الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministre de l'enseignement supérieur et de la recherche scientifique

جامعة 20 أوت 1955 سكيكدة

Université 20 Août 1955 Skikda

Projet de fin d'études

En vue de l'obtention du diplôme de Master en informatique

Spécialité : RSD – Réseaux et systèmes distribués

Système de signature électronique

Etudiant : AMICHE Chemseddine

Encadrant : BOULEHOUACHE Soufiane

Année universitaire : 2023/2024

Dédicace

Je dédie ce modeste travail à :

Mes parents

Ma sœur et mon frère

A tous mes amies et collègues.

Remerciement

Tout d'abord, un grand merci au miséricordieux de m'avoir donné la chance, la santé, la volonté et le courage d'élaborer ce modeste mémoire et l'accomplir enfin après ces années d'études acharnés et de persévérance.

Je remercie mon encadrant S. BOULEHOUACHE pour sa disponibilité, son aide, ses encouragements et ses critiques constructives qui m'ont permis de mener à bien ce travail.

Je remercie les membres du jury qui m'ont honoré en jugeant ce travail.
J'exprime mes sincères remerciements à tous les professeurs qui m'ont enseigné durant mon parcours à l'université de Skikda.

Pour terminer, mes profonds remerciements vont également à toutes les personnes qui m'ont aidé et soutenue de près ou de loin à la réalisation de ce mémoire.

Résumé

Avec l'essor que rencontre l'informatique quotidiennement, une actualité spécifiée par les innovations dans les technologies de l'information et de la communication s'est facilement imposée, et par concomitance, des changements possibles dans la gestion des services publiques afin de répondre aux attentes des citoyens, qui sollicitent des services numériques en temps réel, à moindre coûts et de grande valeur. Le concept de la dématérialisation dans le secteur publique intervient, les organisations se voient obligées de s'adapter aux changements apportés avec le développement de la technologie afin d'atteindre leurs objectifs primordiaux tel que la transparence, l'interopérabilité et la satisfaction des citoyens, cela nécessite l'adoption d'outils technologiques pour moderniser le travail manuel.

En suivant ces évolutions technologiques, et dans le but de simplifier le cycle de vie du document interne et assurer sa valeur légale, les entreprises dorénavant doivent opter pour une dématérialisation numérique des documents administratifs consistant à remplacer les documents et supports d'information matériels ou papier par des fichiers numériques.

De nouvelles méthodes de gestion orientée vers l'administration électronique basée sur le principe l'élimination du papier, visant à améliorer l'efficacité de l'administration, tant sur le plan des délais, de la productivité des agents et de la qualité du service fourni doivent être aussi entreprises.

Mots-clés : Numérisation, dématérialisation, Signature électronique, Signature numérique, organisation.

Abstract

With the growth that computing encounters daily, a topicality specified by innovations in information and communication technologies has easily imposed itself, and concomitantly, possible changes in the management of public services in order to respond to the expectations of citizens, who request digital services in real time, at low cost and of high value. The concept of dematerialization in the public sector intervenes, organizations are obliged to adapt to the changes brought about with the development of technology in order to achieve their primordial objectives such as transparency, interoperability and citizen satisfaction, this requires the adoption of technological tools to modernize manual labor. In order to simplify the life cycle of internal documents and ensure the legal value in accordance with these technical development, companies need to choose digital non -materialization of management documents consisting of documents, information equipment or files. there is. Digital paper

The new management method is focused on electronic management in accordance with the principles of documents that aim to enhance the effectiveness of management, both in both conditions and conditions, conditions, and conditions, and in both conditions, and in both conditions. Is the quality of service quality.

Keywords : Digitization, non -materialized, electronic signature, digital signature, organization.

ملخص

مع محاولة التعرف على المعلومات اليومية، من السهل فرض واقعة محددة من خلال الابتكارات في تقنيات المعلومات والاتصالات، ومع تزامن التغييرات الممكنة في إدارة الخدمات العامة من أجل الاستجابة انتباه المواطنين الذين يطلبون الخدمات الرقمية في الوقت الحقيقي، بتكلفة أقل وقيمة كبيرة. مفهوم الدمج في القطاع العام المعني، يجب على المنظمات أن تتكيف مع التغييرات المناسبة مع تطور التكنولوجيا لتحقيق أهدافها الأولية مثل الشفافية وقابلية التشغيل البيني وإرضاء المواطنين، وهذا يتطلب اعتماد الأدوات التكنولوجية لتحديث العمل اليدوي.

في ظل هذه التطورات التكنولوجية، ومع تبسيط دورة حياة المستندات الداخلية وضمان القيمة القانونية، يتعين على الشركات اختيار تدوين رقمي للمستندات الإدارية المتوافقة مع استبدال المستندات ودعامات المعلومات أو الورق من خلال الملفات الرقمية.

أساليب جديدة للإدارة موجهة نحو الإدارة الإلكترونية تعتمد على مبدأ إزالة الورق، مما يؤدي إلى تحسين كفاءة الإدارة، بالإضافة إلى خطة التأخير وإنتاجية الوكلاء وجودة الخدمة من المهم أن تكون شركات أخرى.

الكلمات المفتاحية: الرقمنة، غير المتجسد، التوقيع الإلكتروني، التوقيع الرقمي، التنظيم.

Tableau des abréviations

Mot	**Abréviation de**
TIC	Technologies de l'Information et de la Communication
SI	Système d'information
GED	Gestion électronique de document
IAM	Identity and Access Management
CRLDP	Point de distribution de la liste de certificats révoqués
SKI	Identificateur de la clé du sujet
AKI	Identificateur de la clé de l'émetteur
CAdES	CMS Advanced Electronic Signature
XAdES	XML Advanced Electronic Signatures
PAdES	Advanced Electronic Signatures
XML-Dsig	XML Digital Signature
SEQ	La signature électronique qualifiée
UML	Unified Modeling Language

Liste des figures

Liste des tableaux

Sommaire

Introduction générale

Introduction générale

A. Contexte

Les signatures électroniques remplacent progressivement les signatures manuscrites, offrant une solution efficace, sécurisée et pratique pour authentifier les parties impliquées dans les transactions et les processus contractuels.

Le sujet de ce mémoire est d'étudier en détail le concept de signature électronique et d'étudier ses bases techniques et pratiques. Examinons de plus près les différentes technologies derrière les signatures électroniques, en nous concentrant sur leur fonctionnement et leurs implications en matière de sécurité et de confidentialité.

Nous examinons comment cela peut permettre de gagner du temps, d'augmenter l'efficacité et de réduire les coûts, tout en analysant les risques possibles et les meilleures pratiques pour améliorer la sécurité et la fiabilité.

B. Problématique

Dans un monde où les technologies numériques influencent de plus en plus nos interactions et nos transactions, la signature électronique peut-elle apporter une solution fiable et sécurisée pour authentifier les documents et garantir leur validité ?

Cette problématique soulève plusieurs questions clés :

1. Quels sont les principes fondamentaux de la signature électronique et comment fonctionne-t-elle techniquement ?
2. Quels sont les avantages d’une signature électronique par rapport aux signatures manuscrites traditionnelles ?
3. Quels sont les enjeux et les risques liés à la sécurité et à la confidentialité des données lors de l'utilisation d'une signature électronique ?

Après avoir explorer ses questions, nous pourrons mieux assimiler le rôle et l’importance de la signature électronique dans la société ainsi que les opportunités qu’elle peut apporter.

C. Objectifs

Ce mémoire sur la signature électronique vise à atteindre plusieurs objectifs :

- Supprimer le coût lié au papier et à l'impression ;
- Apporter un gain de temps en accélérant le processus de signature ;
- Signer rapidement les documents en format électronique ;
- Avoir une traçabilité des documents signés ;
- Diminuer les possibilités de falsifications des documents et les fausses signatures ;
- Sécuriser les données, de la signature électronique de documents à l'archivage.

D. Plan du mémoire

Le travail a comme intitulé « Système de signature électronique », pour sa réalisation nous avons subdivisé l'étude en trois chapitres hormis l'introduction et la conclusion générale :

- **Chapitre 01 :** L'état de l'art ;
- **Chapitre 02 :** Étude de l'existant et conception ;
- **Chapitre 03 :** Réalisation et implémentation.

Chapitre 01 : L’état de l’art

Introduction

L'intégration des Technologies de l'Information et de la Communication (TIC) revêt une importance cruciale pour toute organisation, même si elle les utilise depuis longtemps. Cependant, avec l'essor informatique, la transformation numérique pose un défi au travail traditionnel au sein des organisations, notamment en ce qui concerne la gestion des documents internes et leur authenticité. Ainsi, la dématérialisation s'est avérée nécessaire pour surmonter certains obstacles, tels que la réduction de l'usage intensif du papier (notamment dans le cadre du concept du zéro papier) et la prévention des falsifications de signature grâce à l'innovation de la signature électronique.

Dans cette section, nous présenterons une revue de la littérature sur ce thème dans son cadre théorique, ainsi que des généralités sur la dématérialisation, afin de donner un aperçu du domaine abordé dans le mémoire.

1. La dématérialisation

Un concept innovant qui doit être adopté au sein de l'organisation

1.1. Définition

Dématérialiser ses documents consiste à remplacer les documents depuis le format papier de son organisation par des fichiers numériques ou bien à les produire directement au format numérique via son système d'information SI (dématérialisation native). Elle vise également à stocker et à conserver ses documents électroniques sur des ordinateurs ou des serveurs informatiques. [1]

1.2. Les étapes clés de la dématérialisation

Tout d'abord, il est important de rappeler que la dématérialisation est une des facettes de la Gestion Électronique de Documents (GED) – l'autre étant la gestion des processus ou WORKFLOW.

La réussite du projet est aussi conditionnée par une prise en compte pertinente de facteurs très divers, de l'existant documentaire au réseau informatique. La transformation des objets physiques en une version numérique implique un certain nombre d'étapes, qui sont nécessaires et imposées [2] :

---

[1] : La dématérialisation : définition, méthodes et comparatifs, URL : https://www.archimag.com/demat-cloud/2019/11/13/glossaire-dematerialisation-10-mots-cles-definitions#securite

[2] : LUDOVIC DESAUBRY ; sur la dématérialisation des dossiers documentaires : les enjeux technique https://memsic.ccsd.cnrs.fr/mem_00523899/document ; consulté le 17/03/2024

- Préparation des documents ;
- Processus physique de numérisation ;
- Indexation des documents ;
- Stockage ;
- Contrôle.

Voici plusieurs aspects clés autour desquels un projet de dématérialisation peut être élaboré et développé :

- **Connaissance de l'existant :** Cette étape implique la création d'une liste exhaustive des différents types de documents à numériser ;
- **Évaluation de l'opportunité du projet :** Il est crucial d'évaluer l'opportunité du projet en prenant en compte des facteurs tels que le retour sur investissement, les risques et la réglementation ;
- **Réalisation du projet :** Une fois les études préliminaires achevées et les facteurs clés évalués, il est important de surveiller attentivement les points essentiels pour garantir le bon déroulement du projet ;
- **Conduite du changement :** L'introduction de la numérisation et éventuellement d'un système d'archivage électronique peut nécessiter des changements dans les habitudes de travail, ce qui demande la définition de nouvelles procédures ou règles ;
- **Suivi des archives :** Il est nécessaire de mettre en place des procédures pour assurer la qualité des archives conservées, ainsi que pour migrer les archives vers de nouveaux supports de stockage ou formats informatiques ;
- **Dématérialisation des traitements :** Au-delà de l'espace économisé et de la performance accrue dans la recherche documentaire, la dématérialisation peut également améliorer les processus. Il est donc important de recenser les traitements pouvant être dématérialisés et d'évaluer les bénéfices potentiels qui en découlent.

1.3. Les composants d'un service dématérialisé

On peut décomposer un service de dématérialisation en quatre grandes briques techniques, comme illustré dans la figure-1- qui représente les composants essentiels d'un service dématérialisé :

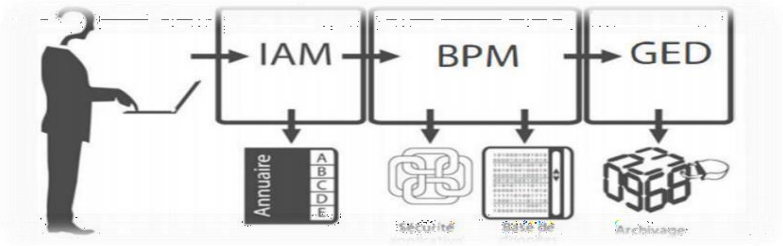

Figure -1- Les composants d'un service dématérialisé [3]

- **Gestion des identités et des accès (IAM, Identity and Access Management) :** Cette fonction permet de contrôler les utilisateurs du service, de leur attribuer des droits et de garantir leur utilisation conforme et sécurisée ;
- **Gestion des processus métier (BPM, Business Process Management) :** Elle vise à définir les flux d'informations entre les utilisateurs, notamment la circulation des données, les circuits de décision, le travail collaboratif et les traitements automatisés ;
- **Gestion électronique de documents (GED) :** Cette solution permet de gérer le cycle de vie de l'information, allant du simple classement, conservation et recherche de fichiers à des mécanismes sophistiqués d'indexation et de stockage sur le long terme, parfois appelé "archivage électronique" ;
- **Sécurité applicative :** Fondée sur la cryptographie, elle englobe les mécanismes visant à garantir l'intégrité des documents, leur provenance, leur confidentialité, l'authentification des personnes et la traçabilité des actions.

1.4. Les niveaux de la dématérialisation

La mise en œuvre de la dématérialisation peut avoir plusieurs niveaux, tant en termes de niveau de papiers conservé qu'en termes de valeur légale, voici différents niveaux de dématérialisation des documents :

---

[3] : Dimitri Mouton, 1iere édition, Eyrolles le juillet 12, 2012, une préface sur la sécurité de la dématérialisation de la signature électronique au coffre-fort numérique, 310pages

- **Numérisation des documents papier :** Il s'agit de convertir des documents papier en versions numériques pour faciliter leur transmission par voie électronique, sans valeur légale. Les originaux sont souvent conservés en version papier, tandis que les copies numérisées sont utilisées pour le travail quotidien, par exemple par courrier électronique ;
- **Transmission des documents numérisés :** Cette méthode implique la transmission des informations contenues dans des documents papier sous forme de données structurées. Cependant, seule la version papier conserve une valeur légale et fiscale, ce qui nécessite souvent sa conservation. Cette approche est largement utilisée dans les entreprises actuellement ;
- **Dématérialisation à la source :** Il s'agit de la transmission exclusive de données structurées, sans recours au papier. Dans ce cas, aucun document papier n'est nécessaire, ce qui en fait la méthode la plus simple à mettre en œuvre lorsque les informations à transmettre n'ont pas de valeur légale ;
- **Dématérialisation à valeur probante :** Cette approche implique la transmission de données numérisées, structurées ou non, qui sont signées électroniquement et archivées dans un "coffre-fort numérique". C'est la forme la plus avancée de dématérialisation, permettant de rendre totalement électroniques les documents ayant une valeur légale et fiscale. [4]

1.5. Système de gestion électronique des documents (GED)

1.5.1. Définition du GED

La gestion électronique de documents (GED) est un dispositif permettant l'acquisition, le classement (rangement et indexation) et l'exploitation des documents numériques, ces documents étant reçus où produits. La GED permet d'optimiser ou automatiser des opérations de gestion, d'exploitation et de contrôle des documents, via des WORK FLOWS ou flux de travail. Elle s'appuie sur une gestion des droits d'accès.

