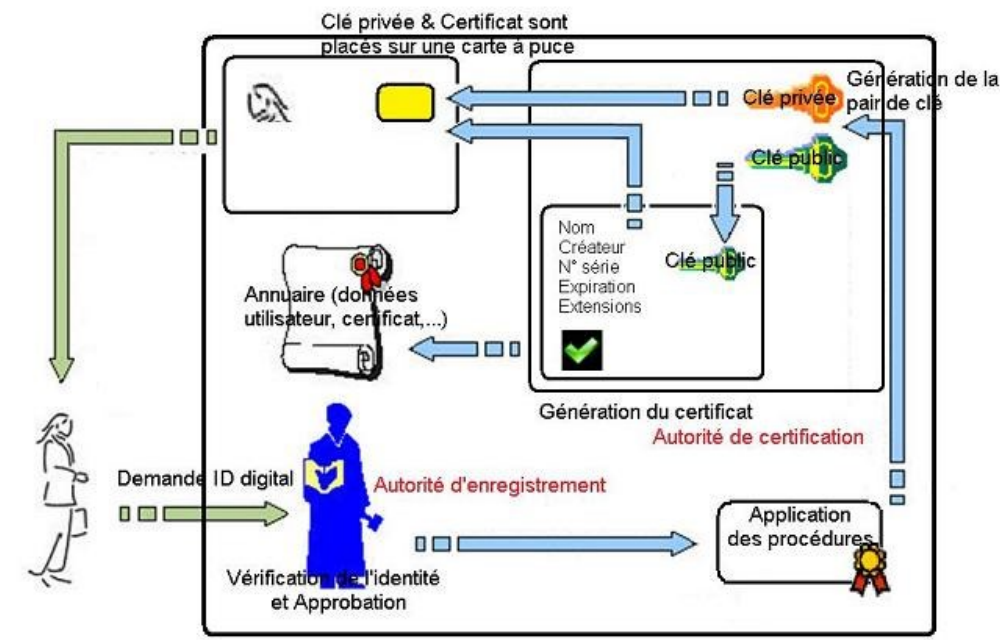


Fig. 15: Architecture PKI hiérarchique [36]

La PKI est importante, car la technologie basée sur les certificats aide les organisations à établir une signature, un chiffrement et une identité fiables entre les personnes, les systèmes et les objets.

### III. La signature électronique dans les fichiers PDF

## III.1 Définition et structure d'un fichier PDF

### III.1.1 Définition

PDF est l'abréviation de Portable Document Format. Ce format de fichier polyvalent a été inventé par Adobe pour faciliter la présentation et l'échange de documents en toute sécurité, quel que soit le matériel, l'application ou le système d'exploitation utilisé.

Le Portable Document Format a été développé par Adobe Systems; la version 1.0 a été publiée en 1993. La popularité croissante de ce format, à l'origine propriétaire, a conduit à une normalisation ISO en 2008 (PDF 1.7, ISO 32000-1) et en 2017 (PDF 2.0, ISO 32000-2)[37, p. 11].

PDF est désormais un standard ouvert, géré par l'ISO (International Organization for Standardization). Les documents PDF peuvent contenir des liens et des boutons, des champs de formulaire, des contenus audio et vidéo, ainsi que des fonctions de logique applicative. Ils peuvent être signés par voie électronique et sont faciles à consulter sous Windows ou MacOs à l'aide de l'application Adobe Acrobat Reader gratuite[38].

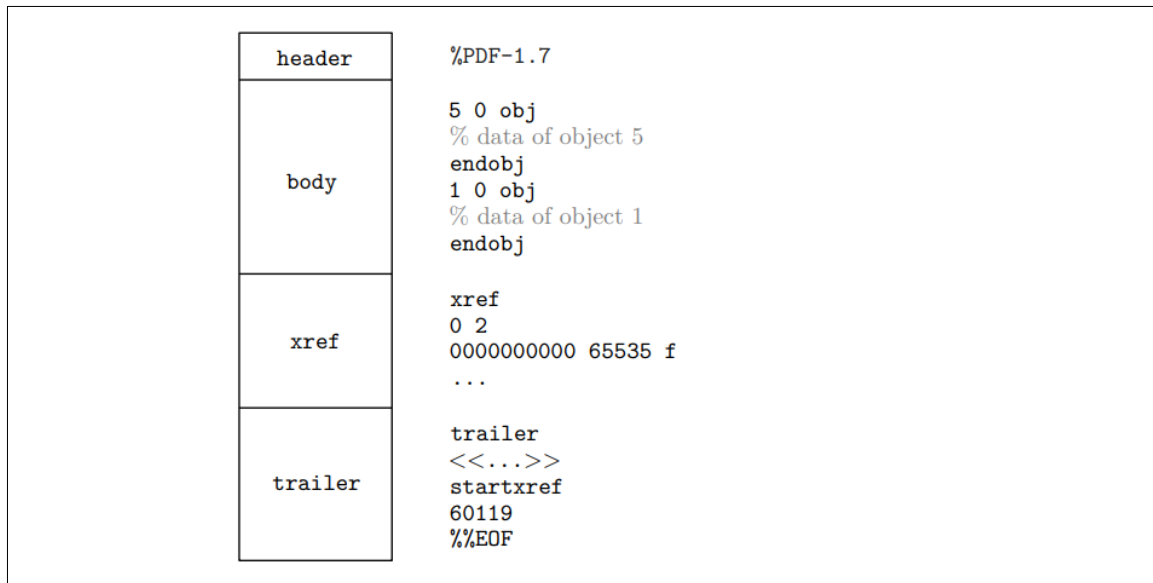
### III.1.2 Structure interne des fichiers PDF

#### III.1.2.1 Structure de base des fichiers PDF

Le contenu du fichier PDF est organisé dans l'ordre suivant à l'intérieur du fichier[39] :

- **en-tête** : Quelle que soit la version PDF, un fichier PDF commence par un en-tête contenant un identifiant unique pour le PDF et la version du format tel que **% PDF 2.0** ou **%PDF-1.x** où x varie de 1 à 7 ;
- **corps** : le corps d'un fichier PDF consiste en une séquence d'objets indirects représentant le contenu d'un document. Il peut également contenir des flux d'objets, chacun contenant une séquence d'objets indirects ;
- **table de concordance** : la table de références croisées contient des informations qui permettent un accès aléatoire à des objets indirects dans le fichier afin que le fichier entier n'ait pas besoin d'être lu pour localiser un objet particulier.
- **bande-annonce** : la bande-annonce d'un fichier PDF permet à un lecteur averti de retrouver rapidement la table de correspondance et certains objets particuliers. Les

lecteurs conformes doivent lire un fichier PDF à partir de sa fin. La dernière ligne du fichier ne doit contenir que le marqueur de fin de fichier, **%%EOF**.



*Fig. 16 : Structure d'un fichier PDF [37, p. 14]*

Un objet d'un fichier PDF comprend à plusieurs types d'objets différents qui sont des types suivants :

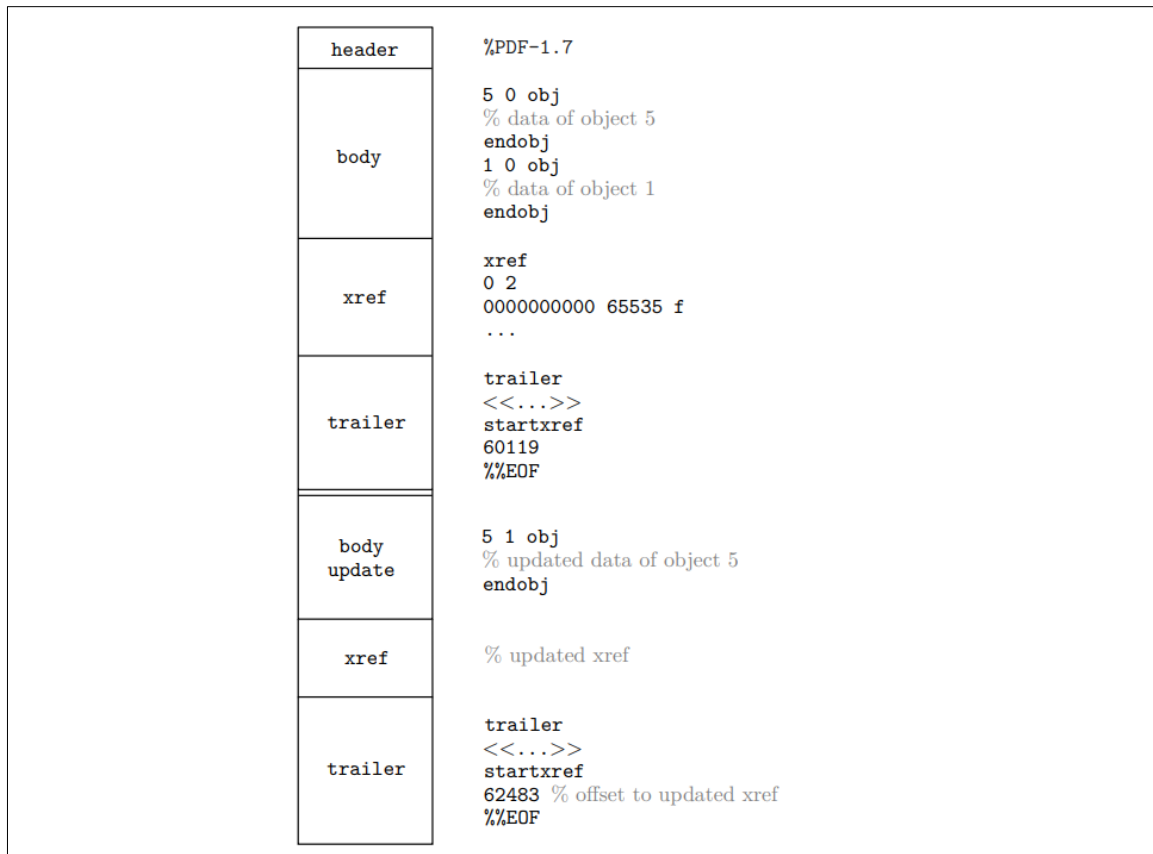
- ✓ **valeurs booléennes** : représentant conditionnel vrai ou faux
- ✓ **nombres** : valeurs entières et réelles
- ✓ **chaînes** : contient des caractères entre parenthèses
- ✓ **tableaux** : PDF prend en charge les tableaux unidimensionnels. Des tableaux de dimensions supérieures peuvent être construits en utilisant des tableaux comme éléments imbriqués ;
- ✓ **dictionnaires** : collection d'objets sous forme de paires clé-valeur. Il peut avoir zéro entrée ;
- ✓ **streams** : représente une séquence d'octets qui peut également être de longueur illimitée ;
- ✓ **objet nul** : représente une valeur nulle.