La GED est généralement considérée comme le fer de lance d'une famille de solutions de dématérialisation des processus et de traitement des données comprenant aussi la gestion électronique du courrier (GEC). [1][3]

---

[4] : BONITA Soft La dématérialisation, https://fr.bonitasoft.com/bibliotheque/la-dematerialisation , consulté le 18/03/2024

La gestion de contenu d'entreprise (ECM), qui vise à prendre en compte l'information numérique non structurée, hors bases de données, le records management (RM), pour la gestion des documents d'activité ou documents d'archive engageants pour l'entreprise, et le réseau social d'entreprise (RSE), outil facilitant le fonctionnement partagé et collaboratif dans l'entreprise.

1.5.2. Les catégories du GED

Il existe cinq catégories :

- **La GED administrative :** Il permet de numériser puis de classer les documents administratifs (factures, fiches techniques, formulaires, devis …) ;
- **La GED bureautique :** regroupe l'offre de progiciels de travail collaboratif permettant d'échanger des documents, de les lire dans leur format d'origine (Word, Excel, Powerpoint, Outlook …) ;
- **La GED COLD (Computer Output on Laser Disc) :** qui permet d'archiver sous une forme électronique les états produits par l'informatique d'un organisme (relevés de compte, factures, etc.) ;
- **La GED technique (GED métier) :** qui concerne la manipulation de documents dont le format et le contenu sont propres à un métier (plans, schémas etc.) [1]

1.5.3. Archivage électronique

- L'archivage électronique vise à conserver les documents numériques sur le long terme, notamment en constituant un fonds sécurisé des documents probatoires ou patrimoniaux de l'entreprise. Il englobe généralement les documents dans leur version finalisée ainsi que les données associées.
- Un système d'archivage électronique empêche toute altération des données et des documents. En respectant les durées de conservation définies, il interdit leur destruction en dehors d'une procédure de contrôle stricte. Pour cela, il repose sur une structure de conservation et de stockage organisée selon un plan de classement des activités.

Il est important de faire la distinction entre l'archivage électronique et le coffre-fort électronique/numérique. Le coffre-fort électronique est un dispositif technique visant à sécuriser les documents au format numérique qui y sont déposés afin de garantir leur intégrité. Il met en œuvre des processus d'identification et de traçabilité, mais il ne prend pas en compte les durées de conservation des documents. [1][3]

1.6. La sécurité de la dématérialisation

Est un ensemble de mesures prises pour diminuer les risques, en premier lieu elle se divise en trois familles complémentaires et il convient de les mettre en œuvre conjointement [3] :

1.6.1. La sécurité technique :

Cette dimension met en place des infrastructures robustes indépendamment des applications qui y sont exécutées. Les mesures prises ne sont pas spécifiques aux besoins métier, aux données traitées ou aux utilisateurs, mais visent plutôt à garantir un niveau de sécurité absolu en termes de disponibilité des machines et de résistance aux attaques, aux pannes et à d'autres événements nuisibles.

1.6.2. La sécurité applicative juridique :

Elle consiste à utiliser des mécanismes assurant la sécurité des données traitées au sein du service, y compris la sécurité juridique. Cela englobe les mesures prises au sein d'une application pour répondre aux besoins fonctionnels de sécurité du service, notamment en ce qui concerne les échanges et les traitements réalisés. Si le service implique des aspects juridiques tels que la conclusion de contrats, la capacité à prouver des événements, la garantie de confidentialité ou la conservation des documents à long terme, alors les mesures de sécurité juridique entrent dans cette catégorie.

1.6.3. La sécurité comportementale :

Cette dimension vise à sensibiliser les utilisateurs et à les former pour les inciter à éviter les comportements à risque, conscients ou inconscients. La majorité des attaques contre les systèmes d'information proviennent de l'intérieur, qu'il s'agisse d'employés malveillants, de personnes inconscientes des conséquences de leurs actions, d'anciens collaborateurs mécontents ou de pirates extérieurs ayant exploité l'ingénierie sociale pour obtenir des informations confidentielles. La mise en place de procédures précises, connues de tous, appliquées et régulièrement vérifiées, permet de prévenir de nombreux comportements inadaptés et de réduire les risques.

1.6.4. La chaîne de la sécurité :

Ces trois aspects de la sécurité (technique, applicative et comportementale) ne sont ni distincts ni exclusifs, mais complémentaires. Négliger l'un de ces aspects affaiblit l'ensemble du système d'information. En effet, la sécurité globale est aussi forte que son maillon le plus faible, et toute

lacune dans l'un des domaines peut compromettre la sécurité de l'ensemble du service dématérialisé.

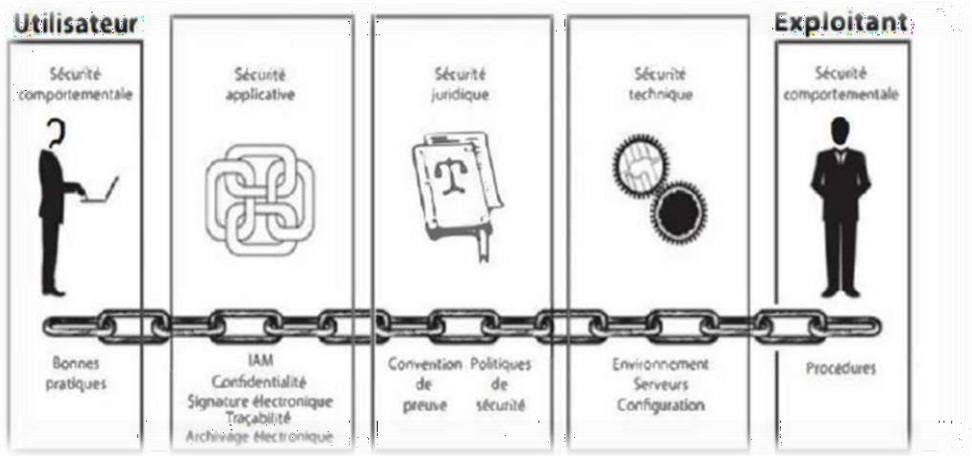

Figure 2- la chaine de sécurité [3]

2. Signature électronique

Une innovation qui défit la signature manuscrite

2.1. Définition de la signature électronique

La signature électronique assure l'intégrité d'un document dans le temps tout en authentifiant son auteur, de manière similaire à une signature manuscrite sur un document papier. Elle possède la même valeur légale qu'une signature manuscrite, mais se distingue par le fait qu'elle n'est pas visuelle, mais plutôt une suite de caractères.

La mise en place de la signature électronique implique l'utilisation d'une clé privée, un code chiffré, pour identifier l'auteur. Un logiciel effectue un hachage du message électronique, le rendant totalement illisible grâce à la cryptographie.

La signature électronique est un document électronique spécifique qui doit être logiquement lié (par des liens numériques) au document électronique principal, qui est en réalité l'objet de la signature électronique. [5]

[5] : Jean-Luc PAROUTY, Roland DIRLEWANGER, Dominique VAUFREYDAZ, la signature électronique, contexte, applications et mise en œuvre.

2.2. Les Caractéristiques d'une signature électronique

- **Authentique :** L'identité du signataire doit être vérifiable et retrouvable ;
- **Infalsifiable :** La signature ne peut être falsifiée, ce qui empêche toute personne de se faire passer pour un autre ;
- **Non-réutilisable :** La signature est spécifique au document signé et ne peut être déplacée vers un autre document ;
- **Inaltérable :** Une fois le document signé, il est impossible de le modifier sans altérer la signature ;
- **Irrévocable :** La personne qui a signé ne peut nier sa signature une fois qu'elle est apposée sur le document. [6]

2.3. Niveau de signatures électroniques

Selon l'article 7, 8 et 9 de la loi n°15-04 du 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques, publiée dans le Journal Officiel de la République Algérienne N°6, les points suivants sont établis (voir ANNEXE 01) :

- Seule la signature électronique est assimilée à la signature manuscrite, qu'elle soit le fait d'une personne physique ou morale ;
- La signature électronique repose sur un certificat électronique qualifié. Elle se présente sous forme électronique et est créée par un dispositif sécurisé ;
- La signature électronique est juridiquement efficace et valide conformément aux dispositions de la loi.

2.3.1. La signature électronique qualifiée (SEQ) : elle doit répondre aux conditions suivantes

- La signature électronique avancée est créée à l'aide d'un dispositif de création qualifié et repose sur un certificat qualifié de signature électronique ;
- Elle est strictement liée au signataire et ne peut être utilisée que par lui ;
- Associée à un carnet d'identification du signataire pour garantir son authenticité ;
- Conçue selon des moyens sécurisés pour protéger son intégrité et son authenticité ;
- Créée de manière à ce que le signataire puisse la conserver sous son contrôle exclusif ; [6] :

Bill FASSINOU, URL : https://www.developpez.com/actu/248771/Des-chercheurs-ont-reussi-a-briser-des-signatures-numeriques-de-documents-PDF-de-21-des-visionneuses-PDF-les-plus-connues/

- Elle est liée aux données auxquelles elle se rapporte de manière à ce que toute modification ultérieure des données soit détectée.

2.4. Le contenu et les formats des signatures électroniques

Une fois le processus décrit précédemment réaliser, la signature électronique doit être complétée par les éléments nécessaires à sa vérification par le destinataire. Doit être mise en forme à l'aide de l'un des formats standards de la signature électronique. Les éléments complémentaires à ajouter dans une signature électronique sont au nombre de trois :

- Le certificat du signataire et 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 ;
- Une preuve de non-révocation du certificat du signataire. [3]

2.4.1. Les différents standards

Les formats de signature électronique les plus courants organisent le stockage de la signature et du contenu signé selon l'un des trois modes suivants :

- **Signature enveloppée ou encapsulée :** Dans ce mode, les données signées sont incluses à l'intérieur de la signature elle-même. Cela signifie que les données signées sont encapsulées dans la signature électronique, formant ainsi une seule entité ;
- **Signature enveloppante :** Contrairement à la signature enveloppée, dans ce mode, la signature électronique est intégrée à la structure des données signées. Autrement dit, la signature est enveloppée par les données elles-mêmes, faisant partie intégrante de la structure des données signées ;
- **Signature détachée :** Dans ce mode, la signature électronique et les données signées sont stockées dans deux structures distinctes. La signature est séparée des données signées, ce qui permet de les stocker et de les gérer indépendamment l'une de l'autre.

On trouve les signatures sous plusieurs formats :

- ***ADVANCED ELECTRONIC SIGNATURE* « CMS » Binaires :** PKCS #7 / CMS / CAdES est une norme qui permet la signature « enveloppée » ou « détachée » ;
- ***ADVANCED ELECTRONIC SIGNATURES* « XML » :** XML-Sig / XML-DSig / XAdES est une norme améliorant la norme XMLDsig, avec le format XAdES, les informations relatives à la signature (identité, date…) sont dans le fichier xml qui est généré (signature « enveloppée » ;
- ***ADVANCED ELECTRONIC SIGNATURES* « PDF » :** PAdES est une norme pour laquelle la signature peut être identifiable dans le fichier et visible.

2.4.2. Formats de document signé

En principe, il est possible de signer électroniquement tous les types de fichiers (Word, XML, PDF, JPG, etc.). Néanmoins, les pratiques recommandées favorisent l'utilisation du format PDF, car il offre une meilleure préservation et protection du contenu.

2.4.3. Types de données à signer électroniquement

Il n'existe aucune restriction technique quant aux types de données pouvant être signés électroniquement. La signature peut être appliquée aussi bien à des documents bureautiques (comme les traitements de texte, les tableurs, les présentations, les fichiers PDF) qu'à des images, des données informatiques (comme les fichiers XML, les extractions de bases de données), des plans d'architecte, des données géographiques, des fichiers audios, des vidéos, et bien d'autres encore. Cependant, il convient de noter qu'il existe une limitation liée au format de la signature : par exemple, une signature PAdES ne peut être apposée que sur un document PDF. En revanche, les formats XAdES et CAdES permettent de signer tous les types de documents, quel que soit leur format.

Deux cas particuliers nécessitent une attention spécifique : les signatures apposées sur des fichiers ZIP et les e-mails. Il est important de souligner que la signature électronique apposée sur un fichier ZIP contenant plusieurs documents ne vaut pas signature individuelle de chacun des documents contenus dans le fichier ZIP. En d'autres termes, signer l'enveloppe (le fichier ZIP) ne signifie pas signer le contenu spécifique de l'enveloppe.

2.5. La vérification d'une signature électronique

La vérification d'une signature électronique se divise en trois étapes distinctes :

- La vérification technique, qui implique de s'assurer que la signature est correctement formatée sur le plan technique et qu'elle correspond précisément au document signé ;
- La vérification de la chaîne de confiance, qui requiert de vérifier que le certificat du signataire provient d'une autorité de certification réputée et fiable ;
- La vérification juridique, qui consiste à évaluer la validité de la signature dans le contexte spécifique de son utilisation, en conformité avec les exigences légales applicables. [3]

2.5.1. La vérification technique

Le processus de vérification technique est automatisé par le logiciel de vérification de signature, et peut être décomposé comme suit (illustré dans la figure-3 ci-dessous) :

- Extraction du certificat du signataire à partir de l'enveloppe de signature ;

- Extraction de la clé publique du signataire à partir du certificat ;
- Utilisation de cette clé publique pour effectuer un calcul RSA sur la signature, produisant ainsi le hachage du document initialement signé ;
- Calcul du hachage du document reçu ;
- Comparaison du hachage calculé avec celui obtenu à partir du calcul RSA : si les deux hachages sont identiques, la signature est valide car elle correspond au document reçu ; dans le cas contraire, soit le document a été altéré après la signature, soit la signature portait sur un autre document, rendant ainsi la signature invalide.

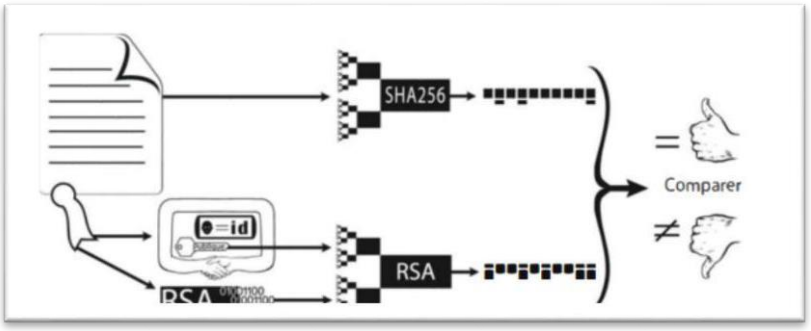

Figure -3- vérification technique de la signature électronique [3]

2.5.2. La vérification de la chaine de confiance

L'enveloppe de signature englobe l'intégralité de la « chaîne de certification », comprenant le certificat du signataire, qui est émis par une autorité de certification, ainsi que les certificats des autorités de certification intermédiaires.

Une fois que la validité technique de la signature a été confirmée, il est nécessaire de vérifier les points suivants :

- La validité du certificat du signataire ;
- Que l'un des certificats de cette chaîne a été désigné comme étant digne de confiance dans le contexte de l'application en question.

2.5.3. La vérification juridique

Malheureusement, la vérification juridique de la signature électronique est souvent négligée lors des processus de vérification, car elle est entièrement tributaire du contexte d'application et nécessite donc une intervention humaine ; elle est difficilement automatisable. Cette étape de vérification vise à garantir que le signataire est légitimement autorisé à apposer sa signature sur le document.

2.6. Fondement technologique

La signature électronique sécurisée est intimement liée aux technologies de cryptographie à clé publique, également connue sous le nom de cryptographie asymétrique. La cryptologie comprend deux branches principales : la cryptographie et la cryptanalyse. Son objectif est de sécuriser les messages ou les données en concevant des procédés ou des algorithmes de chiffrement utilisant des secrets ou des clés, garantissant ainsi la confidentialité, l'authenticité et l'intégrité des données.

Les clés, qui se présentent sous forme de séquences d'octets, possèdent des caractéristiques spécifiques propres à l'algorithme auquel elles sont associées. Par conséquent, il est risqué de mesurer la robustesse d'un algorithme uniquement en fonction de la longueur de ses clés.

La cryptanalyse, qui consiste à analyser des textes chiffrés pour retrouver les informations cachées, constitue la composante complémentaire de la cryptographie. Ainsi, les cryptographes, qui détiennent les clés, effectuent le chiffrement ou le déchiffrement, tandis que les cryptanalystes, qui n'ont pas accès aux clés, s'adonnent au décryptage. [7]

2.6.1. Les aspects cryptographiques de la signature électronique

Réaliser une signature électronique est un mécanisme de scellement cryptographique.

La signature électronique consiste à effectuer un calcul RSA à l'aide de la clé privée sur le document à signer mais cela n'était possible que si le document comportait moins de 256 caractères (pour une bi-clé de 2 048 bits) - ce qui est notoirement insuffisant.

Le rôle de la signature électronique étant de marquer son engagement sur les termes d'un document, il est fondamental que le calcul RSA, qui lie le document au signataire, porte bien sur l'intégralité du contenu du document signé.

Pour ramener un document de 200 kilo-octets ou plus à moins de 256 octets, on utilise une fonction de hash (SHA256 ou MDC55). Le déroulement d'une signature électronique, du strict point de vue cryptographique, est donc le suivant :

- Le document est condensé à l'aide d'une fonction de hash, par exemple SHA256 ;
- Le hash du document est soumis à un calcul RSA à l'aide de la clé privée du signataire (cette opération nécessite la saisie du code PIN du signataire si le certificat est sur un support physique) ;

---

[7] : La signature électronique (2018) CLUSIF, URL : https://clusif.fr, consulté le 24/03/2024

- Le résultat de ce calcul est, au sens technique, un scellement garantissant l'intégrité du document et réalisé par un acteur identifié, le signataire.

2.6.2. La cryptographie asymétrique

- Lorsqu'il est question de deux clés, on parle de cryptographie asymétrique ; l'une est dénommée publique car elle est accessible à tout le monde, tandis que l'autre est privée car elle n'est connue et accessible que par son propriétaire ;
- Bien qu'elles soient directement liées à l'identité de l'utilisateur, les deux clés utilisées doivent être aléatoires. La connaissance de la clé publique ne permet pas de déduire la clé privée, mais inversement, la connaissance de la clé privée permet généralement de déduire la clé publique. Bien qu'elles puissent être facilement générées, il existe une corrélation entre elles : toute donnée chiffrée par l'une des clés ne peut être déchiffrée qu'avec l'autre clé ;
- La principale utilisation de la cryptographie asymétrique est initialement le chiffrement de données ;

Dans la figure-4- ci-dessous, un document est envoyé de manière confidentielle à Alice en utilisant sa clé publique pour chiffrer le document, lequel ne peut être déchiffré qu'à l'aide de sa clé privée propre à elle.

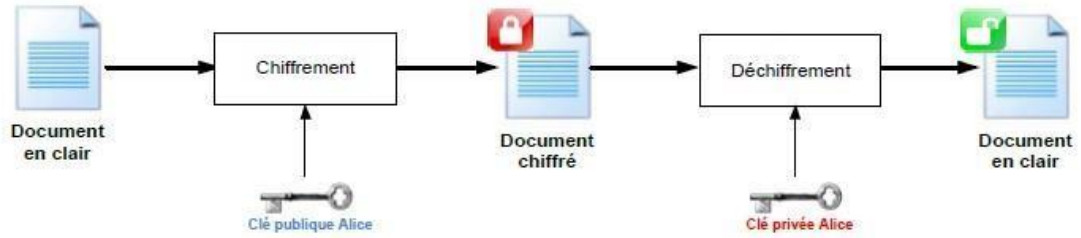

Figure -4- Principe du chiffrement asymétrique [7]

- L'une des principales caractéristiques des systèmes asymétriques est leur capacité à mettre en œuvre la signature électronique, (comme illustré dans la Figure-4.) ;
- Contrairement au chiffrement, la signature est réalisée en utilisant la clé privée du signataire, permettant à toutes ses parties destinataires de vérifier sa signature en utilisant sa clé publique ;

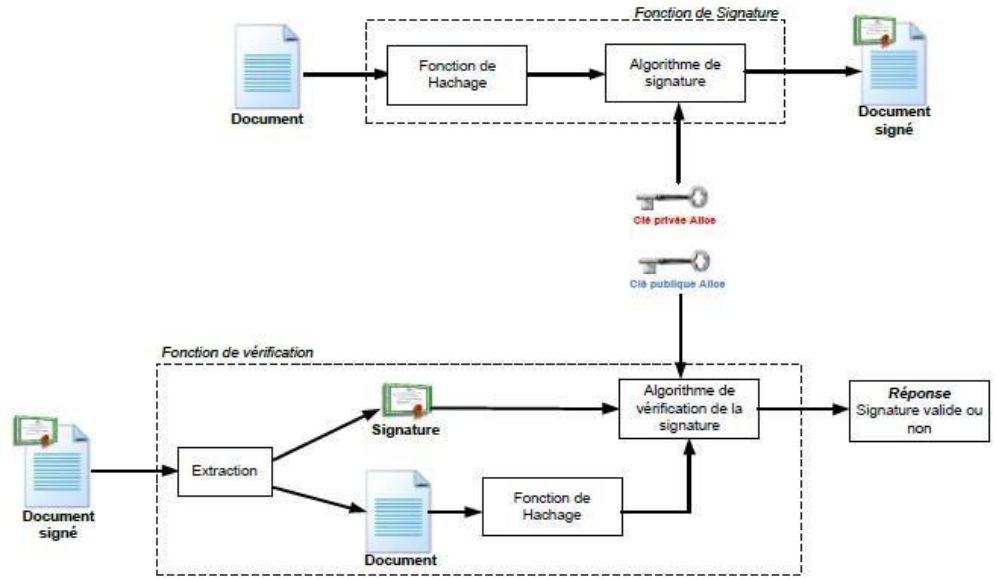

Figure -5- processus de signature [7]

- La cryptographie asymétrique présente deux limitations principales :
- Les données que peuvent traiter des algorithmes tels que RSA sont limitées à la taille de la bi-clé, ce qui nécessite parfois de découper les documents ;
- De plus, les performances de la cryptographie asymétrique sont souvent insatisfaisantes ;
- Pour pallier ces limitations, une solution consiste à utiliser conjointement la cryptographie symétrique pour le chiffrement. Quant à la signature électronique, elle fait appel aux fonctions de hachage, (comme décrit dans la Figure -5-.).

2.6.3. La cryptographie symétrique

- Contrairement à la cryptographie asymétrique, les systèmes symétriques utilisent une seule et unique clé partagée entre l'émetteur et le récepteur ;
- Les algorithmes de ces systèmes se basent sur des opérations élémentaires telles que des permutations, des rotations, des expansions et des réductions, qui manipulent les caractères du texte en clair et ceux de la clé ;

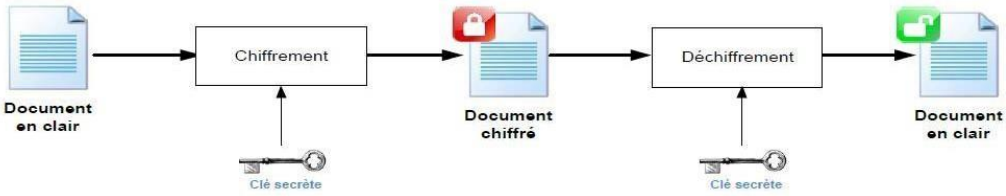

Figure-6- Principe du chiffrement symétrique [7]

- Les systèmes symétriques sont principalement employés pour garantir la confidentialité des données transmises, mais ils peuvent aussi servir dans des protocoles d'authentification de partenaires ou de vérification d'intégrité ;
- La principale contrainte liée à l'utilisation de la cryptographie symétrique concerne la nécessité de transmettre la clé secrète de manière confidentielle.

2.6.4. Fonction de hachage (condensat ou empreinte)

Les fonctions de hachage sont des mécanismes unidirectionnels et « sans collision », produisant une sortie de taille fixe appelée empreinte ou condensat, qui est caractéristique des données en entrée.

Ces fonctions sont dites unidirectionnelles car il est impossible de retrouver les données originales à partir de l'empreinte. Une fonction est considérée comme « sans collision » ou « injective » lorsqu'il est extrêmement difficile de trouver deux ensembles de données différents qui produisent la même empreinte. Calculer le condensat d'un document et le comparer à sa valeur initiale permet de vérifier l'intégrité d'un document.

Une fonction de hachage doit respecter les règles et propriétés suivantes :

- La longueur de l'empreinte doit toujours être la même, quelle que soit la longueur des données en entrée ;
- Il est impossible de retrouver les données d'origine à partir de l'empreinte : les fonctions de hachage ne fonctionnent que dans un sens ;
- Il ne doit pas être possible de prédire une empreinte (il est impossible de deviner l'empreinte en examinant les données) ;
- Enfin, pour obtenir des données différentes, les empreintes doivent être différentes ; [5]

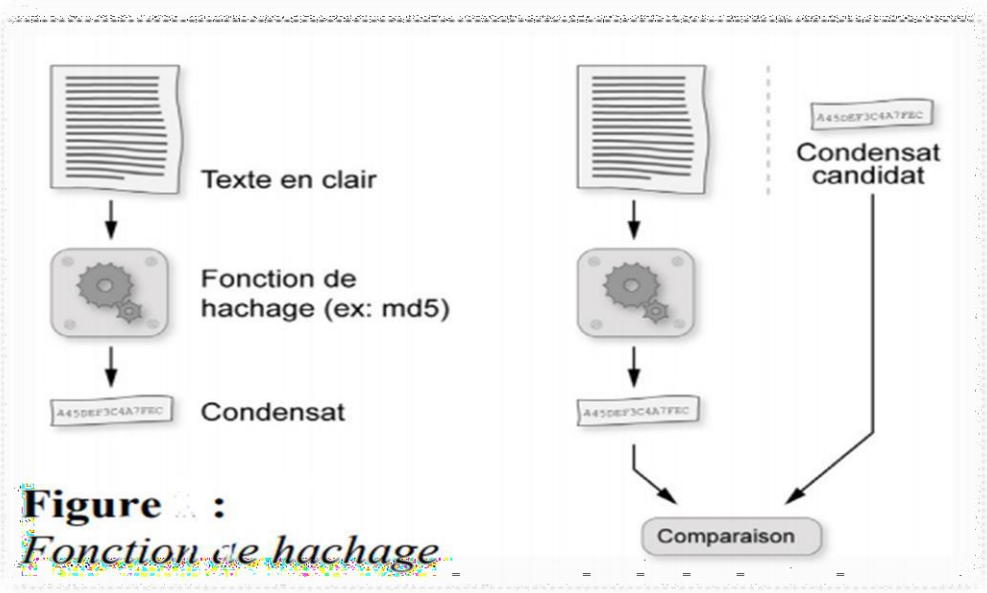

Figure -7- fonction de hachage [5]

- Il existe plusieurs algorithmes pour calculer l'empreinte, on utilise comme exemple le hash SHA256 dans l'exemple ci-dessous : le tableau N°1 représente différents scriptes qui ont été condensé grâce à la fonction de hash SHA256 :

Donnée	Condensant
Chemseddine AMICHE	Cdffcad155a1aeed21aa19b1887f77960149441ffb63a616c94a591c003b05b3
Système de signature électronique	C1daf2284d7dfabdd6f73f54f06443333ea07013a1923b36cb6cafc3a9dda9f4
Spécialité réseaux et systèmes distribués	83746beda40181f3ee8cfa3b65d4d52c40ff2dcd2a6585b2122729429803fc4d
Université 20 août 1955 Skikda	4831749c95d62858f1d341c17a0ad231421995e31a5c909c2ad69909434fe396

Tableau N°1 : Exemples d'empreintes

Source : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html

[8] : Constructions et vérification d'une signature électronique, URL : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html

2.7. Valeur juridique de la signature électronique

En Algérie, la réglementation sur la signature électronique est définie par la loi n°15-04 du 1er février 2015, qui établit les principes généraux relatifs à la signature et à la certification électroniques (voir ANNEXE 01, 02).