Tout objet dans un fichier PDF peut être étiqueté comme un objet indirect. Les objets indirects reçoivent un identifiant d'objet unique par lequel d'autres objets peuvent s'y référer. Les références croisées à ceux-ci sont conservées dans une table d'index et marquées avec le

mot-clé **xref** qui suit le corps principal et donne le décalage d'octet de chaque objet indirect depuis le début du fichier.

### III.1.2.2 Fonctionnement de la mise à jour d'un PDF signé

Pour mieux cerner comment la détection d'une modification, d'un document PDF signé est faite, il est important de comprendre le fonctionnement interne de la mise en jour d'un document PDF signé.



*Fig. 17 : Mise à jour incrémentale d'un PDF[37, p. 15]*

Lors de la mise à jour incrémentale d'un document PDF, les modifications doivent être suspendues à la fin du fichier. Ce style de mise à jour laisse le contenu original intact, seules les nouvelles données apparaissent à la fin, accompagnées d'une nouvelle bande-annonce et d'une section de références croisées. Ceci est avantageux dans le domaine des signatures numériques, où le hachage calculé sur la plage d'octets spécifiée conserve sa valeur[37, p. 13].

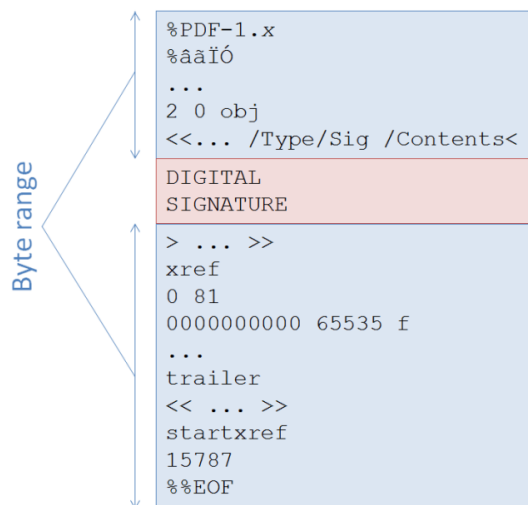
Après ces détails sur la structure interne d'un document au format PDF, voyons maintenant comment la signature électronique est insérée dans les documents au format PDF.

### III.1.2.3 Ajout de la signature électronique dans PDF

L'ajout de signatures numériques au PDF comprend 2 étapes[40].

- Créez un dictionnaire de signatures et réservez ByteRange. Initialement, tous les octets du contenu de la signature sont des zéros.
- Générez une valeur de signature « d'une manière ou d'une autre » et écrivez le contenu de la signature en hexadécimal au début du ByteRange réservé

Si vous ouvrez le fichier PDF signé numériquement avec un éditeur de texte, vous verrez quelque chose comme ceci.



```
%PDF-1.x
%âãĭó
...
2 0 obj
<<... /Type/Sig /Contents<
DIGITAL
SIGNATURE
> ... >>
xref
0 81
0000000000 65535 f
...
trailer
<< ... >>
startxref
15787
%%EOF
```

*Fig. 18 : Visualisation PDF signé numériquement avec un éditeur de texte[41, p. 26]*

## Conclusion

En résumé, nous avons détaillé, dans ce chapitre, les technologies cryptographiques qui permettent de mettre en place une solution de signature électronique. Et ensuite, nous avons vu son intégration dans les documents électroniques au format PDF.

# Chapitre 4 : Outils, Implémentation et Présentation du module de signature électronique

## Introduction

Mettre en place un système de cryptographie comme la signature électronique demande de compétences avancés et parfois une expérience avérée. Pour faciliter aux développeurs cette tâche fastidieuse, des outils ont été mis en place pour une implémentation beaucoup plus facile de la signature électronique dans les systèmes d'informations. Nous passerons ensuite à la présentation de notre module de signature électronique.

### I. Outils

La mise en œuvre d'une solution de signature électronique constitue une tâche très lourde due à la complexité des concepts et techniques qui se dissimilent derrière cette technologie. Mais aussi au processus à suivre qui très rigoureux. Et cela se comprend par l'importance et la valeur que regorge la signature électronique.


À notre niveau, pour l'implémentation et l'intégration de la signature électronique, nous allons utiliser un concept de la programmation orienté objet est la réutilisation. Ainsi, nous bénéficierons de l'expérience des autres pour pouvoir produire une solution de signature électronique de documents administratifs.

Cette réutilisation constitue l'utilisation de bibliothèques qui ont implémenté les algorithmes et l'architecture de base pour signer et lier une signature électronique à un document numérique.

Détaillons maintenant les bibliothèques rencontrées pour développer les fonctionnalités d'un système de signature électronique.



## I.1 GroupDocs

GroupDocs est une API de traitement de documents qui intègre beaucoup de bibliothèques pour  charger, assembler, rechercher, convertir, annoter, comparer et signer des documents PDF, des feuilles de calcul, des présentations, des images, des livres électroniques et bien plus encore dans vos applications C#, .NET et Java[42]. Pour le cas de la signature électronique, nous avons la bibliothèques « GroupDocssignature », pour les API permet aux développeurs d'intégrer la signature électronique dans n'importe quelle application mobile, tablette ou Web ou plus. Il prend en charge le texte, l'image ou les signatures numériques pour différents formats de fichiers. Grâce aux signatures numériques, l'API de signature électronique permet aux utilisateurs d'authentifier et de signer des documents à l'aide de mots de passe et de certificats numériques.

### I.1.1 Types de signature supportés

Les types de signature pris en charge sont les suivants[43] :

- ✓ Signature de code-barres : prend en charge plus de 60 types de codes-barres pouvant être utilisés pour signer électroniquement des documents ;
  - ✓ Signature numérique : créez une signature numérique basée sur PFX un certificat existant ;
  - ✓ Signature de champ de formulaire : créez de nouveaux champs de formulaire ou mettez à jour ceux existants avec le document ;
  - ✓ Signature des métadonnées : stockez et récupérez les propriétés des métadonnées avec une sérialisation et un cryptage personnalisé ;
  - ✓ Signature par code QR : signez électroniquement des documents avec des codes QR de différents types ;
  - ✓ Recherchez des signatures dans les documents signés électroniquement.
- **Code-barres**

Un code à barres ou un code-barres est un moyen de présenter des données sous une forme visuelle et lisible par machine. D'une manière générale, un code-barres est une image de forme rectangulaire composée de lignes noires parallèles et d'espaces blancs de différentes largeurs.

Les codes-barres sont utilisés dans divers domaines où une identification rapide est nécessaire : dans le cadre du processus d'achat dans les magasins de détail, dans les entrepôts pour suivre les stocks et sur les factures pour faciliter la comptabilité, entre autres utilisations.



*Fig. 19 : Signature électronique avec signature code-barres[44]*

- **Code QR**

Le QR-code est une sorte de code- barres bidimensionnel composé de carrés noirs disposés dans une grille carrée sur fond blanc. Le code QR peut être lu par l'appareil photo d'un smartphone ou par des appareils spécialisés dédiés à la lecture QR - scanners portables, terminaux pratiques, scanners fixes utilisés après l'avoir placé sur un bureau ou intégré dans d'autres appareils. Habituellement, les codes QR contiennent des données qui pointent vers un site Web ou une application, des e-mails ou des numéros de téléphone, des identifiants de produits.



*Fig. 20 : Signature électronique par QR-code[45]*

### **I.1.2 Limites de l'API GroupDocs**

L'API permet d'apposer une signature électronique sur des documents numériques en vue de les authentifier. Cependant elle admet quelques limites.

L'API expose des services de haut niveau en termes d'intégration de signature électronique. Toutefois les licences proposées sont relativement très chères. Par ailleurs elle ouvre un accès gratuit. Mais cet accès est très restreint et moins transparents par rapport aux attentes des développeurs qui veulent intégrer la signature électronique dans leurs applications.

En effet, elle ne donne pas aux développeurs la prise en main sur la génération des clés, l'accès aux données signées.

Developer Small Business	Developer OEM	Site Small Business	Site OEM	Metered Small Business	Metered OEM
1 Developer And 1 Deployment Location	1 Developer And Unlimited Deployment Locations	Up To 10 Developers And Up To 10 Deployment Locations	Up To 10 Developers And Unlimited Deployment Locations	Unlimited Developers And Pay As You Use	Unlimited Developers And Pay As You Use
\$1199	\$3597	\$5995	\$16786	from \$1999/month	from \$1999/month
with Free Support	with Free Support	with Free Support	with Free Support	with Free Support	with Free Support
Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote
\$1598	\$5394	\$9990	\$28771	from \$1999/month	from \$1999/month
with Paid Support	with Paid Support	with Paid Support	with Paid Support	with Paid Support	with Paid Support
Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote
\$1199	\$3597	\$5995	\$16786	from \$1999/month	from \$1999/month
with Paid Consulting	with Paid Consulting	with Paid Consulting	with Paid Consulting	with Paid Consulting	with Paid Consulting
Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote	Buy or Quote

Fig. 21 : Prix des licences temporaires proposées[46]

## I.2 L'API IText

IText est elle aussi une API l'instar de GroupDocs pour l'intégration, beaucoup plus facile pour les développeurs, de la signature électronique. IText n'est pas un outil d'utilisateur final. Elle est diffusée sous deux licences : MPL<sup>1</sup> et LGPL<sup>2</sup>. Ceci la procure son caractère d'API open source : « Logiciels créés par et pour les développeurs ». Elle est soutenue par une forte communauté de développeurs dans beaucoup de pays. Ce qui offre aux développeurs qui veulent intégrer la signature électronique, une certaine souplesse et la possibilité de faire des choix diversifiés pour l'implémentation. L'API IText offre les services de base pour la mise en œuvre d'une solution de signature électronique.

Elle permet de réaliser plusieurs types de signature électronique :

- Code-barres ;
- QR-code ;
- Signature numérique.

<sup>1</sup> Mozilla Public License (ou MPL, Licence publique Mozilla en français)

<sup>2</sup> Lesser General Public License (Licence Publique Générale Limitée en Français)

## I.2.1 Avantages de l'API IText

IText a toujours été à l'avant-garde des signatures numériques en PDF en prenant en charge PAdES et en étant l'un des premiers à prendre en charge les signatures dans la dernière version PDF 2.0.

Notre API mature et facile à utiliser a été minutieusement testée par l'industrie et s'est avérée un succès lorsqu'elle est utilisée dans plusieurs cas d'utilisation[47].

L'API IText n'exige pas aux développeurs un choix sur le type de fichier pour les clés et même aussi pour les certificats. Ce qui donne aux développeurs la possibilité de faire des choix libres et adaptés par rapport à leurs besoins. Cette facilitation représente un motif valable pour le choix de cette dernière.

## I.2.2 Limites de l'API IText

Bien qu'IText offre plusieurs avantages, il présente également certains inconvénients[48] :

- **intégrations prêtes à l'emploi limitées** : le logiciel peut nécessiter des efforts supplémentaires pour s'intégrer à des applications spécifiques au niveau de l'entreprise, ce qui entrave une transformation numérique fluide ;
- **tarification complexe** : la structure de tarification semble quelque peu complexe, ajoutant un peu d'ambiguïté lors de l'évaluation des coûts-avantages.

## I.3 Comparaison entre les deux API

Sur ce passage, nous donnons quelques éléments comparatifs sur les API que nous avons décrits en haut. Ceci rentre dans le cadre de l'orientation et la validation de notre choix de l'API avec laquelle nous allons travailler pour implémenter une solution de signature électronique.

API	Version standard	Open source	Tarifs	Technologies supportées
IText	Séparation des clés dans deux fichiers différents	Oui	Prix disponible sur demande	Java et C#

## GroupDocs

Prend un type de fichier qui met la clé privée et publique ensemble

Oui

Prix consultables, mais assez chères

Java et C#

Pour la mise en place de notre solution de signature électronique, nous avons opté pour l'API IText.

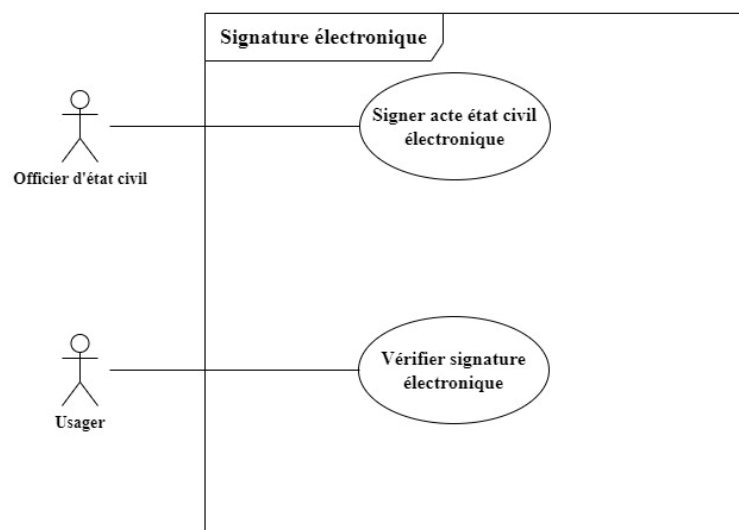
## II. Implémentation

Pour l'implémentation de notre application, nous avons tout d'abord montré les fonctionnalités de notre module de signature électronique et procéder à la génération des clés privées et publiques mais aussi au certificat qui constituent les éléments de bases pour apposer une signature électronique sur un document. Pour ce faire, nous nous sommes servis de « Keytool » de Java via l'interface graphique « KeyStore Explorer ».

### II.1 Diagramme de cas d'utilisation

Dans notre système nous avons deux acteurs :

- **L'officier d'état civil** : le maire qui effectue la signature électronique de l'acte d'état civil ;
- **L'usager** qui fait une vérification de l'acte signer



*Fig. 22 : Diagramme cas d'utilisation*

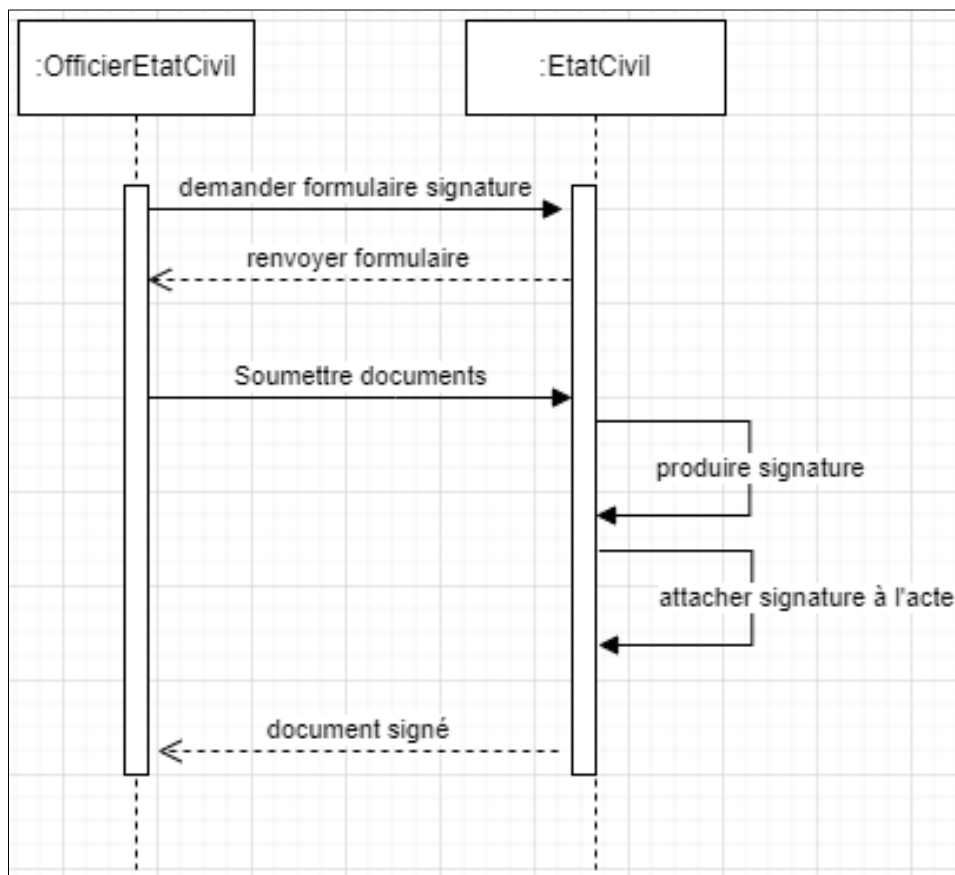
## II.2 Diagrammes de séquence

Un diagramme de séquence est un diagramme UML qui représente la séquence de messages entre les objets au cours d'une interaction. Un diagramme de séquence comprend un groupe d'objets, représentés par des lignes de vie, et les messages que ces objets échangent lors de l'interaction.

Les diagrammes de séquence représentent la séquence de messages transmis entre des objets. Ils peuvent également représenter les structures de contrôle entre des objets.

### II.2.1 Diagramme de séquence signer acte d'état civil

Ce diagramme représente les interactions lors de la signature d'un acte d'état civil.



*Fig. 23:Diagramme séquence signature électronique*

## II.2.2 Diagramme de séquence vérifier signature acte d'état civil

Ce diagramme représente les interactions lors de la vérification de la signature d'un acte d'état civil.

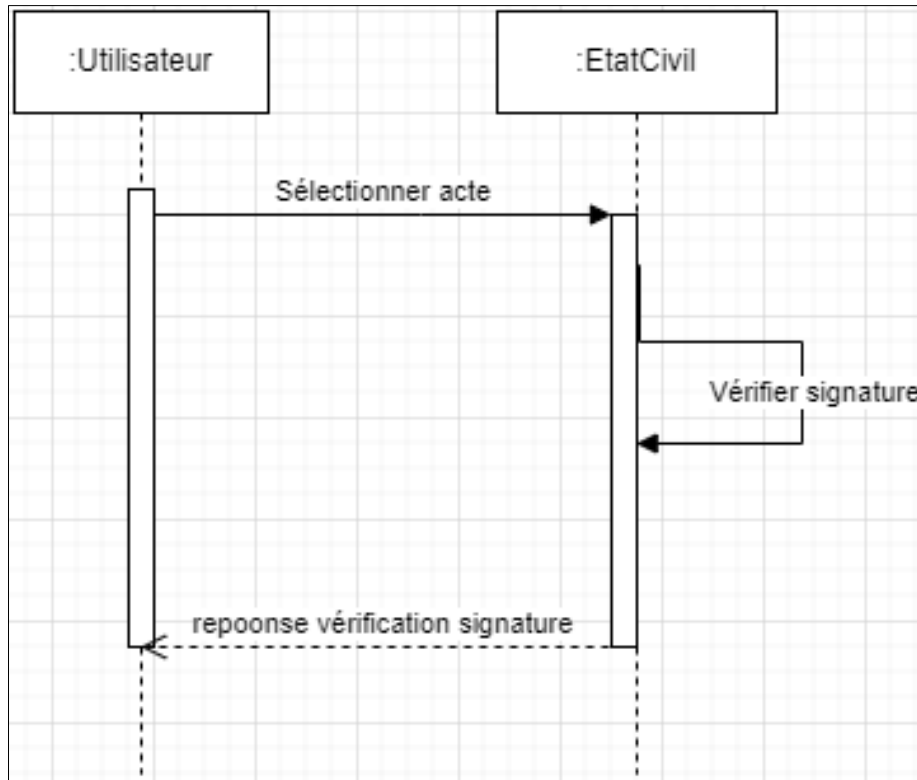


Fig. 24: Diagramme séquence vérification signature électronique

## II.3 KeyStore Explorer

KeyStore Explorer est une interface graphique open source remplaçant les utilitaires de ligne de commande Java keytool et jarsigner. KeyStore Explorer présente leurs fonctionnalités, et bien plus encore, via une interface utilisateur graphique intuitive[49]. KeyStore Explorer peut être utilisé pour créer et parcourir des KeyStores via son interface graphique intuitive. Il prend en charge une variété de KeyStore, paires de clés, privés formats de clé et de certificat et peut convertir entre eux. Il peut être utilisé pour créer votre propre certificat CA et signez des certificats et des CRL avec une large gamme d'extensions de certificat est pris en charge.



KeyStore nous permet la génération d'un système de certificat hiérarchique. Ainsi nous pourrions générer des certificats signés par une autorité certification.

En lançant l'application, nous tombons sur cette fenêtre.