Conformément aux articles de la loi susmentionnée :

- **Art. 6 :** La fonction première d'une signature électronique est d'authentifier l'identité du signataire et de témoigner de son accord avec le contenu de l'écrit électronique ;
- **Art. 7 :** Une signature électronique qualifiée répond aux critères suivants :
    - Elle est basée sur un certificat électronique qualifié ;
    - Elle permet l'identification du signataire ;
    - Elle est réalisée à l'aide d'un dispositif sécurisé de création de signature électronique ;
    - Elle est spécifiquement liée au signataire ;
    - Elle est créée par des moyens que seul le signataire peut contrôler exclusivement ;
    - Elle est liée aux données auxquelles elle se rapporte, de manière à détecter toute modification ultérieure de ces données ;
- **Art. 8 :** Seule la signature électronique qualifiée est considérée équivalente à une signature manuscrite, qu'elle soit émise par une personne physique ou morale ;
- **Art. 9 :** En dépit des dispositions de l'article 8, une signature électronique ne peut être privée de sa validité juridique ni être rejetée comme preuve en justice pour les motifs suivants :
    - Elle est sous forme électronique ;
    - Elle ne repose pas sur un certificat électronique qualifié ;
    - Elle n'est pas créée par un dispositif sécurisé de création de signature électronique. [8]

Annexe 01 : loi n°15-04 du 1/02/2015 : les règles relatives à la signature et à la certification électronique

Annexe 02 : Les autorités algériennes de certification électronique

2.8. Construction et vérification d'une signature électronique

À partir du Journal Officiel de la République Algérienne N°6, conformément aux articles 12 et 13 de la loi n°15-04 du 1er février 2015 établissant les règles générales relatives à la signature et à la certification électronique, le dispositif de vérification de la signature électronique qualifiée doit être fiable et répondre aux critères suivants :

- Les données utilisées pour la vérification de la signature électronique doivent correspondre aux données affichées lors de cette vérification ;
- La vérification de la signature électronique doit être effectuée de manière sécurisée et le résultat de cette vérification doit être correctement affiché ;
- Le contenu des données signées doit pouvoir être déterminé de manière sécurisée lors de la vérification de la signature électronique ;
- L'authenticité et la validité du certificat électronique requis pour la vérification de la signature électronique doivent être vérifiées de manière sécurisée ;
- Le résultat de la vérification ainsi que l'identité du signataire doivent être clairement et correctement affichés ;
- La signature électronique fait appel à deux familles d'algorithmes : les algorithmes de chiffrement asymétriques ou à clé publique et les fonctions de hachage, afin de garantir l'authenticité, l'intégrité, l'in-falsifiabilité, la non-réutilisabilité, la non-altérabilité et la non-irrévocabilité d'un document ;
- Les algorithmes asymétriques couramment utilisés sont RSA et DSA, tandis que les fonctions de hachage les plus courantes sont MD5 et SHA ;
- Par exemple, si la direction souhaite envoyer un document signé électroniquement à Chemseddine Amiche, elle commence par générer l'empreinte du document à l'aide d'une fonction de hachage ;
- Ensuite, elle crypte cette empreinte avec sa clé privée ;[5]

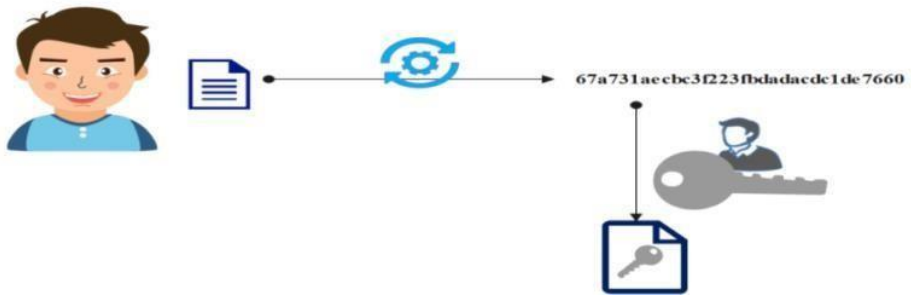

Figure -8- Génération de l'empreinte puis crypter par clé privée

Source : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html

- Elle obtient ainsi la signature de son document. Ensuite, elle transmet ces deux éléments à Chemseddine ;
- Pour vérifier l'authenticité du document, Chemseddine doit d'abord décrypter la signature en utilisant la clé publique de la direction. Si cela échoue, cela signifie que le document n'a pas été émis par la direction de l'école ;
- Ensuite, Chemseddine crée l'empreinte du document qu'elle a reçu en utilisant la même fonction de hachage que celle de la direction (on suppose qu'ils suivent un protocole déjà établi) ;
- Enfin, il compare l'empreinte générée avec celle provenant de la signature.

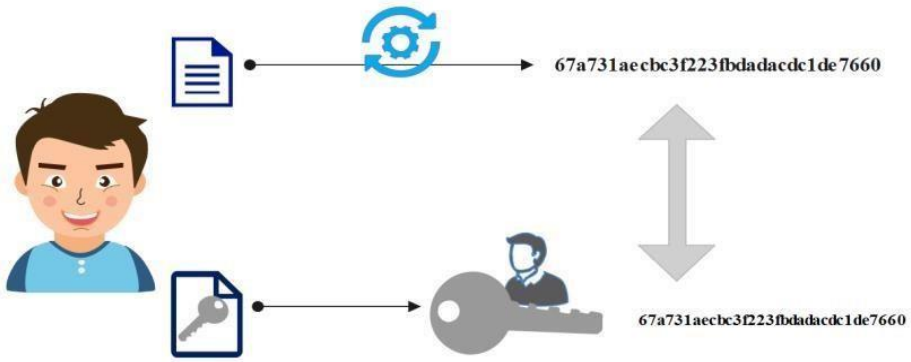

Figure -9- Décrypter l'empreinte envoyé par la clé publique

Source : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html

Si les deux empreintes sont identiques, cela valide la signature. Ainsi, nous pouvons être certains que :

- Le document a été envoyé par la direction ;
- Le document n'a pas été altéré depuis sa signature par la direction.

En revanche, si les empreintes diffèrent, cela pourrait signifier que :

- Le document a été altéré depuis sa signature par la direction ;
- Le document reçu n'est pas celui que la direction a signé.

2.8.1. Confidentialité de la clé de confiance

- Le processus de vérification de la signature repose entièrement sur la confiance accordée par le vérificateur à la clé publique de l'émetteur ;
- Dans l'exemple précédent, l'approche consiste à transmettre à Chemseddine, par un moyen quelconque, la clé publique d'un tiers en le persuadant qu'il s'agit de celle de la direction ;
- Tout message signé avec la clé privée correspondante sera considéré par Chemseddine comme étant signé par la direction ;
- Le principe algorithmique de la signature électronique implique que la transmission sécurisée de la clé publique de la direction à Chemseddine soit primordiale. La direction signe un ensemble de clés publiques qu'elle peut certifier ;
- Elle transmet à Chemseddine sa propre clé publique de manière sécurisée, ainsi que la liste des clés publiques qu'elle a signées, via un canal quelconque. Chemseddine peut alors choisir de faire confiance à toutes ces clés, et éventuellement à celles signées par les titulaires de ces clés ;
- Toutefois, garantir que chaque utilisateur possède à tout moment toutes les clés publiques nécessaires semble difficile ;
- Une solution efficace consiste à faire signer l'identité ainsi que la clé publique de chaque utilisateur par une autorité de confiance commune à tous les partenaires ;
- Chaque utilisateur n'a alors besoin de récupérer qu'une seule clé publique, celle de l'autorité, pour valider les clés publiques de tous les autres utilisateurs. Cette approche est à la base des infrastructures de gestion de clés (IGC) ;
- Dans ce système, un certificat contient diverses informations sur son titulaire, telles que son nom, prénom, adresse électronique, etc. ;
- Ces informations sont signées par la clé privée de l'autorité de certification, garantissant ainsi leur authenticité. Pour faciliter la vérification des signatures, les documents ou messages signés contiennent le certificat du signataire ;
- Pour vérifier les signatures des messages reçus de la direction, Chemseddine extrait d'abord le certificat de la direction du document ou du message, puis vérifie la signature du certificat

en utilisant la clé publique contenue dans le certificat de l'autorité de certification qui a émis le certificat de la direction ;

- Ensuite, il vérifie la validité du certificat et enfin, il vérifie la signature du message en utilisant la clé publique contenue dans le certificat de la direction ;
- Ainsi, la confiance dans les clés publiques d'une population d'utilisateurs potentiels est ramenée à la confiance dans un petit nombre de clés publiques d'autorités de certification.

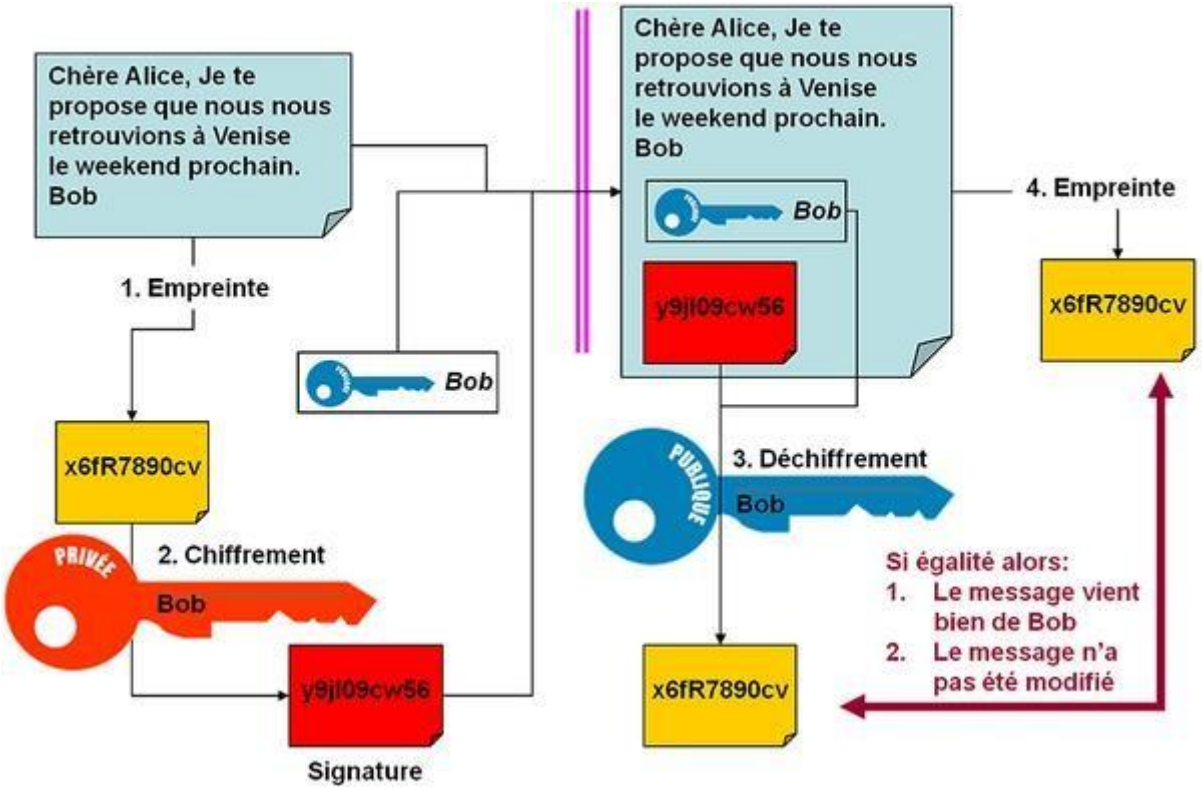

Figure -10- construction et vérification d'une signature électronique [5]

Source : https://stormimon.developpez.com/dotnet/signature-electronique/

2.9. Horodatage

L'horodatage électronique se présente comme un ensemble de données électroniques associées à d'autres données également électroniques à un instant précis, prouvant ainsi l'existence de ces données à cette date et heure spécifiques.

Les fonctions de l'horodatage électronique sont les suivantes :

- Fixer de manière précise la date d'un document ;
- Établir un certificat attestant de l'existence d'une donnée à un moment donné ou de l'exécution d'une opération électronique spécifique (comme une signature électronique ou l'envoi recommandé électronique).

Un horodatage électronique est qualifié s'il répond aux critères suivants :

- Lire la date et l'heure des données de manière à exclure raisonnablement la possibilité de modification indétectable des données ;
- Être réalisé sur une horloge exacte synchronisée avec le temps universel coordonné ;
- Être signé à l'aide d'une signature électronique avancée ou être scellé avec un cachet électronique avancé fourni par un prestataire de services de confiance qualifié, ou par une méthode équivalente. [5]

2.10. Certificat de signature électronique

2.10.1. Définition du certificat électronique

- Le certificat de signature électronique qualifiée est émis par une autorité de certification (AC) agréée par le gouvernement, respectant des normes strictes en matière de fiabilité, de stockage du certificat, de détection de fraude et de révocation, ainsi que des contrôles financiers et de sécurité. Il établit un lien certain entre le signataire et sa signature. Individuel et spécifique, ce certificat est attribué à une personne physique après vérification de documents légaux et de son identité réelle ;
- Ce certificat est utilisé par la personne pour signer électroniquement des documents, engageant ainsi l'entreprise dans son ensemble. Il est similaire à une carte d'identité numérique authentique car sa délivrance est soumise à des processus rigoureux impliquant une vérification physique de l'identité de la personne ;
- Le certificat se présente sous la forme d'un fichier contenant des informations sur le signataire ainsi qu'une clé de cryptographie permettant d'effectuer des opérations de signature ; [3]

- Selon l'article 15 de la loi n°15-04 du 1er février 2015 fixant les règles générales relatives à la signature et à la certification électronique, le certificat électronique qualifié doit respecter les exigences suivantes (voir ANNEXE 02) :
- Il doit être émis par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée.
- Il ne peut être délivré qu'au signataire ;
- Le certificat électronique, un petit fichier créé et géré par un programme spécialement conçu à cet effet, doit comporter diverses informations, notamment celles relatives au signataire. [7] :

Version du certificat : indiquant que le certificat électronique est délivré à titre qualifié
Numéro de série : code d'identité du certificat électronique
Description de l'algorithme de signature du certificat
Nom du prestataire de service autorisé
Période de validité : date de début et de fin de validité du certificat
Nom du signataire : nom du détenteur du certificat
Qualité spécifique du signataire : Clé publique du détenteur du certificat
Identité l'autorité de certification
Identité du détenteur du certificat
Extension (optionnel)
Signature de l'autorité de certification

Tableau N°2 : Structure simplifiée d'un certificat électronique selon l'ART 15 et la norme X.09 [7]

- X.509 est la norme la plus répandue pour la création des certificats. Elle spécifie les formats des certificats à clé publique, les listes de révocation de certificat, les attributs de certificat, ainsi qu'un algorithme de validation du chemin de certification. Cette norme est définie par l'Union internationale des télécommunications (UIT).

2.10.2. Le format du certificat

Un certificat est un fichier qui contient des informations sur son porteur et sur les utilisations autorisées de ce certificat. Il est structuré selon le modèle de la famille X.500 de l'UIT, qui est également utilisé dans la conception des annuaires LDAP. Ce fichier est signé numériquement par son émetteur, communément appelé « autorité de certification ».

Le format des certificats est défini par la norme X.509v3, qui est spécifiée plus en détail dans la norme RFC 5280. Il n'y a pas de différence fondamentale entre un certificat attribué à une personne physique, à un serveur ou à une autorité de certification.

Les principales parties du certificat :

- Les informations relatives au porteur du certificat ;
- Les détails techniques concernant le certificat et la clé publique certifiée ;
- Les indications sur les utilisations autorisées du certificat ;
- Les informations sur l'autorité émettrice du certificat ;
- La signature numérique apposée sur le certificat par son émetteur.

L'ensemble des informations contenues dans les certificats d'une même famille forment ce que l'on appelle le « profil » du certificat.

2.10.3. Les informations techniques sur le certificat

Les données techniques présentes dans un certificat sont diverses :

- Des informations purement techniques, telles que la version du certificat qui indique la conformité à la norme X.509 ;
- Le numéro de série, unique parmi les certificats émis par le même organisme ;
- Les détails de la clé publique associée au certificat, comprenant le type de clé (généralement RSA) et la clé publique elle-même, représentée sous forme d'une suite d'octets utilisée pour les calculs RSA, notamment lors de la vérification des signatures électroniques ;
- Des éléments permettant de vérifier la validité du certificat, tels que les dates de début et de fin de validité, ainsi que le point de distribution de la liste des certificats révoqués (CRLDP) utilisé dans le processus de vérification. De plus, des identificateurs de clés du sujet (SKI), représentant un hash de la clé publique du titulaire, et de l'émetteur (AKI) sont inclus pour reconstruire la chaîne de confiance. [7]

2.10.4. Services de confiance

La réglementation et les lois juridiques concernant l'archivage électronique englobent également d'autres services de confiance, notamment le cachet électronique, l'horodatage, le service d'envoi recommandé électronique, l'authentification de sites web, ainsi que l'archivage électronique.