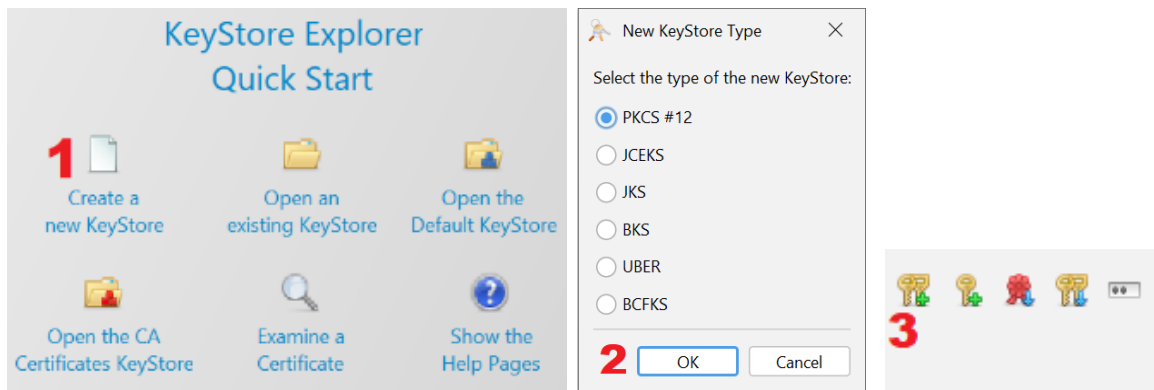


Fig. 25 : Choix du type de KeyStore et démarrage de la génération de la paire de clés

Ici nous procédons à la génération de la paire de clés à savoir la clé privée et publique de l'autorité de certification. Cette paire de clés sera utilisée pour signer les certificats des entités demandeurs. Nous choisissons d'abord PKCS#12 qui est un type de keyStore standard très utilisé, ensuite on clique l'icône des doubles clés comme indiquer sur l'image ci-dessus pour commencer proprement la génération.

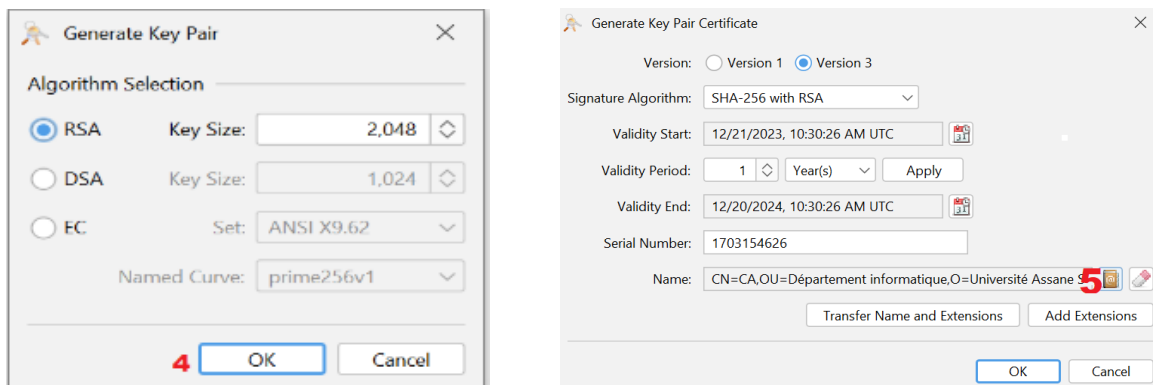


Fig. 26 : Choix de l'algorithme, de la taille de la clé et des informations liés au certificat

Ici nous avons choisi l'algorithme à utiliser et la taille de la paire de clés qui extrêmement importante. Il y a aussi les informations liées au certificat la montre la figure en haut. Par exemple la durée de validité, la version du certificat, etc.



Common Name (CN):	CA	+	-
Organization Unit (OU):	Département informatique	+	-
Organization Name (O):	Université Assane SECK de Ziguinchor	+	-
Locality Name (L):	Ziguinchor	+	-
State Name (ST):	Casamance	+	-
Country (C):	SN	+	-

Reset

**6** OK Cancel

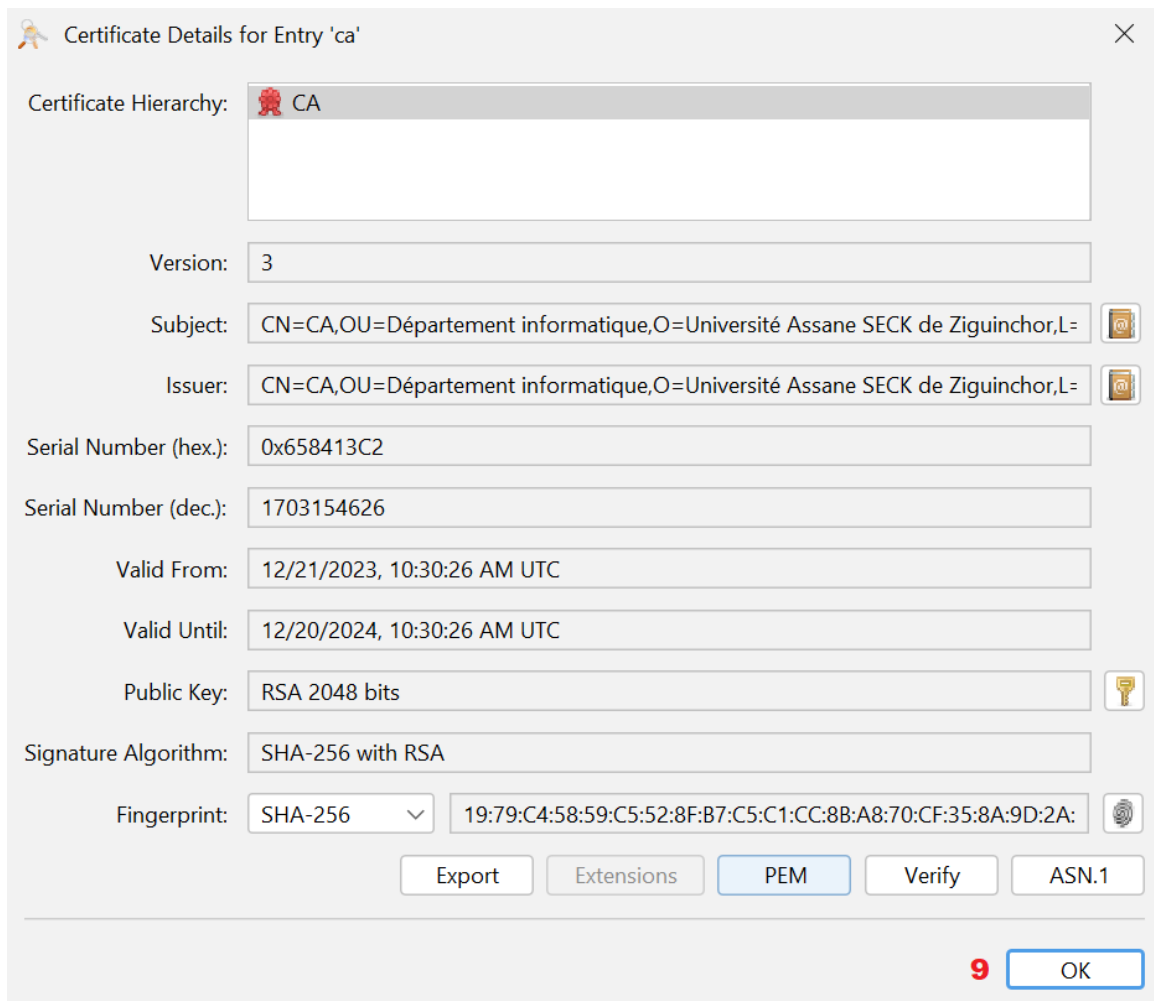
*Fig. 27 : Information à remplir sur l'autorité de certification*

New Key Pair Entry Alias		New Key Pair Entry Password	
Enter Alias:	CA	Enter New Password:	.....
		Confirm New Password:	.....
<b>7</b>	OK Cancel	<b>8</b>	OK Cancel

*Fig. 28 : définition de l'alias et du mot de passe*

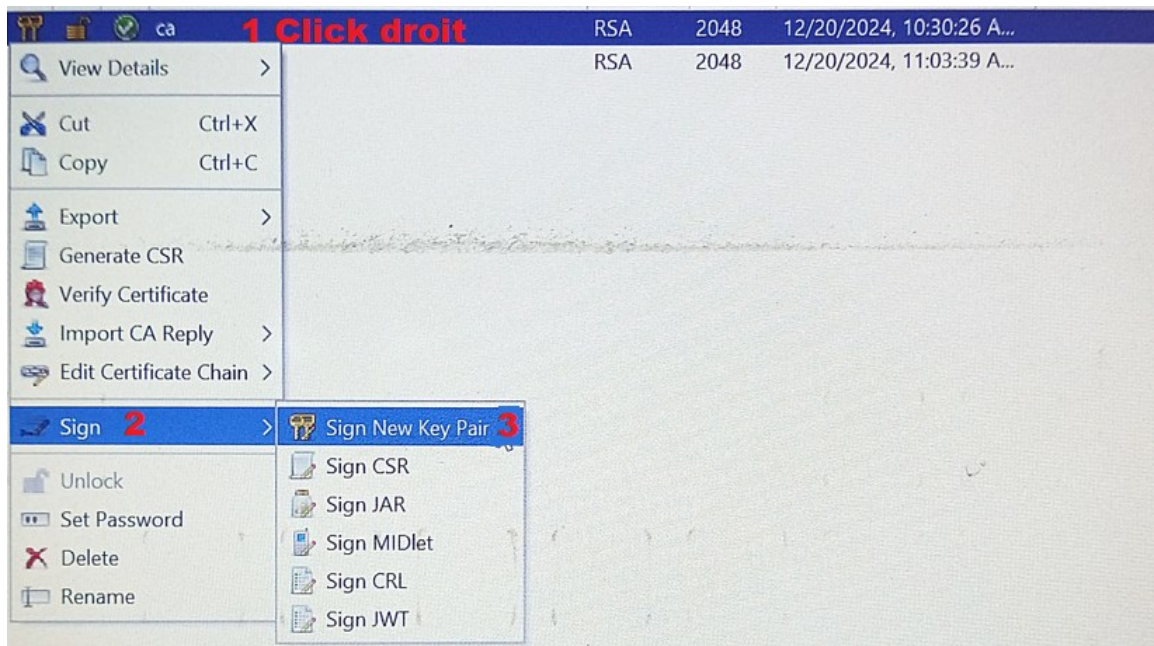
Nous avons ici les informations sur l'autorité de certification qui sont des éléments constitutifs de son certificat.

L'alias permet d'extraire la clé privée à partir du fichier keyStore généré. Le mot de passe restreint l'accès à celle-ci.



*Fig. 29 : Certificat de l'autorité de certification*

Maintenant nous pouvons passer à la génération du certificat d'une entité désirant utilisée la signature électronique pour signer des documents numériques. Ce certificat sera signé lui-même par l'autorité de certification émettrice. Pour cela, voici ci-dessous la procédure à suivre.



*Fig. 30 : étape 1 de la génération du certificat de l'entité réceptrice : Mairie*

Pour produire un certificat signer par l'entité émettrice on fait un clic droit sur le KeyStore de l'autorité de certification et on suit les étapes comme mentionné sur la figure ci-dessus.

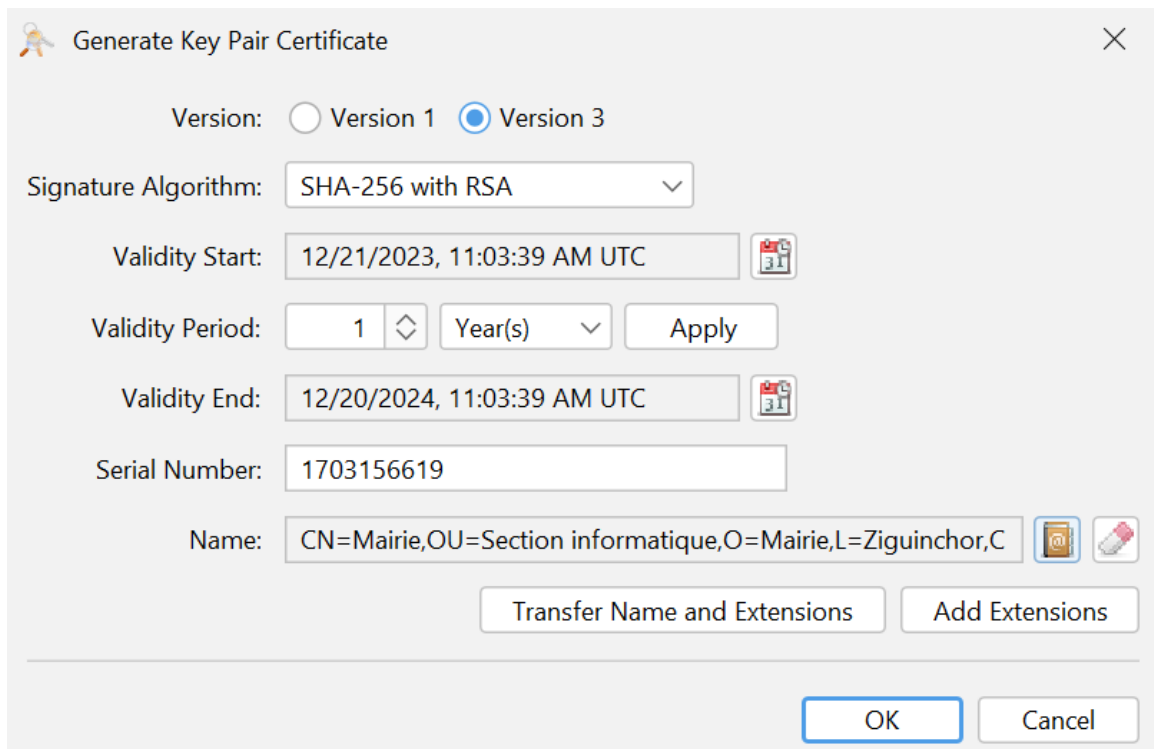
The 'Name' dialog box contains the following fields and values:





- Common Name (CN): Mairie
- Organization Unit (OU): Section informatique
- Organization Name (O): Mairie
- Locality Name (L): Ziguinchor
- Country (C): SN

Buttons at the bottom: OK, Cancel, and a Reset button.

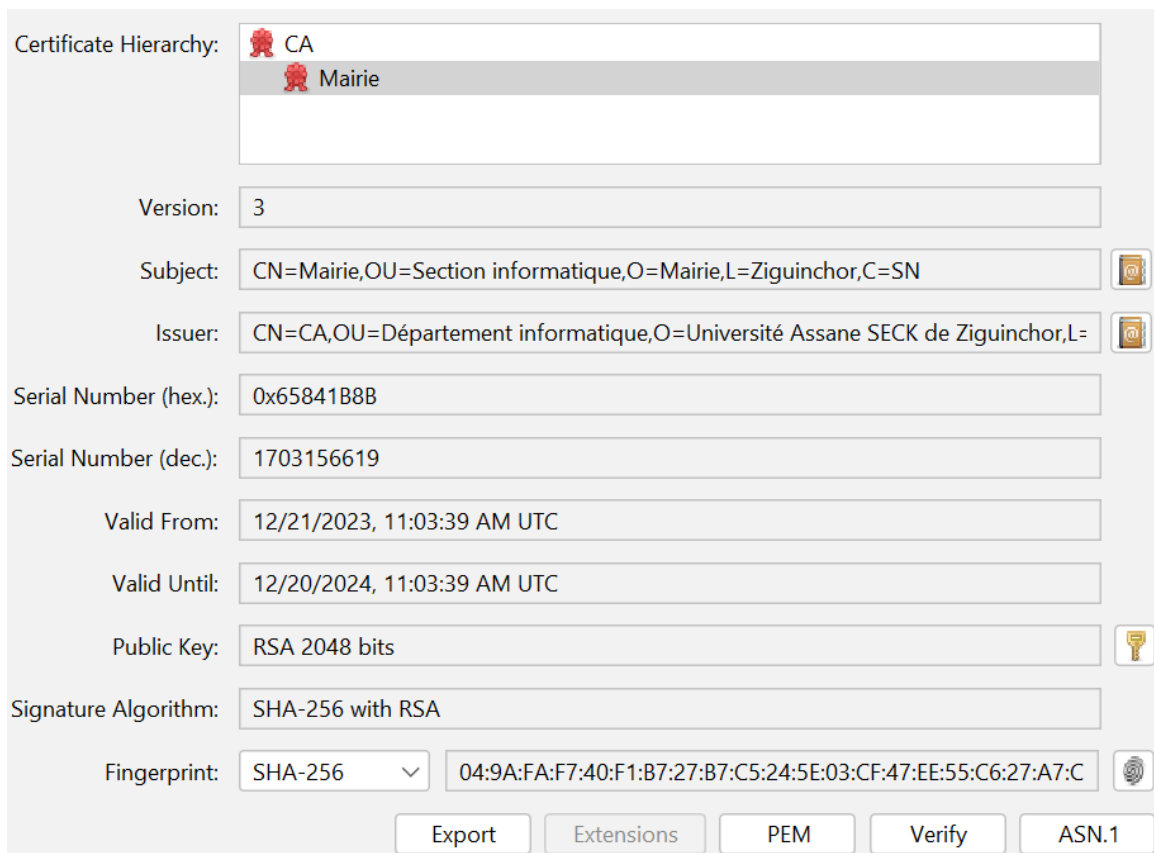
*Fig. 31 : Saisi information de l'entité réceptrice du certificat*







Sur cette figure ci-dessus, nous remplissons les informations sur l'entité réceptrice du certificat.

 The dialog box is titled "Generate Key Pair Certificate" and contains the following fields and controls:

- Version:  Version 1  Version 3
- Signature Algorithm:
- Validity Start:  
- Validity Period:
- Validity End:  
- Serial Number:
- Name:   
- 
- 

*Fig. 32 : Information liés au certificat*

 The dialog box displays the following certificate details:

- Certificate Hierarchy:  CA  
 Mairie
- Version:
- Subject:  
- Issuer:  
- Serial Number (hex.):
- Serial Number (dec.):
- Valid From:
- Valid Until:
- Public Key:  
- Signature Algorithm:
- Fingerprint:   
- 

*Fig. 33 : Détails sur le certificat de l'entité réceptrice*

On remarque sur la structure du certificat qu'émit par une autorité racine qui garantit sa validité.

Après la génération des clés et des certificats, nous entrons dans le métier, le développement des fonctionnalités de l'application. Ainsi nous avons choisi le langage de programmation java pour le développement de l'application.

## II.4 Le langage java

Oracle Java est le premier langage de programmation et la première plate-forme de développement. Il réduit les coûts, raccourcit les délais de développement, favorise l'innovation et améliore les services d'application. Avec des millions de développeurs utilisant plus de 60 milliards de solutions JVM (Java Virtual Machine) dans le monde, Java reste la plate-forme de développement de choix pour les entreprises et les développeurs[50].



Java propose, à travers l'API JCA (Java Cryptography Architecture), depuis sa deuxième version, des services cryptographiques sans se préoccuper de l'implémentation des algorithmes. JCA a été conçu pour suivre plusieurs objectifs[51] :

- laisser l'implémentation à des fournisseurs ;
- être extensible : différentes implémentations de fonctions cryptographiques utilisant différents algorithmes peuvent être proposées par différents fournisseurs ;
- assurer l'indépendance et garantir l'interopérabilité entre les différentes implémentations.

Par-dessus le langage, pour une meilleure structuration du code source, une rapidité dans l'implémentation et le respect de nombreuses bonnes pratiques en développement, nous avons aussi utilisé Spring Framework.

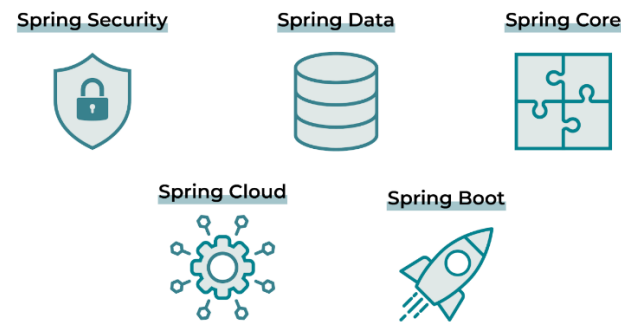
### II.4.1 Spring Framework

Spring Framework est, un **cadre de travail existant** que les développeurs peuvent utiliser[52],



une infrastructure open source d'entreprise couramment utilisée qui permet de créer des applications autonomes de production qui fonctionnent sur la machine virtuelle Java (JVM)[53]. Spring Framework offre un système d'injection de dépendances très puissants qui permet aux objets de définir leurs propres dépendances que le conteneur Spring. Ainsi, les développeurs peuvent créer des applications modulaires constituées de composants faiblement couplés qui sont idéaux pour les micro-services et les applications de réseau distribué.

Spring Framework est subdivisé en plusieurs composants appelés modules. Ces modules sont repartis en fonctions des domaines métiers où ils interviennent.



*Fig. 34 : Les composants Spring[52]*

**Spring Core** : ce composant est la base de l'écosystème Spring. Il contient le « core container » (ce qui permet l'injection de dépendances vue précédemment), mais il contient également Spring MVC qui permet de faire du web et de Data Access qui fournit des éléments fondamentaux pour la communication avec les bases de données.

**Spring Data** : ce composant permet de communiquer avec de nombreux types de bases de données.

**Spring Security** : ce composant permet de gérer l'authentification, l'autorisation, mais aussi la sécurité des API.

**Spring Cloud** : L'implémentation de l'architecture micro-service s'avère très complexe et demande des compétences avancées et une expérience confirmée, ce qui pourrait être un frein pour les développeurs. Ainsi, pour lever d'éventuelles contraintes de cette architecture logicielle, Spring Framework fournit Spring Cloud.