Un service de confiance est un service électronique généralement fourni moyennant rémunération, qui comprend :

- La création, la vérification et la validation des signatures électroniques, des cachets électroniques, ou des horodatages électroniques, ainsi que des certificats associés à ces services ;
- La création, la vérification et la validation de tous les certificats pour l'authentification de sites web ;
- La conservation des signatures électroniques, des cachets électroniques, ou des certificats liés à ces services. [3]

2.11. L’enjeu de l’Archivage électronique et le coffre-fort

- L'archivage électronique est apparu dès la création des documents, offrant ainsi à l'organisation productrice la possibilité de les exploiter tout au long de leur cycle de vie ;
- Principalement ancré dans le domaine de la gouvernance des systèmes d’information, l'archivage électronique implique :
- La gestion électronique de documents pour la classification, l'indexation, la recherche multicritères, sémantique, plein-texte ;
- La garantie de la sécurité des systèmes, l'interopérabilité, la production de preuves, la journalisation, la surveillance des réglementations en vigueur ;
- Le stockage sur des infrastructures matérielles et logicielles ;
- L'utilisation d'outils de conservation à long terme du contenu numérique et la veille technologique ;
- L'archivage des contenus électroniques désigne l'ensemble des actions, outils et méthodes déployés pour collecter, identifier, sélectionner, classer, détruire et conserver des contenus électroniques sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps ;
- Les contenus archivés sont considérés comme immuables et ne peuvent donc être modifiés. Ceci est notamment rendu possible en garantissant l'authenticité par le biais de l’empreinte électronique, la signature électronique, la traçabilité des accès et divers autres moyens ; [9]

---

[9] : La différence entre le coffre-fort numérique et E-archivage, URL : https://www.oodrive.fr/blog/securite/difference-entre-coffre-fort-electronique-et-archivage-numerique/ consulté le 29/03/2024

- La durée de conservation des archives est déterminée en fonction de la valeur du contenu, généralement sur le moyen ou long terme. Pour garantir cette conservation, l'archivage numérique se conforme à la norme NF Z42-013 établie par l'AFNOR ; [10]
- Le concept de coffre-fort électronique a été normalisé par l'AFNOR dans la norme NF Z42-020, offrant ainsi un espace sécurisé pour l'archivage électronique ;
- Le coffre-fort électronique offre un ensemble de fonctionnalités indispensables à un stockage sécurisé, dépassant les capacités de l'archivage classique. Intégré à l'archivage, il permet la conservation des documents ainsi que des métadonnées associées, facilitant ainsi les recherches documentaires ;
- Les coffres-forts électroniques assurent l'intégrité des documents grâce à des empreintes numériques apposées lors du dépôt, garantissent la pérennité des documents par le biais de contrôles périodiques et de la duplication du stockage, préservent la confidentialité des échanges grâce au cryptage et aux mécanismes de contrôle d'accès, et enfin assurent la traçabilité en enregistrant toutes les interactions des utilisateurs avec les documents.[10]

2.12. L’usage du parapheur électronique

Le parapheur électronique est un logiciel collaboratif permettant d'intégrer des documents au sein d'une chaîne de validation entièrement dématérialisée. Ces documents sont intégrés dans des circuits sécurisés, limitant ainsi l'accès aux contenus uniquement aux personnes autorisées. L'utilisation d'un parapheur électronique garantit une meilleure confidentialité et sécurité des documents internes.

Une fois le document dématérialisé et validé, il peut être signé électroniquement, ce qui lui confère une valeur probante. Cette signature électronique authentifie le signataire et atteste que le document a été approuvé par une personne identifiée. [11]

---

[10] : L’Association française de normalisation est l'organisation française qui représente la France auprès de l'Organisation internationale de normalisation (ISO).

[11] : Le parapheur électronique ; URL : https://www.neoledge.com/fr/parapheur-electronique-rival-parapheur-papier/?fbclid=IwAR1U7uHf1Eez16_BwLmMWhmm20RYtlB_exSKufVcrzyQCyyAzrv1CiBQcy4 , consulté le 01/04/2024

Quelques autres avantages du parapheur électronique sont les suivants :

- Gestion automatique de la soumission des documents au signataire et du retour du document signé dans la chaîne métier de validation ;
- Centralisation des documents à signer, permettant au signataire d'accéder à tous les documents à signer depuis un seul endroit ;
- Possibilité d'inclure préalablement des étapes de validation et de corrections avant la signature ;
- Gestion des délégations de signature en cas d'absence du signataire lorsqu'il est hors du lieu de travail.

Conclusion

Dans ce premier chapitre, nous avons introduit les notions de base concernant la signature électronique, en rappelant ses principes fondamentaux. Nous avons souligné son rôle en tant qu'outil innovant qui, dans des organisations telles que les caisses de protection sociale, modernise l'expérience utilisateur tout en éliminant les méthodes de travail traditionnelles, notamment la signature manuscrite des documents, ce qui permet de gagner du temps. Nous avons également examiné les fondements techniques, les caractéristiques et les avantages de la signature électronique dans ce contexte organisationnel.

Bien entendu, nous avons également abordé des notions relatives à la dématérialisation, qui est logiquement introduite, car elle représente un élément essentiel pour la concrétisation du projet de mise en œuvre du système de signature électronique. L'objectif de cette étude est donc de présenter en détail les différentes étapes nécessaires pour réaliser ce projet, ce que nous explorerons dans les chapitres suivants.

Chapitre 02 : Étude de l’existant et analyse des besoins

Introduction

Dans ce chapitre, nous allons aborder la conception du système de signature électronique des factures d'une application de gestions des réservations d'hôtels afin d'avoir une vision détaillée des différentes interactions de l'application avec leur table de description textuelle pour pouvoir l'implémenter par la suite dans le chapitre suivant. Cette conception représente le fonctionnement du projet.

1. Conception du système de signature électronique

La conception est une étape cruciale dans le développement d'un projet informatique. Il repose sur la création de différents diagrammes UML qui décrivent toutes les fonctions et interactions utilisateur du système prévu.

1. Diagramme de cas d'utilisation

1.1. Identification des acteurs

Le seul acteur qui interagit avec le système est un administrateur muni d'une clé privée et d'une clé publique qui différencie un technicien d'un autre

1.2. Identification des cas d'utilisation et les fonctionnalités du système

La signature électronique est un procédé technologique permettant de garantir l'intégrité d'un document électronique, il n'est pas facile de conceptualiser une signature électronique, car elle est une suite de caractères qui s'appuie sur une technique de chiffrement ayant pour but de garantir la confidentialité des données, donc le système de signature électronique doit avoir les fonctionnalités suivantes :

- S'authentifier ;
- Générer une facture signer électroniquement ;
- Vérifier la signature électroniquement de la facture générée.

1.3. Les différents diagrammes de cas d'utilisation

1.3.1. Le diagramme global du système de signature électronique d'une facture

Dans la figure -11- ci-dessous, nous avons illustré le diagramme de cas d'utilisation global du système de signature électronique

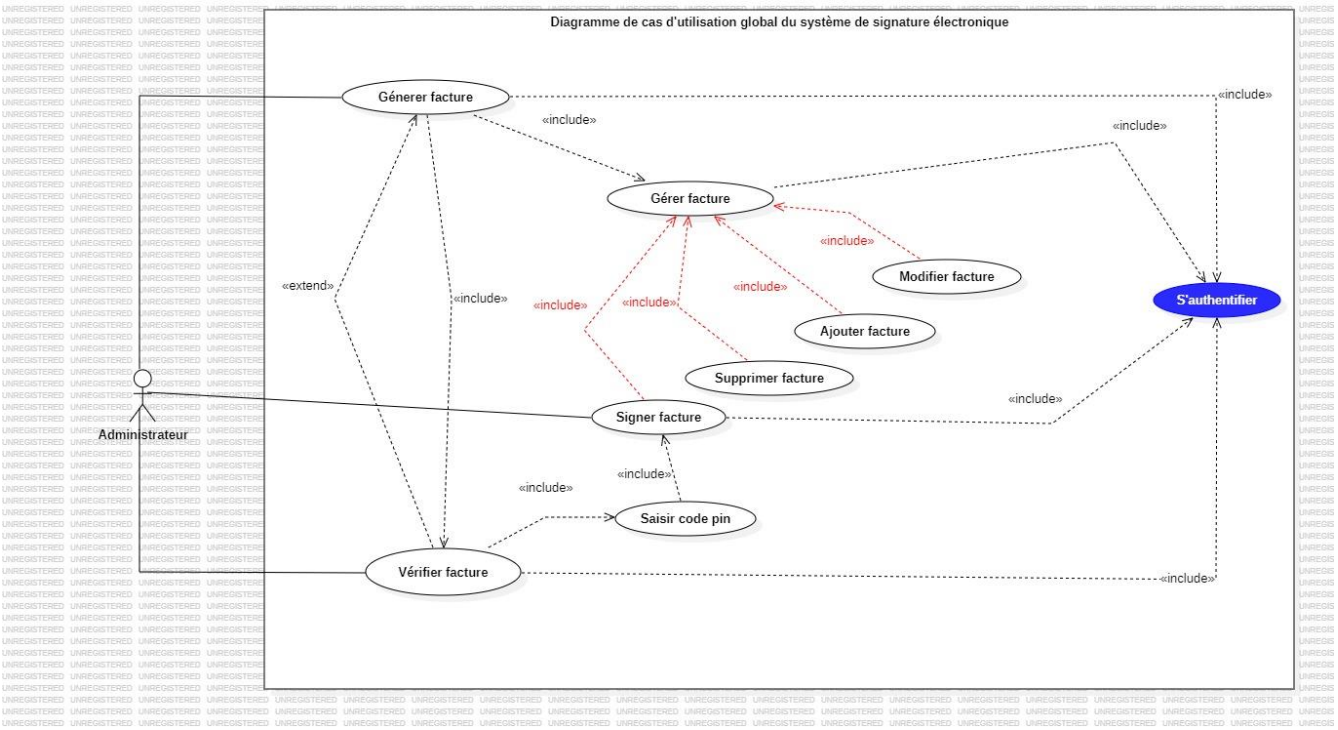

Figure -11- Diagramme cas d'utilisation global de la signature électronique d'une facture

Source : réalisé par l'étudiant avec StarUML

1.3.2. Créer une signature électronique sur une facture

 La description textuelle du diagramme de cas d'utilisation dans le tableau ci-dessous :

Sommaire d'identification du cas d'utilisation « création d'une signature électronique sur une facture »	
Titre	Créer une signature d'un document électroniquement
Résumé	L'administrateur signe un document grâce à son certificat électronique
Acteur	Administrateur

Date de création	25/06/2024
Version	1.0
Réalisateur	Chemseddine AMICHE
Description des scenarios	
Précondition	• L'administrateur Authentifié ; • Disposé d'un certificat électronique légal contenant une clé privée et publique.

Scénario Nominal	1. L'administrateur demande de signer une facture ; 2. Le système affiche le formulaire de signature électronique ; 3. L'administrateur choisi le document pour visualisation des données ; 4. Générer la facture ; 5. Saisir un code pin pour procéder à la signature de la facture ; 6. Enregistrer la signature électronique effectué sur la facture ; **Point d'extension (processus de signature) :** • Le système demande le code pin ; • L'administrateur saisit le code pin ; • Le système vérifie la validité du code pin sur le serveur et demande la clé privée ; • Le système vérifie la validité de la clé privée ; • Le système qui dispose d'un algorithme mathématique extrait les données du document électronique en créant des données correspondant au document à signé et génère le HASH : • Le système crypte le HASH par la clé privé. 6. Le système enveloppe la signature avec le document signé ;

	7. Le système génère la facture cryptée et signée selon un format électronique ;
Scénario alternatif	A1 : Si clé privée n'est pas vérifié, le HASH ne sera pas généré ; A2 : Si le code pin n'est pas validé, la signature ne sera pas générée. • L'enchainement A1 démarre au point 4 de l'extension ; • L'enchainement A1 démarre au point 1 de l'extension.
Post condition	Une facture est signée électroniquement selon un (code pin) certificat qualifié.

Tableau N°3 : Création d'une signature électronique pour une facture

Source : réalisé par l'étudiant

Dans la figure -12- ci-dessous, nous avons illustré le diagramme de cas d'utilisation du processus de création d'une signature électronique d'une facture :

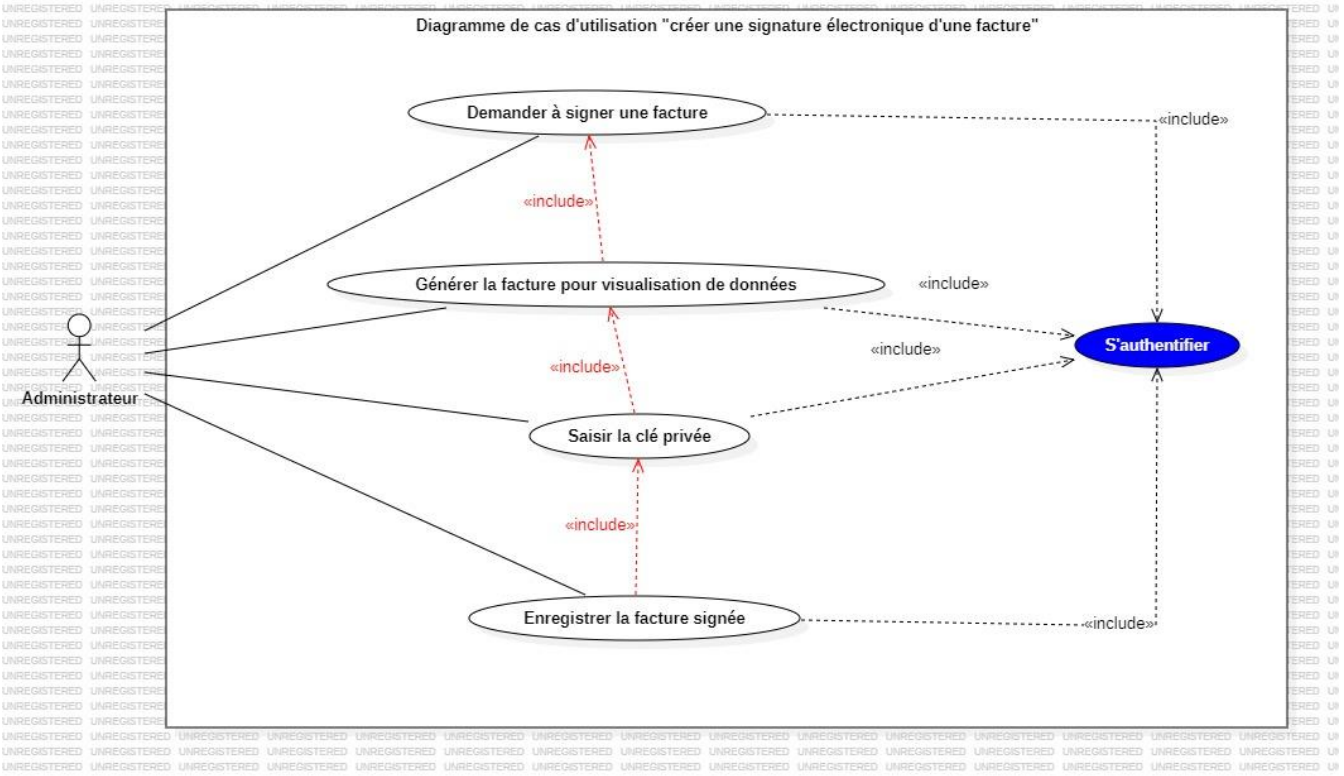

Figure -12- Diagramme de cas d'utilisation du processus de création d'une signature électronique d'une facture

Source : réalisé par l'étudiant avec StarUML

1.3.3. Vérifier une facture

- La description textuelle du diagramme de cas d'utilisation dans le tableau ci-dessous :

Sommaire d'identification du cas d'utilisation « Vérifier signature d'un document »	
Titre	Vérifier une facture
Résumé	L'administrateur vérifie une facture grâce à son certificat électronique délivré par l'autorité
Acteur	Administrateur

Date de création	25/06/2024
Version	1.0
Réalisateur	Chemseddine AMICHE
Description des scenarios	
Précondition	• L'administrateur Authentifié ; • Disposé d'un certificat électronique légal de l'autorité contenant une clé privée et publique ;
Scénario Nominal	1. L'administrateur demande de vérifier la signature d'une facture ; 2. Le système affiche le formulaire de vérification immédiate de la signature électronique ; 3. L'administrateur importe la facture à vérifier et les données originales ; 4. Demandé de saisir la clé publique ; 5. L'administrateur saisie la clé publique ; 6. Le système génère le HASH du document, décrypte la signature avec la clé publique du signataire et augmente la signature du document ;

	7. Le système compare entre les deux HASH ; 8. Le système génère le document original avec la signature valide selon un format électronique ; 9. Enregistrer la facture et l'imprimer.
Scénario alternatif	A1 : Si le document n'est pas disponible, il n'y aura pas de signature ; A2 : Si le certificat électronique et la clé publique ne sont pas vérifiés, la signature ne sera pas décryptée et les deux HASH ne seront pas comparés. • L'enchainement A1 démarre au point 2 du point d'extension ; • L'enchainement A2 démarre au point 6.
Post condition	Document original généré avec la signature valide selon un format électronique.

Tableau N°4 : Vérification de la signature électronique d'une facture

Source : réalisé par l'étudiant

Dans la figure -13- ci-dessous, nous avons illustré le diagramme de cas d'utilisation du processus de vérification d'une signature électronique d'une facture

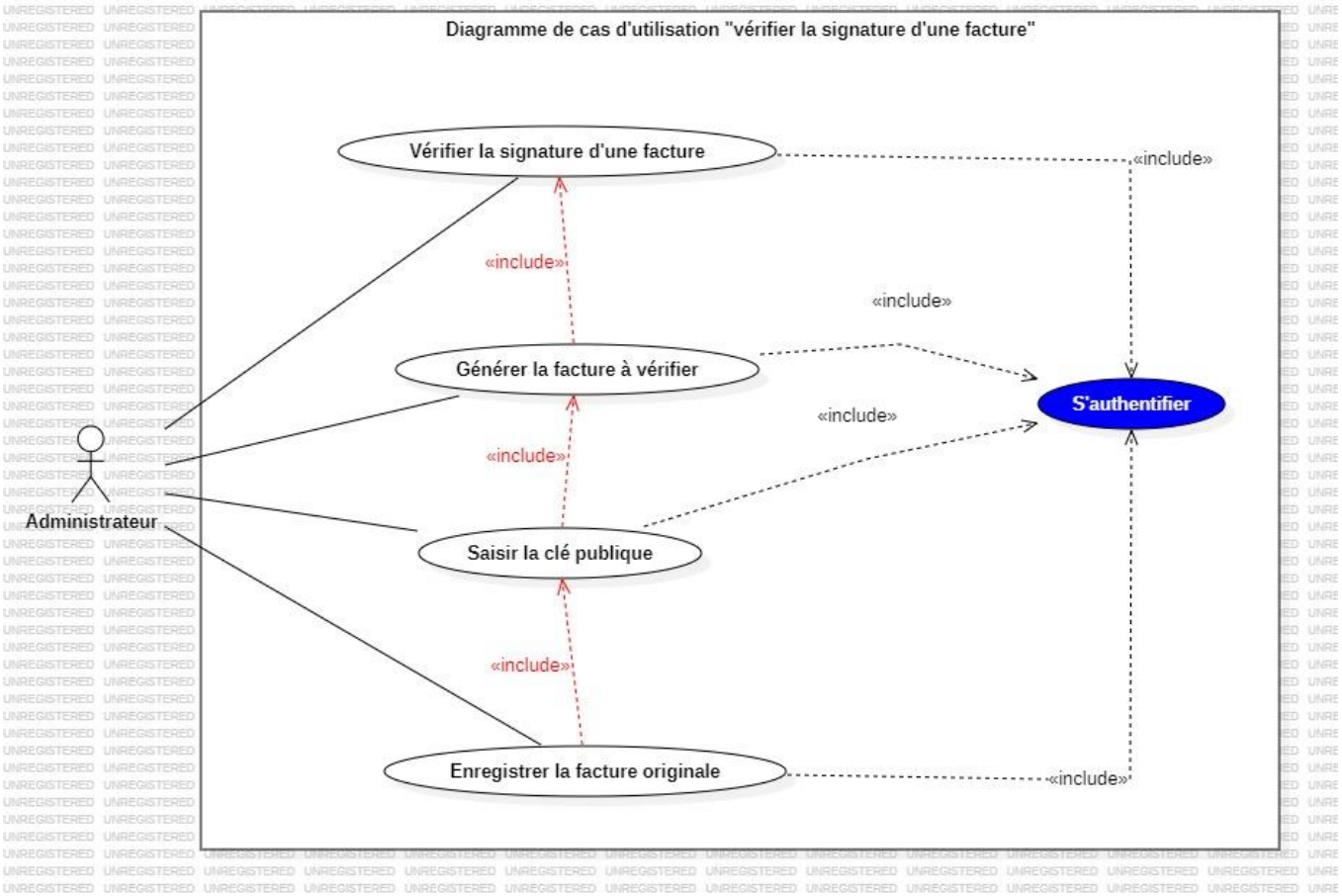

Figure -13- Diagramme de cas d'utilisation du processus de vérification d'une signature électronique d'une facture

Source : réalisé par l'étudiant avec StarUML

1.3.4. Authentification au système

- La description textuelle du diagramme de cas d'utilisation dans le tableau N°13 ci-dessous :

Sommaire d'identification du cas d'utilisation **« S'authentifier »**	
Titre	Authentification au système
Résumé	L'administrateur s'authentifie pour pouvoir accéder à des fonctionnalités qui lui ont été réservé.

Acteur	Administrateur
Date de création	25/06/2024
Version	1.0
Réalisateur	Chemseddine AMICHE
Description des scenarios	
Précondition	• Système accessible ; • Avoir les droits d'accès.
Scénario Nominal	1. L'administrateur accède à s'authentifier ;
	2. Le système affiche le formulaire d'authentification ; 3. L'administrateur saisit son login et son mot de passe dans le formulaire d'authentification ; 4. Le système vérifie l'existence du compte de l'administrateur et la validité des données entrantes ; 5. L'administrateur accède au système.
Scénario alternatif	A1 : Erreur d'authentification : erreur durant la saisie du mot de passe ou du nom d'utilisateur incorrecte ou problème de connexion. A2 : Formulaire invalide : champs de saisie vide, connexion impossible puis le système redonne la main à l'administrateur ; L'enchainement A1 démarre au point 3 ; L'enchainement A2 démarre au point3.
Post condition	L'administrateur authentifié, accède au système.

Tableau N°5 : Authentification au système

Source : réalisé par l'étudiant

2. Diagramme de séquence

2.1. Diagramme de séquence « S'authentifier au système »

Dans la figure -14- ci-dessous, nous avons illustré le diagramme de séquence du processus d'authentification au système

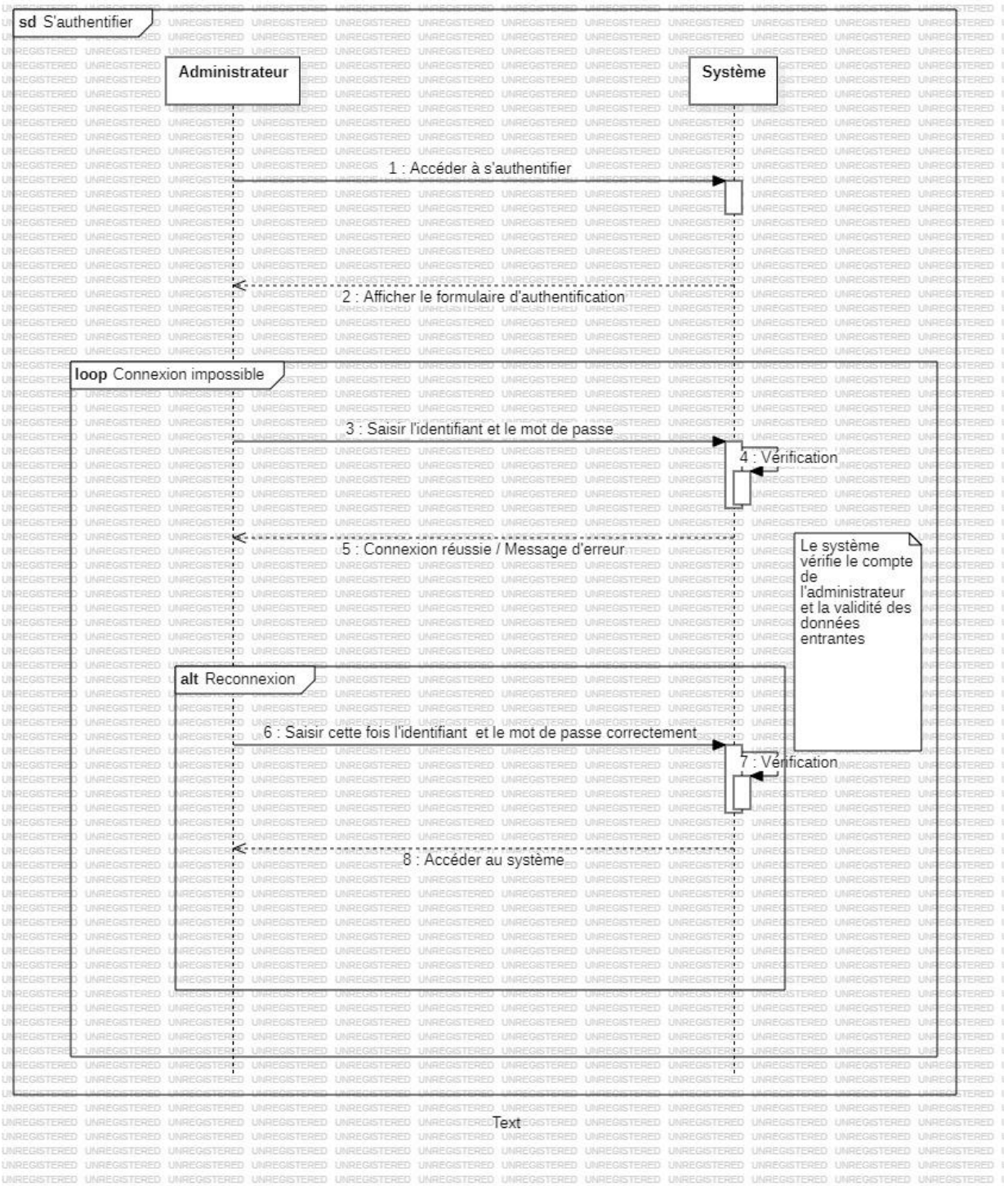

Figure -14- Diagramme de séquence du processus d'authentification au système

Source : réalisé par l'étudiant à partir de STARUML

2.2. Diagramme de séquence « création d'une signature électronique d'une facture »

Dans la figure -15- ci-dessous, nous avons illustré le diagramme de séquence du processus de création d'une signature électronique d'une facture

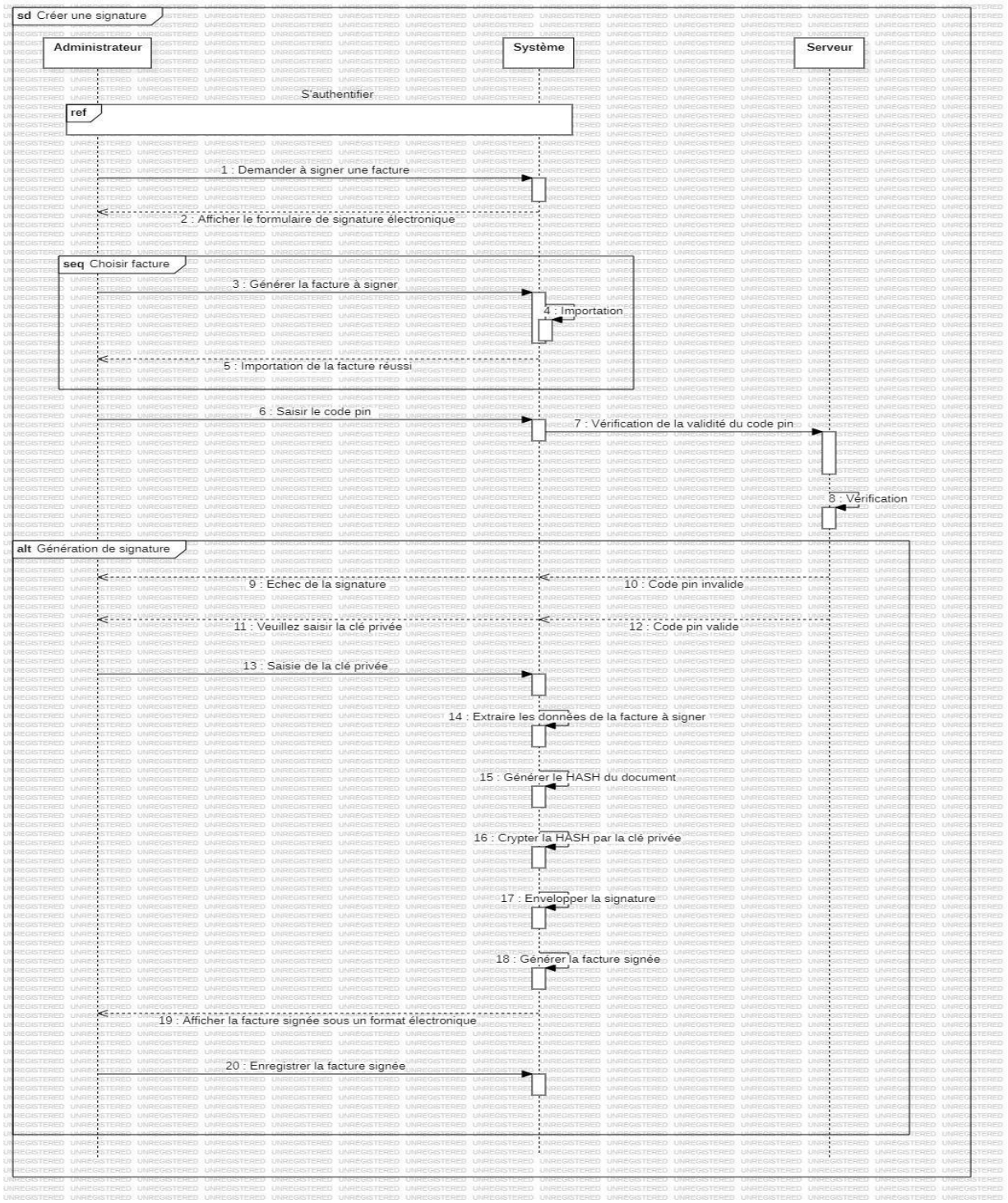

Figure -15- Diagramme de séquence du processus de création d'une signature électronique d'une facture