**Spring Boot** : c'est un composant très particulier de Spring Framework, dans la mesure où il nous permet de mettre en œuvre tous les autres. Spring Boot s'offre beaucoup d'avantages grâce avec trois fonctionnalités importantes :

- l'autoconfiguration automatique de Spring ;
- des starters de dépendances ;
- des endpoints Actuator pour fournir des données sur l'application.

Pour l'édition du code source, nous avons choisi l'IDE IntelliJ qui est très puissant avec son système de plugins et offre une autocomplétion merveille.

## II.4.2 L'environnement de développement IntelliJ IDEA



IntelliJ est un des IDE Java les plus modernes. Il propose un système d'autocomplétion parmi les plus aboutis du marché, ainsi que des fonctionnalités avancées de refactoring et une interface utilisateur offrant une très bonne expérience[54]. Système complet, avec des systèmes d'auto-complétions intelligente, d'analyse de code en temps réel, de refactoring avancé, l'intégration d'outils de tests et de debugging, mais aussi une pléthore de raccourcis clavier permettant de réaliser n'importe quelle tâche rapidement.

IntelliJ est payant, avec même des licences relativement chères. En contrepartie, il offre une version communauté avec des fonctionnalités de bases mais moins performante et très limitée. Il donne aussi des licences académiques pour permettre d'accéder gratuitement à tous les IDE et outils collaboratifs de JetBrains pour enseigner les cours de programmation dans votre école[55]. Ces licences se font sur demande mais avec des motifs valables.

Comme, nous comptons mettre en place une application web, nous aurons besoin de certaines technologies web.



## II.5 Les technologies web utilisées

### II.5.1 Le langage HTML et le moteur de template thymeleaf

- L'**HTML**, pour **HyperText Markup Language**, constitue le langage de bases d'un site internet. Ce n'est pas un langage de programmation mais un langage de balisage qui permet d'écrire de l'hypertexte et ainsi de définir la structure sémantique d'une page web[56]. Il définit la structure du contenu. Un document HTML est une suite d'éléments utilisés pour encadrer différentes parties du contenu afin de les faire apparaître ou se comporter d'une certaine façon.  

- **Thymeleaf** est un moteur de modèles Java côté serveur moderne pour les environnements Web et autonomes. L'objectif principal de Thymeleaf est d'apporter des modèles naturels et élégants à votre flux de travail de développement : du HTML qui peut être correctement affiché dans les navigateurs et également fonctionner comme des prototypes statiques, permettant une collaboration plus forte au sein des équipes de développement.  



Avec des modules pour Spring Framework, une multitude d'intégrations avec vos outils préférés et la possibilité de connecter vos propres fonctionnalités, Thymeleaf est idéal pour le développement Web **JVM HTML5** moderne, même s'il peut faire bien plus[57].

## II.5.2 CSS et la librairie Bootstrap

- Les **Cascading StyleSheets** ou **CSS** sont la première technique à apprendre après  le HTML. Alors que HTML s'utilise pour définir la structure et la sémantique du contenu, les CSS sont employées pour composer et déterminer l'apparence de ce contenu[58]. Le CSS permet, lui, d'arranger le contenu et de définir la présentation : couleurs, image de fond, marges, taille du texte... Comme vous vous en doutez, le CSS a besoin d'une page HTML pour fonctionner[59, p. 6].
- Le framework Bootstrap est un framework CSS. Le but de Bootstrap est de permettre, par  exemple, de rendre facilement un site responsive design (adapté à tous les écrans : ordinateur, mobile, tablettes) sans avoir besoin de coder toute la partie CSS[60]. Le Framework propose des modèles en HTML, CSS et JavaScript, pour mettre en page des composants de navigations, des boutons, des images, des blocs. Il définit un système de grille qui lui est propre.

La connaissance du CSS est donc un prérequis indispensable à l'utilisation de ce framework. De plus, la plupart des composants Bootstrap utilisent également du code JavaScript ; une connaissance de base de ce langage est donc également conseillée même si elle n'est pas strictement obligatoire[61].

## II.5.3 JavaScript le la librairie JQuery

- **JavaScript** est un langage de programmation qui vous permet de mettre en œuvre des  éléments complexes sur des pages Web. Langage de script léger, orienté objet, principalement connu comme le langage de script des pages web[62]. C'est un langage à objets utilisant le concept de prototype, disposant d'un typage faible et dynamique qui permet de programmer suivant plusieurs paradigmes de programmation : fonctionnelle, impérative et orientée objet. Le standard qui spécifie JavaScript est **ECMAScript**[63].



- **JQuery** est ce qu'on appelle une « librairie » ou une « bibliothèque » JavaScript. Le rôle d'une librairie, en informatique, est de simplifier l'utilisation d'un certain langage de programmation en fournissant un ensemble de codes déjà prêts à l'emploi. En l'occurrence, la librairie jQuery consiste en un ensemble de blocs de codes JavaScripts préconçus et qui vont être généralement enfermés dans des méthodes. Il va donc nous suffire d'appeler ces méthodes pour exécuter le code qu'elles contiennent[64].



Elle est la bibliothèque JavaScript la plus utilisée et nous permet de créer des effets dynamiques sur nos pages web comme des changements de couleur, des animations, et des effets de fondu.

Après avoir fait une présentation des outils et technologies web utilisés nous, allons passer à la présentation des interfaces utilisateur de notre application.

### III. Présentation de l'application

#### III.1 Page d'accueil



*Fig. 35 : Page d'accueil de l'application*

Cette interface constitue la porte d'entrée dans notre plateforme de signature électronique. Il s'agit d'une interface montrant les technologies liées à ce travail et l'objectif visé par cette application.

Pour effectuer une opération de signature, nous avons choisi des utilisateurs par défaut pour le test des fonctionnalités de notre application.

#### III.2 Interface de connexion



*Fig. 36 : Procédure de connexion à l'application*

Ainsi nous nous retrouvons sur l'interface ci-dessous, représentant le formulaire de connexion à l'application.

*Fig. 37 : Formulaire de connexion*

Après avoir validé avec le bouton de connexion, nous sommes redirigés sur la page ci-après. Cette page, avec un menu contextuel, permet d'effectuer des opérations de signature électronique à travers un formulaire mais aussi de vérification.



*Fig. 38 : Menu de l'application*

Pour signer un acte, on clique sur l'onglet « Signature » pour être redirigé vers le formulaire de signature.

### III.3 Formulaire de signature électronique

The screenshot shows the "Opération de signature" form with the following fields and values:

- Document à signer (.pdf): Choisir un fichier | extrait d'acte de naissance\_1.pdf ✓
- Votre clé privée (.key): Choisir un fichier | esign.key ✓
- Votre certificat(.cer): Choisir un fichier | esign.cer ✓
- Certificat de l'autorité de certification(.cer): Choisir un fichier | ca.cer ✓
- Buttons: Signer

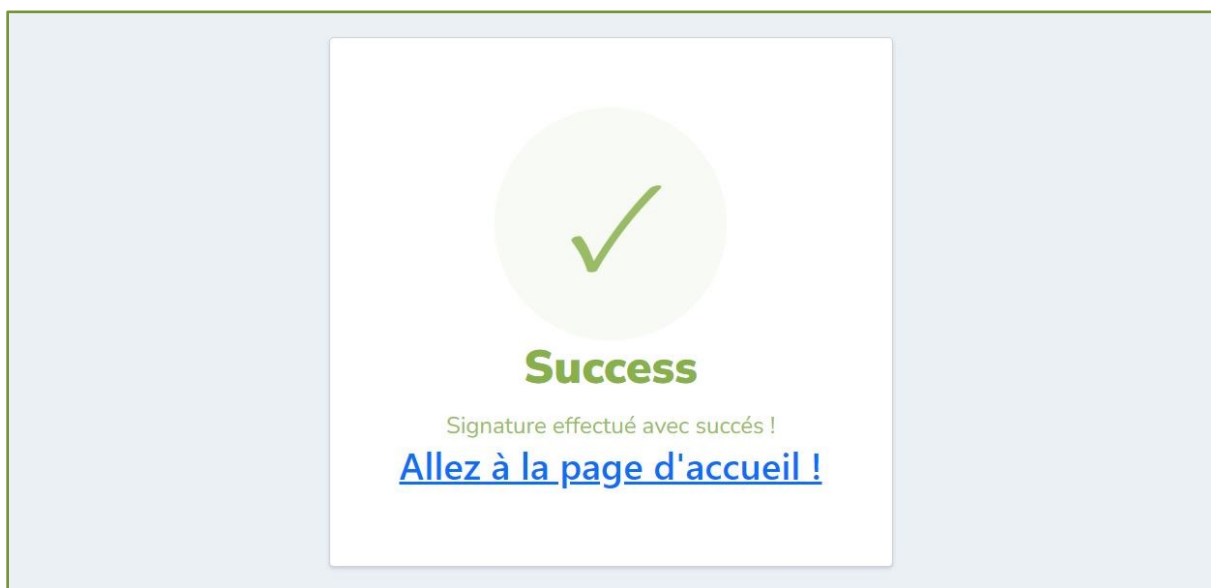
*Fig. 39 : Formulaire de signature électronique*

Le formulaire est rempli en donnant :

- l'acte d'état civil électronique à signer au format PDF ;

- La clé privée du signataire avec laquelle l'acte sera paraphé, l'extension acceptée par notre application est « **.key** » ;
- Le certificat du signataire représentant sa carte d'identité, l'extension acceptée par notre application est « **.cer** » ;
- Le certificat de l'autorité de certification délivrant le certificat du signataire, l'extension acceptée par notre application est « **.cer** ».

Voici la page affichée si la signature est réussie.



*Fig. 40 : Opération de signature réussie*

En validant le formulaire avec les bonnes informations la signature est effectuée et elle est matérialisée sur l'acte par un affichage des informations du signataire issues de son certificat. Cependant soulignons que ceci n'est que la face externe de la signature électronique pour montrer à l'aperçu que l'acte a été signé. Mais en réalité la signature électronique est loin de là, elle est enveloppée dans l'acte d'état civil électronique.

La figure ci-dessous montre la partie visuelle de la signature électronique sur un extrait de naissance pris comme exemple.