Source : réalisé par l'étudiant à partir de STARUML

2.3. Diagramme de séquence « vérification de la signature électronique d'une facture »

Dans la figure -16- ci-dessous, nous avons illustré le diagramme de séquence du processus de vérification d'une signature électronique d'une facture

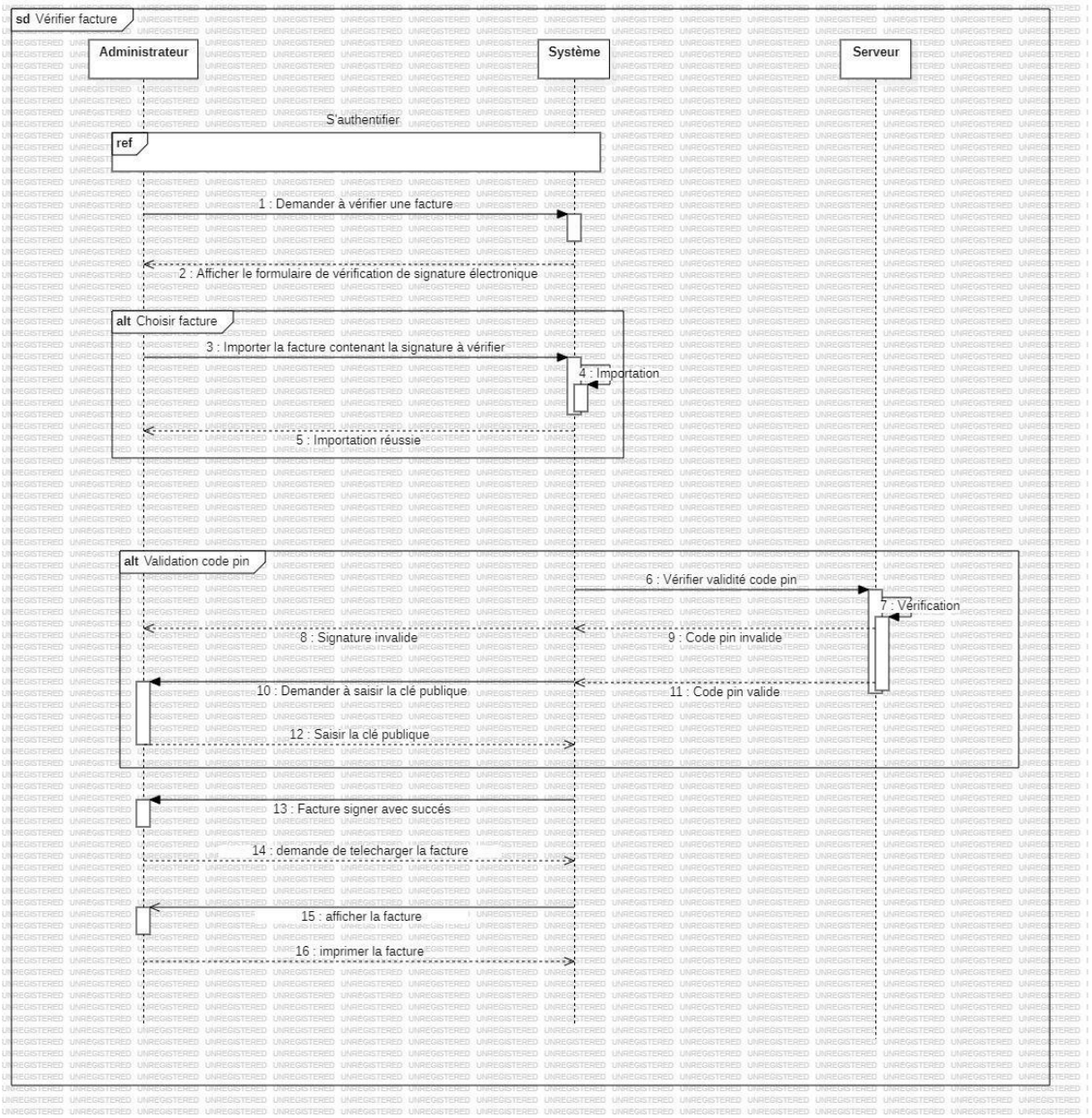

Figure -16- Diagramme de séquence du processus de vérification d'une signature électronique d'une facture

Source : réalisé par l'étudiant à partir de STARUML

3. Diagramme de classe

Pour faire l'étude du module e-signature, nous avons adopté le développement de notre application gestion des réservations d'Hotels pour pouvoir gérer le taux énorme de factures afin d'économiser le temps, optimisé la qualité du travail et réduire les coups de réalisation. Le diagramme de classe ci-dessous explique les différentes entités de l'application global.

Dans la figure -17- ci-dessous, nous avons illustré le diagramme de classe du système global :

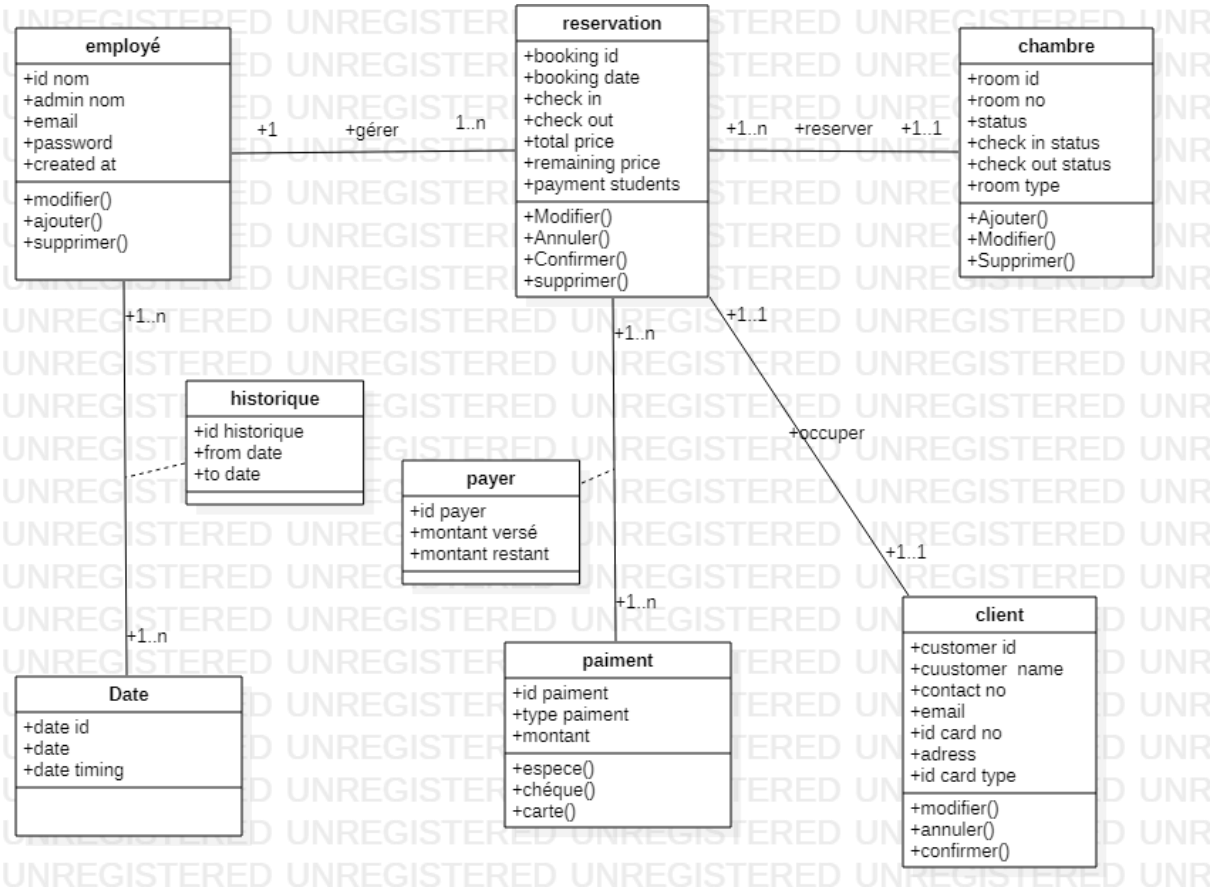

Figure -17- Diagramme de classe du système de signature électronique

Source : réalisé par l'étudiant à partir de STARUML

4. Modèle relationnel

reservation (reservation_id, client_id*, room_id*, shift_id, booking_date, check_in, check_out, total_Price, remaining_price, payment_student);
client (client_id, customer_name, contact_no, email,
id_card_type_id*, id_card_no, adress);
chambre (room_id, room_no, status, check_in_status, check_out_status, delete status, room_type);
date (shift_id, shift, shift_timing);
employé (id,name,username, employé, employé type, email, password, created at);
paiment (id payment, type paiment, montant);
historique (id_historique, from date, to date);
Payer (id_payé, id_reservation*, id_paiment*, montant verse, montant restant);

Conclusion

Dans ce chapitre, nous avons illustré la conception du système de signature électronique, en utilisant la représentation graphique d'UML ; en effet, ces différents diagrammes nous ont aidé à mieux comprendre le fonctionnement de ce système et ont facilité la réalisation finale de l'application. Par la suite, au prochain chapitre nous présenterons l'étape de réalisation et d'implémentation du système E-signature, nous expliquerons les outils de développement qui doivent être utilisés respectant ainsi la conception élaborée dès le début.

Chapitre 03 : Implémentation & réalisation

Réalisation du système

Introduction

Dans le cadre du développement des applications selon la conception mis en œuvre dans le chapitre précèdent, nous allons procéder à la réalisation de notre système de signature électronique en prenant exemple une plateforme de gestion des réservations d'hôtels, nous allons intégrer un module spécialisé a crypté une signature électronique sur une facture électronique puis la vérifiée sur le même module.

1. Outils de développement

1.1. Visual Studio Code

Visual Studio Code (VS Code) est un éditeur de code source et un environnement de développement intégré (IDE) de Microsoft. Il est open-source et cross-platform, c'est-à-dire qu'il fonctionne sur Windows, Linux et Mac. Il a été conçu pour les développeurs web, mais il prend en charge de nombreux autres langages de programmation tels que C++, C#, Python, Java, etc. Il offre de nombreuses fonctionnalités comme la coloration syntaxique, l'auto-complétions, la mise en évidence des erreurs, la navigation de code, le débogage, la gestion de versions, l'intégration avec Git, et beaucoup d'autres. Il est également extensible à l'aide d'une grande variété d'extensions développées par la communauté, permettant aux développeurs de personnaliser l'éditeur selon leurs besoins.

1.2. WAMP SERVER

XAMPP est un ensemble de logiciels libres. Le nom est un acronyme venant des initiales de tous les composants de cette suite. Ce dernier réunit donc le serveur Web Apache, la base de données relationnelle et système d'exploitation MySQL ou MariaDB ainsi que les langages scripts Perl et PHP. L'initiale X représente tous les systèmes d'exploitation possibles, à savoir Linux, Windows et Mac OS X.

- Apache : le serveur Web open source Apache est utilisé mondialement et permet de délivrer des contenus Web. L'application de serveur est mise à disposition en open source par l'Apache Software Foundation.
- MySQL/MariaDB : avec MySQL, XAMPP se compose de l'un des systèmes de gestion de base de données relationnelle les plus populaires au monde. En combinaison avec le

serveur Web Apache et le langage script PHP, MySQL sert à l'enregistrement de données pour des services Web. Les versions actuelles de XAMPP favorisaient MariaDB à l'insu de MySQL comme gestionnaire de base de données, marquant un détachement avec ce dernier.

- PHP : Il s'agit d'un langage script côté serveur permettant de créer des pages Web ou applications dynamiques. PHP peut être mis en place sur toutes les plateformes possibles et est compatible avec divers systèmes de base de données.
- Perl : le langage script Perl est utilisé pour l'administration système, le développement Web et la programmation en réseau. De plus, des applications Web dynamiques peuvent être programmées de la même manière que PHP.

1.3. PHP (Personnal Home Pages)

Le PHP, pour Hypertext Preprocessor, désigne un langage informatique, ou un langage de script, utilisé principalement pour la conception de sites web dynamiques. Il s'agit d'un langage de programmation sous licence libre qui peut donc être utilisé par n'importe qui de façon totalement gratuite. Créé au début des années 1990 par le Canadien et Groenlandais Rasmus Lerdorf, le langage PHP est souvent associé au serveur de base de données MySQL et au serveur Apache. Avec le système d'exploitation Linux, il fait partie intégrante de la suite de logiciels libres LAMP.

Visual Studio Code définition ; URL : https://bility.fr/definition-visual-studio-code/

XAMPP définition ; URL : https://www.ionos.fr/digitalguide/serveur/outils/tutoriel-xampp-creer-un-serveur-de-test-local/

PHP définition ; URL : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203597-php-hypertext-preprocessor-definition/

1.4. StarUML

Le logiciel StarUML est un logiciel open-source cédé par son ancien éditeur sous licence GNU GPL, dédié aux plateformes Windows, il est développé en Delphi.

Ses principaux avantages sont sa implicité d'installation et de prise en main, et la possibilité de générer le squelette des classes en langages Java, C++, C#, ActionScript3.0... De plus, le logiciel à été conçu en prévoyant l'ajout de plugin supplémentaires afin de pouvoir être adapté simplement aux besoins évolutifs de ses utilisateurs. Enfin StarUML gère l'exportation des données au format XMI, le standard pour l'échange d'informations de métadonnées UML basé sur XML, ainsi que l'exportation au format jpg afin d'intégrer les diagrammes au sein de documents.

1.5. JavaScript

JavaScript désigne un langage de développement informatique, et plus précisément un langage de script orienté objet. On le retrouve principalement dans les pages Internet. Il permet, entre autres, d'introduire sur une page web ou HTML des petites animations ou des effets.

Créé en 1995 par Brendan Eich, en même temps que la technologie Java, le langage JavaScript se distingue des langages serveurs par le fait que l'exécution des tâches est opérée par le navigateur lui-même, sur l'ordinateur de l'utilisateur, et non sur le serveur web. Il s'active donc généralement sur le poste client plutôt que côté serveur.

1.6. HTML (HyperText Markup Language)

HTML (HyperText Markup Language) est un langage de description (dit de marquage) de pages Web. Il permet de présenter les documents hypertextes destinés à être affichés sur le navigateur. Il s'agit d'un langage coté client (tout comme CSS et Javascript). Il est supporté et développé par W3C. L'origine du HTML remonte au début du Web. En effet, il a été inventé vers les années 1989 afin qu'il puisse présenter les documents qui circulent sur la toile et établir des liens entre eux à travers les liens hypertextes (ou hyperliens).

StarUML définition ; URL : https://air.imag.fr/index.php/StarUML

JavaScript définition ; URL : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203585-javascript/

HTML définition ; URL : https://www.chiny.me/html-c-est-quoi-3-1.php

1.7. CSS (Cascading Style Sheets)

Cascading Style Sheets (CSS) est un langage de programmation qui vous permet de déterminer le design des documents électroniques. À l'aide de simples instructions, présentées dans des codes sources clairs, les éléments de la page Web comme la mise en page, la couleur et la police peuvent ainsi être modulés à souhait. Grâce aux feuilles de style en cascade, la structure sémantique et le contenu du document restent totalement intacts. CSS a été lancé au milieu des années 90 et est à présent considéré comme le langage de feuilles de style standard sur le World Wide Web.