REGION : _____ DEPARTEMENT : _____ ARRONDISSEMENT : _____ COLLECTIVITE LOCALE (Commune ou Communauté Rurale)	REPUBLIQUE DU SENEGAL UN PEUPLE - UN BUT - UNE FOI <b>ETAT CIVIL</b> CENTRE DE (1)
<b>EXTRAIT du REGISTRE DES ACTES de NAISSANCE</b>	
Pour l'année (2) _____ (en lettres)	AN - _____
N° dans le Registre _____ (en lettres)	N° dans le Registre en chiffres _____
Le _____ Année à _____ heures _____ minutes est né (é) à _____ un enfant de sexe [ M ] ou [ F ] (4)	LIEU DE NAISSANCE _____
PRENOMS _____ de _____ et de _____	NOM DE FAMILLE _____ NOM DE FAMILLE DE LA MERE _____
Pays de naissance pour les naissances à l'étranger (3) _____ (écrite en majuscules le lieu de naissance, les prénoms et le nom)	
Delivré par le juge de Paix de _____ le _____ Année sous le numéro _____ inscrit le _____ sur le registre des Actes de Naissance de l'année _____	AN - 20 _____ N° dans le Registre en chiffres _____ AN - 20 _____
EXTRAIT DELIVRE PAR LE CENTRE DE _____ POUR EXTRAIT CERTIFIE CONFORME _____ A _____ Emetteur : e-sign.sn Signé par : serigne@gmail.com Localisation : Ziguinchor Date : 19-02-2024 12:25:30	

Fig. 41 : Apparence de la signature

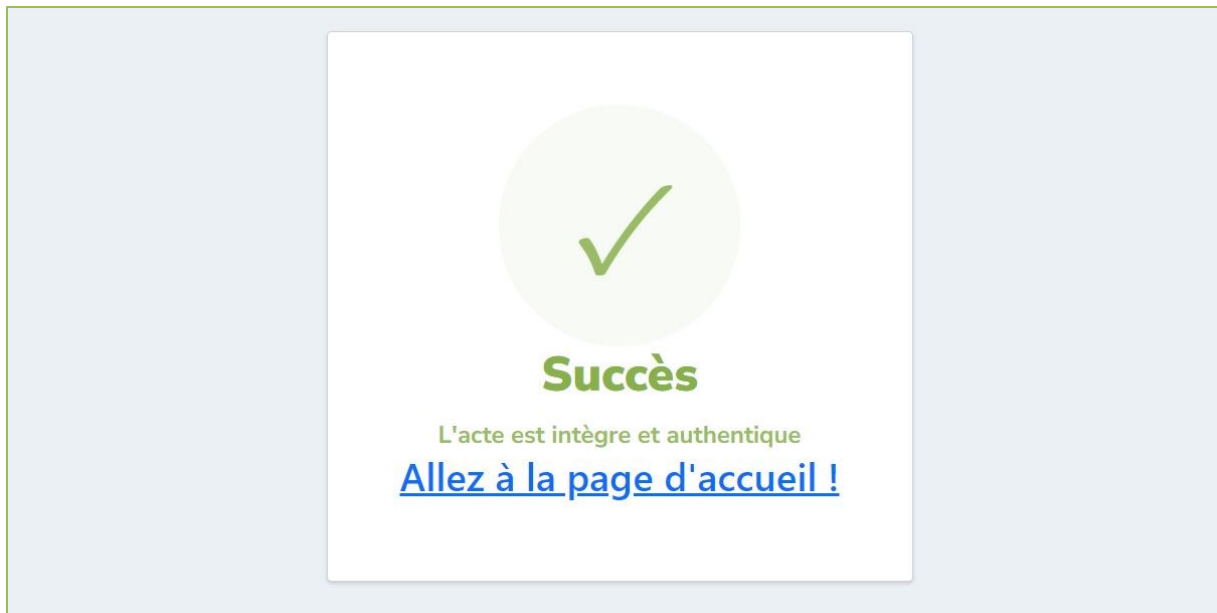
Pour la vérification technique de la signature électronique, nous l'avons réalisée aussi à travers un formulaire. Ce formulaire contient un seul champ pour charger l'acte d'état civil dont la signature électronique doit être vérifiée.

### III.4 Vérification de la signature effectuée

Accueil	Signature	Vérification	serigne@gmail.com
<b>Vérification signature</b>			
Document à vérifier (.pdf):			
Choisir un fichier	extrait d'acte de naissance_1.pdf ✓		
Vérifier			

Fig. 42 : Vérification de la signature électronique

Pour la confirmation de la validité de la signature électronique, nous sommes redirigés sur la page ci-dessous au cas où la vérification est effectuée avec succès.



*Fig. 43 : Signature valide*

## **Conclusion**

En résumé, ce chapitre nous a permis de présenter le résultat concret de notre travail de mémoire. Nous avons présenté les différentes interfaces de l'application. Mais étant donné l'ampleur de ce projet, certaines fonctionnalités n'ont pas encore été développées. Ainsi la suite logique de ce travail de mémoire sera de terminer ces fonctionnalités et d'élargir les choix sur les formats de documents électroniques mais aussi les types de fichiers utilisés pour réaliser la signature.

# Conclusion Générale

La réflexion qui se traduit par le biais du travail présenté dans ce mémoire attire l'attention sur l'adoption et l'intégration de la signature électronique au travers la dématérialisation dans la gestion des actes d'états civils au niveau des municipalités. Une problématique pesante retient les esprits sur les difficultés qu'éprouvent la population pour se procurer un acte d'état civil. La rédaction de ce mémoire relate aussi des arguments sociétaux réels qui renforcent l'inclusion inévitable de la signature électronique dans la dématérialisation des procédures pour la gestion de l'état civil.

Dans l'étude de ce mémoire, nous avons commencé par une description succincte sur la situation actuelle dans le processus de demande d'un acte d'état civil. Ainsi nous constatons que, le processus et les méthodes utilisés, dans la gestion de l'état civil dans nos municipalités, ne permettent pas de mettre à disposition un acte d'état civil sans avoir à l'imprimer.

Nous avons ensuite dans la seconde partie procéder l'étude de la signature électronique en essayant d'abord de le définir, mais aussi de voir ses intérêts pour nos structures municipales et donner les dispositions juridiques qui tourne autour de la signature électronique. La connaissance de ces dispositions est fondamentale pour toutes personnes ou entités désirant adoptées la signature électronique pour authentifier des documents notamment des actes d'état civil. Nous avons vu, aussi sur cette partie, la signature électronique sous l'angle technique en survolant les méthodes, algorithmes et procédés cryptographiques qui permettent la mise en œuvre de la signature électronique.

Au niveau de la troisième partie nous avons fait la description des outils pour faciliter l'implémentation et intégration de la signature électronique et des technologies de développements utilisées.

Sur la quatrième et dernière partie nous avons présenté la solution développée qui est une application web qui permet, travers un formulaire de signer et vérifier un acte d'état civil.

Cependant, soulignons que notre objectif n'est pas atteint à 100% et cela est due à des contraintes techniques, de la complexité de l'environnement cryptographique. Ainsi nous donnons en perspective :

- la possibilité d'intégrer la signature électronique au point qu'elle puisse être apposée sur l'acte d'état civil sous forme de QR code ;

- mettre en place une application mobile pour faire la vérification de la signature électronique à partir du QR code apposé sur l'acte d'état civil ;
- la possibilité de signer plusieurs actes en même temps ;
- élargir le choix sur les formats et types fichiers ;
- intégration de l'horodatage certifiée
- établir des statiques en temps réel sur les signatures effectuées.



# Bibliographie

- [6] *Mise en oeuvre de la dématérialisation: cas pratiques pour l'archivage électronique*. in InfoPro. Paris: Dunod, 2010.
- [11] D. Mouton, *Sécurité de la dématérialisation: De la signature électronique au coffre-fort numérique, une démarche de mise en oeuvre*. Editions Eyrolles, 2012.
- [19] P. Axayacatl, F. BERNAL, C. Antoine, et A. Serhrouchni, « Utilisations des certificats d'attribut pour accélérer l'usage de la signature électronique », févr. 2023.
- [20] J.-F. Pillou et J.-P. Bay, *Tout sur la sécurité informatique*, 5e éd. in CommentCaMarche.net. Malakoff: Dunod, 2020.
- [22] J.-G. Dumas, P. Lafourcade, P. Redon, et G. Poupard, *Architectures de sécurité pour Internet: protocoles, standards et déploiement*. Malakoff: Dunod, 2020.
- [23] D. Lamas, « La cryptographie », 2015.
- [25] G. Dubertret, *L'univers secret de la cryptographie*. in Sciences et plus. Paris: Vuibert, 2015.
- [26] P. Guillot, *La cryptologie: l'art des codes secrets*. in Une introduction à. Les Ulis: EDP sciences, 2013.
- [27] A. Nitaj, « La Cryptographie et la Confiance Numérique », 2013.
- [29] A. Zellagui et N. H.-S. ALI-PACHA, « Sécurité des fonctions de hachage cryptographique », *Commun. Sci. Technol.*, vol. 17, n° 18, p. 13-21, 2021.
- [31] P. A. F. BERNAL, C. ANTOINE, et A. SERHROUCHNI, « Utilisations des certificats d'attribut pour accélérer l'usage de la signature électronique ».
- [41] B. Lowagie, « Digital Signatures for PDF documents ». 2012.
- [59] M. Nebra, *Réalisez votre site web avec HTML 5 et CSS 3*, 3e éd. Paris: Éditions Eyrolles, 2023.

# Webographie

- [1] « La signature électronique : le pilier de la transformation numérique post-Covid ? - Le Monde Informatique », LeMondeInformatique. Consulté le: 2 février 2024. [En ligne]. Disponible sur: [https://www.lemondeinformatique.fr/publi\\_info/lire-la-signature-electronique-le-pilier-de-la-transformation-numerique-post-covid-642.html](https://www.lemondeinformatique.fr/publi_info/lire-la-signature-electronique-le-pilier-de-la-transformation-numerique-post-covid-642.html)
- [2] Y. Samb, « La gestion de l'état civil : acteurs et compétences - GROUPE TAATAAN ». Consulté le: 30 janvier 2024. [En ligne]. Disponible sur: <https://taataan.sn/la-gestion-de-letat-civil-acteurs-et-competences/>
- [3] « Digitalisation du système d'état civil : Plus de 8 millions d'actes déjà (...) - OSIRIS : Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal ». Consulté le: 18 mars 2024. [En ligne]. Disponible sur: <http://www.osiris.sn/Digitalisation-du-systeme-d-etat.html>
- [4] « SENEGAL-COLLECTIVITES-NUMERIQUE / L'Anec mise sur la digitalisation de l'état civil pour offrir aux citoyens des services fiables et sécurisés (Dg) - Agence de presse sénégalaise - APS ». Consulté le: 30 janvier 2024. [En ligne]. Disponible sur: <https://aps.sn/lanec-mise-sur-la-digitalisation-de-letat-civil-pour-offrir-aux-citoyens-des-services-fiables-et-securises-dg/>
- [5] « VERS LA NUMÉRISATION DE 15 MILLIONS D'ACTES D'ÉTAT CIVIL », RTS Officiel. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: <https://www.rts.sn/actualite/detail/a-la-une/vers-la-numerisation-de-15-millions-dactes-detat-civil>
- [7] J.-L. Parouty, R. Dirlwanger, et D. Vaufreydaz, « La signature électronique, contexte, applications et mise en oeuvre. », présenté à Journées Réseaux (JRES 2003), nov. 2003, p. 14 pages. Consulté le: 7 janvier 2023. [En ligne]. Disponible sur: <https://hal.inria.fr/inria-00326414>
- [8] F. Num, « La signature électronique : un outil devenu incontournable », francenum.gouv.fr. Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>
- [9] Fédération des Tiers de Confiance du numérique (FnTC), « Guide de la signature électronique ». Consulté le: 6 janvier 2023. [En ligne]. Disponible sur:

<https://www.leslivresblancs.fr/livre/informatique-et-logiciels/dematerialisation/guide-de-la-signature-electronique>

- [10] « GT-1-GT-Interop-Document-pedagogique-signature-electronique-20120627.pdf ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: <https://clubpsco.fr/wp-content/uploads/2012/07/GT-1-GT-Interop-Document-pedagogique-signature-electronique-20120627.pdf>
- [12] S. O. W. Djibril, « RETOUR SUR L'ADAPTATION DU DROIT AU NUMERIQUE », *Sci. Jurid. Polit.*, vol. 1, n° 001, 2016.
- [13] *Loi n° 2008 - 41 du 20 aout 2008 sur la cryptologie*. 2008. [En ligne]. Disponible sur: [https://www.adie.sn/sites/default/files/lois/2-loi\\_2008\\_41\\_sur\\_la\\_cryptologie\\_0.pdf](https://www.adie.sn/sites/default/files/lois/2-loi_2008_41_sur_la_cryptologie_0.pdf)
- [14] « Numerique 2025\_0.pdf ». Consulté le: 8 avril 2024. [En ligne]. Disponible sur: [https://www.adie.sn/sites/default/files/lois/Numerique%202025\\_0.pdf](https://www.adie.sn/sites/default/files/lois/Numerique%202025_0.pdf)
- [15] « Digitalisation | Société Sénégal Numérique S.A. » Consulté le: 27 janvier 2023. [En ligne]. Disponible sur: <https://www.adie.sn/projets/digitalisation>
- [16] M. Douté, « Signature électronique, vers des échanges sécurisés », janv. 2023.
- [17] « Avantages de l'utilisation de signatures électroniques ». Consulté le: 29 janvier 2023. [En ligne]. Disponible sur: <https://www.adobe.com/fr/sign/hub/features/how-to-solve-esignature-challenges-docx>
- [18] L. rédac' C. RH, « Quels sont les avantages d'une signature électronique ? », Culture RH. Consulté le: 31 janvier 2023. [En ligne]. Disponible sur: <https://culture-rh.com/quels-sont-les-avantages-dune-signature-electronique/>
- [21] « Qu'est-ce que la cryptographie ? - Définition de la cryptographie- AWS », Amazon Web Services, Inc. Consulté le: 11 février 2023. [En ligne]. Disponible sur: <https://aws.amazon.com/fr/what-is/cryptography/>
- [24] « Introduction à la sécurité informatique - Confidentialité et chiffrement ». Consulté le: 14 février 2023. [En ligne]. Disponible sur: [https://moodle.utc.fr/pluginfile.php/16777/mod\\_resource/content/0/SupportIntroSecu/co/CoursSecurite\\_32.html](https://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_32.html)
- [28] gay, « PPT - Cryptographie PowerPoint Presentation, free download - ID:2340078 », SlideServe. Consulté le: 4 mai 2024. [En ligne]. Disponible sur: <https://www.slideserve.com/gay/cryptographie>
- [30] « Décret 2008-720 30 Juin 2008 Certification Electronique Application Loi 2008 08 Transactions Electroniques ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: <https://www.adie.sn/sites/default/files/lois/3->

De%CC%81cret\_2008\_720\_30\_Juin\_2008\_Certification\_Electronique\_Application\_Loi\_2008\_08\_Transactions\_Electroniques\_1.pdf

- [32] « Tutorial PKI | PDF | Public-key cryptography | Cryptographie », Scribd. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: <https://fr.scribd.com/document/34112131/Tutorial-PKI>
- [33] « IBM Documentation ». Consulté le: 24 février 2023. [En ligne]. Disponible sur: <https://ibm.com/docs/fr/sig-and-i/10.0.0?topic=security-certificate-file-types>
- [34] « IBM Documentation ». Consulté le: 24 février 2023. [En ligne]. Disponible sur: <https://ibm.com/docs/fr/ibm-mq/9.2?topic=concepts-public-key-infrastructure-pki>
- [35] « Les PKI - cryptosec ». Consulté le: 24 février 2023. [En ligne]. Disponible sur: <https://www.cryptosec.org/?Les-PKI>
- [36] « PKI ». Consulté le: 30 novembre 2023. [En ligne]. Disponible sur: [https://igm.univ-mlv.fr/~dr/XPOSE2007/vma\\_PKI/pki.html](https://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/pki.html)
- [37] S. Tomáš, « Digital Signature Verification in PDF ». 10 mai 2018. [En ligne]. Disponible sur: <https://dspace.cvut.cz/bitstream/handle/10467/76810/F8-BP-2018-Stefan-Tomas-thesis.pdf?sequence=-1>
- [38] « Qu'est-ce que le format PDF ? Signification de PDF | Adobe ». Consulté le: 3 janvier 2024. [En ligne]. Disponible sur: <https://www.adobe.com/fr/acrobat/about-adobe-pdf.html>
- [39] K. Iqbal, « Format de fichier PDF - Qu'est-ce qu'un fichier PDF ? » Consulté le: 3 janvier 2024. [En ligne]. Disponible sur: <https://docs.fileformat.com/fr/pdf/>
- [40] « How to: PDF PAdES digital signatures using ETSI.CAdES.detached - Advanced and Qualified electronic signature marketplace ». Consulté le: 2 janvier 2024. [En ligne]. Disponible sur: <https://eideasy.com/pdf-pades-external-digital-signatures-using-etsi-cades-detached/>
- [42] Groupdocs, « API de traitement de documents pour les plates-formes .NET et Java », Groupdocs. Consulté le: 1 décembre 2023. [En ligne]. Disponible sur: <https://www.groupdocs.com/fr/>
- [43] « GroupDocs.Signature | API Java sur site à ESign Documents ». Consulté le: 4 décembre 2023. [En ligne]. Disponible sur: <https://releases.groupdocs.com/fr/signature/java/>
- [44] « eSign document with Barcode signature | Documentation ». Consulté le: 1 décembre 2023. [En ligne]. Disponible sur: <https://docs.groupdocs.com/signature/java/esign-document-with-barcode-signature/>

- [45] « eSign document with QR-code signature », Documentation. Consulté le: 1 décembre 2023. [En ligne]. Disponible sur: <https://docs.groupdocs.com/signature/java/esign-document-with-qr-code-signature/>
- [46] « Pricing - Purchase - groupdocs.com ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: <https://purchase.groupdocs.com/pricing>
- [47] iText PDF, « Electronic signatures for PDF documents », iText PDF. Consulté le: 5 décembre 2023. [En ligne]. Disponible sur: <https://itextpdf.com/solutions/electronic-signatures-pdf>
- [48] « Avis, prix et fonctionnalités d'iText - 2024 ». Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: <https://www3.technologyevaluation.com/solutions/53884/itext>
- [49] « Explorateur de magasins de clés ». Consulté le: 18 décembre 2023. [En ligne]. Disponible sur: <https://keystore-explorer.org/>
- [50] « Logiciels Java ». Consulté le: 18 décembre 2023. [En ligne]. Disponible sur: <https://www.oracle.com/fr/java/>
- [51] « Développons en Java - JCA (Java Cryptography Architecture) ». Consulté le: 18 décembre 2023. [En ligne]. Disponible sur: <https://www.jmdoudoux.fr/java/dej/chap-jca.htm#jca>
- [52] « Découvrez le framework Spring », OpenClassrooms. Consulté le: 19 décembre 2023. [En ligne]. Disponible sur: <https://openclassrooms.com/fr/courses/6900101-creez-une-application-java-avec-spring-boot/7074743-decouvrez-le-framework-spring>
- [53] « Qu'est-ce que Java Spring Boot ? | IBM ». Consulté le: 19 décembre 2023. [En ligne]. Disponible sur: <https://www.ibm.com/fr-fr/topics/java-spring-boot>
- [54] « Mettez en place l'environnement de développement », OpenClassrooms. Consulté le: 19 décembre 2023. [En ligne]. Disponible sur: <https://openclassrooms.com/fr/courses/4504856-implementez-une-architecture-orientee-services-soa-en-java/4856331-mettez-en-place-lenvironnement-de-developpement>
- [55] « Licences éducatives gratuites | Assistance à la communauté », JetBrains. Consulté le: 19 décembre 2023. [En ligne]. Disponible sur: <https://www.jetbrains.com/fr-fr/community/education/>
- [56] *Formation Apprendre l'HTML*. Consulté le: 20 décembre 2023. [En ligne Vidéo]. Disponible sur: <https://grafikart.fr/formations/html>
- [57] « Feuille de thym ». Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <https://www.thymeleaf.org/>

- [58] « Composer le HTML avec les CSS - Apprendre le développement web | MDN ». Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <https://developer.mozilla.org/fr/docs/Learn/CSS>
- [60] Sophie, « Qu'est-ce que le framework Bootstrap et quand l'utiliser ? », Blog Tuto.com. Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <http://fr.tuto.com/blog/2020/10/framework-bootstrap.htm>
- [61] gmz-jk, « Apprendre à utiliser le framework Bootstrap | Cours complet (2020) », Pierre Giraud. Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <https://www.pierre-giraud.com/bootstrap-apprendre-cours/>
- [62] « Qu'est-ce que le JavaScript ? - Apprendre le développement web | MDN ». Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: [https://developer.mozilla.org/fr/docs/Learn/JavaScript/First\\_steps/What\\_is\\_JavaScript](https://developer.mozilla.org/fr/docs/Learn/JavaScript/First_steps/What_is_JavaScript)
- [63] « JavaScript | MDN ». Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <https://developer.mozilla.org/fr/docs/Web/JavaScript>
- [64] « Introduction au cours jQuery », Pierre Giraud. Consulté le: 20 décembre 2023. [En ligne]. Disponible sur: <https://www.pierre-giraud.com/jquery-apprendre-cours/introduction/>
-