1.8. Bootstrap

Bootstrap est un framework développé par l'équipe du réseau social Twitter. Proposé en open source (sous licence MIT), ce framework utilisant les langages HTML, CSS et JavaScript fournit aux développeurs des outils pour créer un site facilement. Ce framework est pensé pour développer des sites avec un design responsive, qui s'adapte à tout type d'écran, et en priorité pour les smartphones. Il fournit des outils avec des styles déjà en place pour des typographies, des boutons, des interfaces de navigation et bien d'autres encore. On appelle ce type de framework un "Front-End Framework".

Bootstrap définition ; URL : https://www.journaldunet.com/developpeur/1159810-bootstrap-definition-tutoriels-astuces-pratiques/

CSS définition ; URL : https://www.ionos.fr/digitalguide/sites-internet/web-design/quest-ce-que-le-css/

2. Mise en œuvre du système E-signature

Pour la mise en œuvre de ce module, pour illustré le principe de signature électronique nous avons choisi de développer un site de gestion des réservations d'un hôtel qui consiste a effectué de différentes fonctionnalités tel que la réservation et la gestion de la clientèles pour générer une facture électronique (crée, modifier, supprimer une facture) qui sera signer électroniquement grâce à la fonctionnalité du module e-signature, cette dernière doit être vérifier pour pouvoir délivrée la facture finale.

2.1. L'authentification

L'authentification est obligatoire par l'administrateur qui est tout d'abord une entité légale a effectué une e-signature (juridiquement chaque signataire dispose d'une clé privée et publique selon un certificat électronique délivré par la loi), l'admin s'authentifie comme suit avec un nom d'utilisateur et un mot de passe correcte comme la figure ci-dessous :

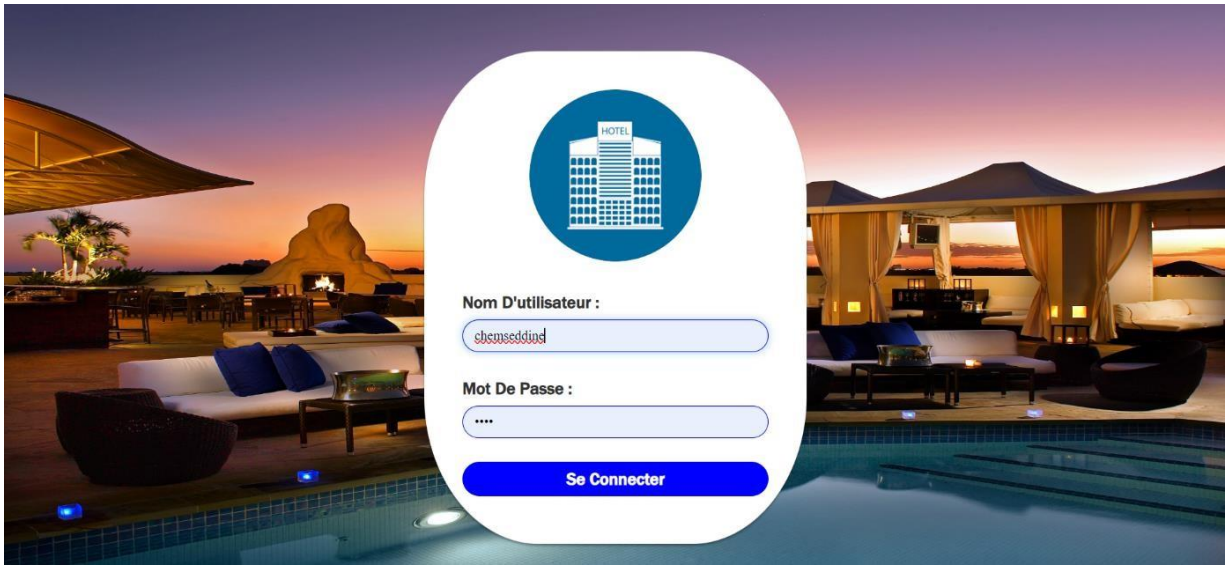

Figure -18- La page d'authentification de l'administrateur

Le nom d'utilisateur et le mot de passe doivent être saisi correctement sinon un message d'erreur s'affichera comme la figure ci-dessous :

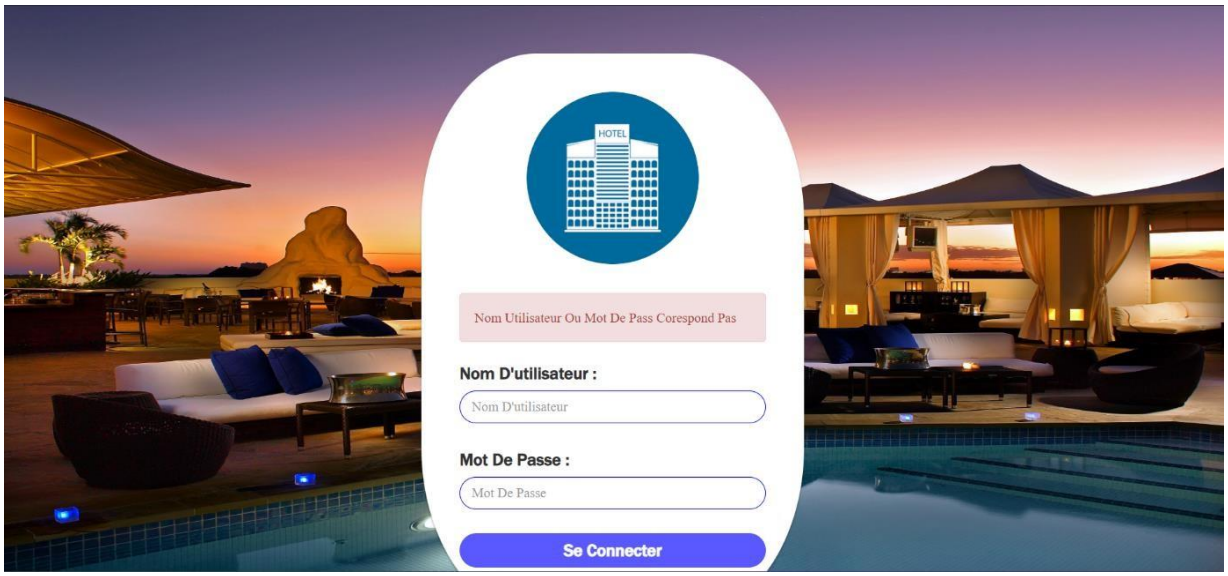

Figure -19- Erreur d'authentification, mot de passe ou nom d'utilisateur incorrect

2.2. Réservation et confirmation

L'admin saisi les informations de la chambre demandé par le client avec les tarifs en détails selon le formulaire de réservation comme la figure ci-dessous :

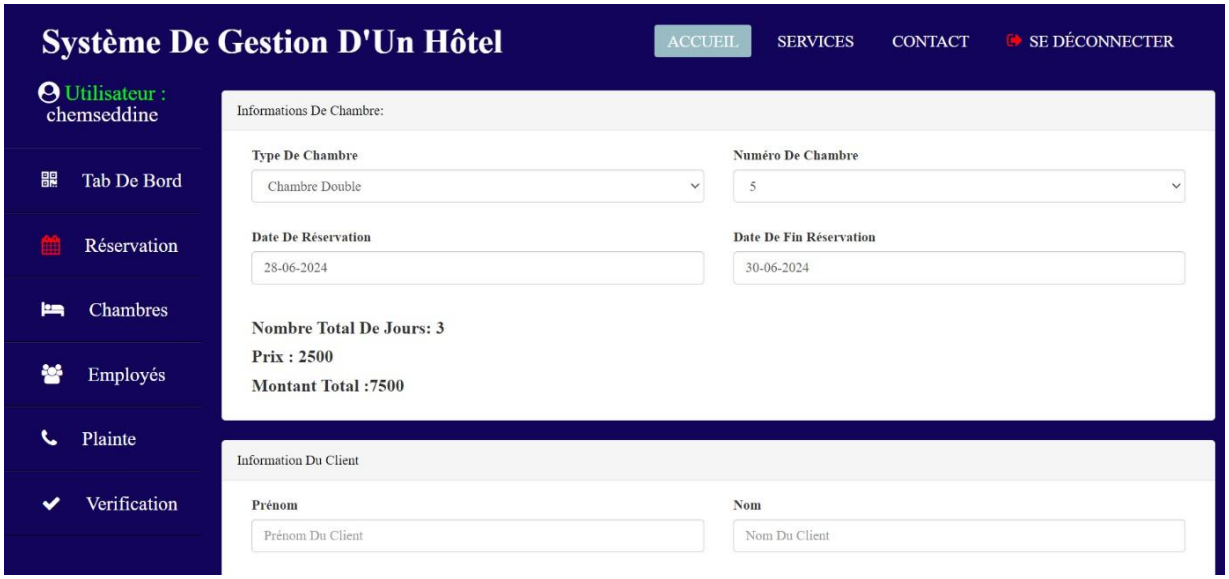

Figure -20- Représente les informations de la chambre saisies lors de la réservation

L’admin saisi les informations du client comme la figure ci-dessous :

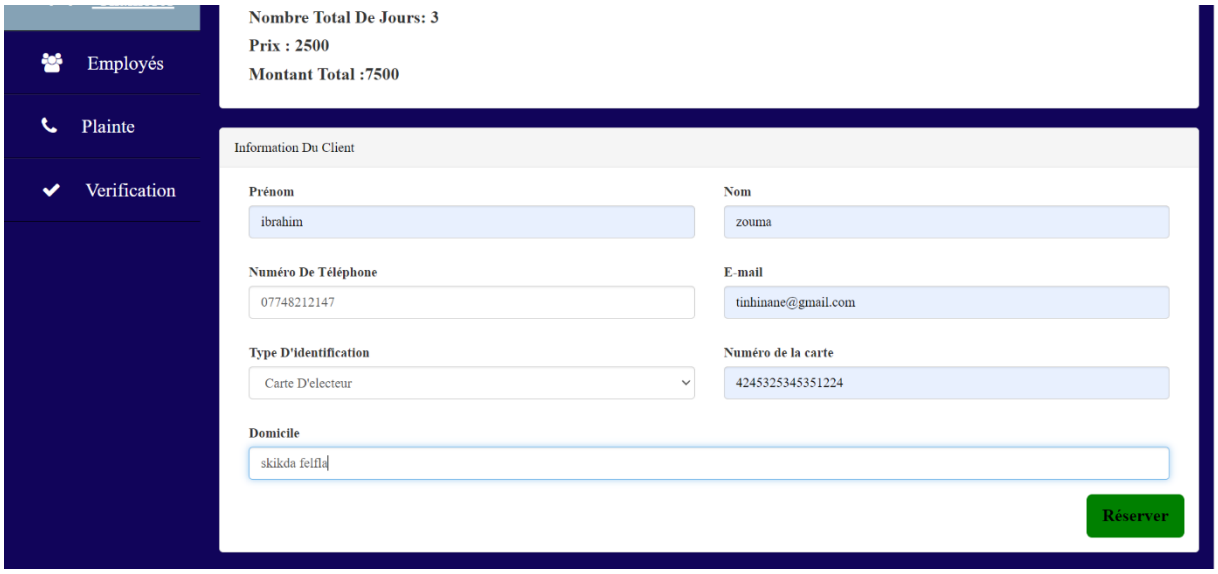

Figure -21- Représente les informations du client saisies lors de la réservation

L’admin confirme et valide la réservation comme la figure ci-dessous :

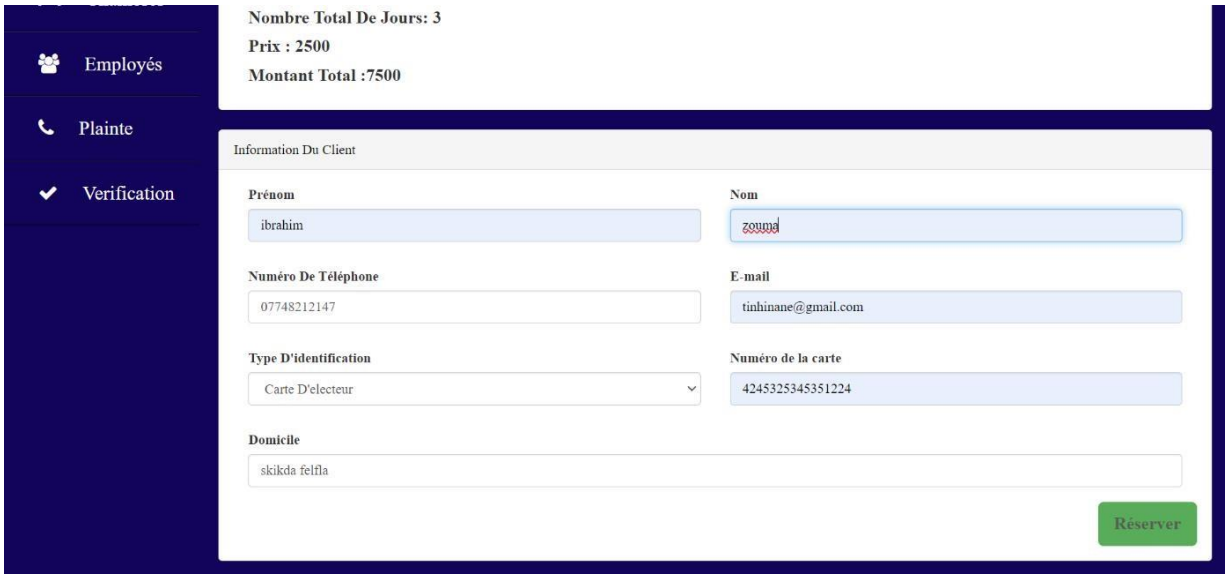

Figure -22- Confirmation des informations saisies

Une fois la réservation effectué un message comme suit sera afficher et la réservation est confirmé en générant une facture électronique prête à être téléchargé selon la figure ci-dessous :

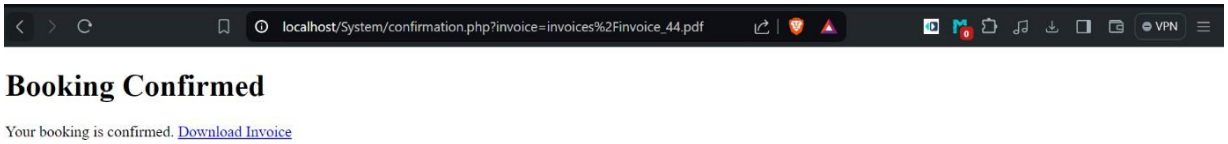

Figure -23- Message de confirmation de la réservation

2.3. Facture signée (cryptée) électroniquement

Une fois la réservation effectué, l'admin peut consulter la facture générer, cette dernière qui est cryptée avec une e-signature unique et une clé privée unique selon la figure ci-dessous :

Figure -24- Les factures sont signées électroniquement

2.4. Vérification (décryptage) de la facture signée électroniquement

La facture générée, elle doit être décryptée avec une clé publique pour être vérifier comme la figure ci-dessous :

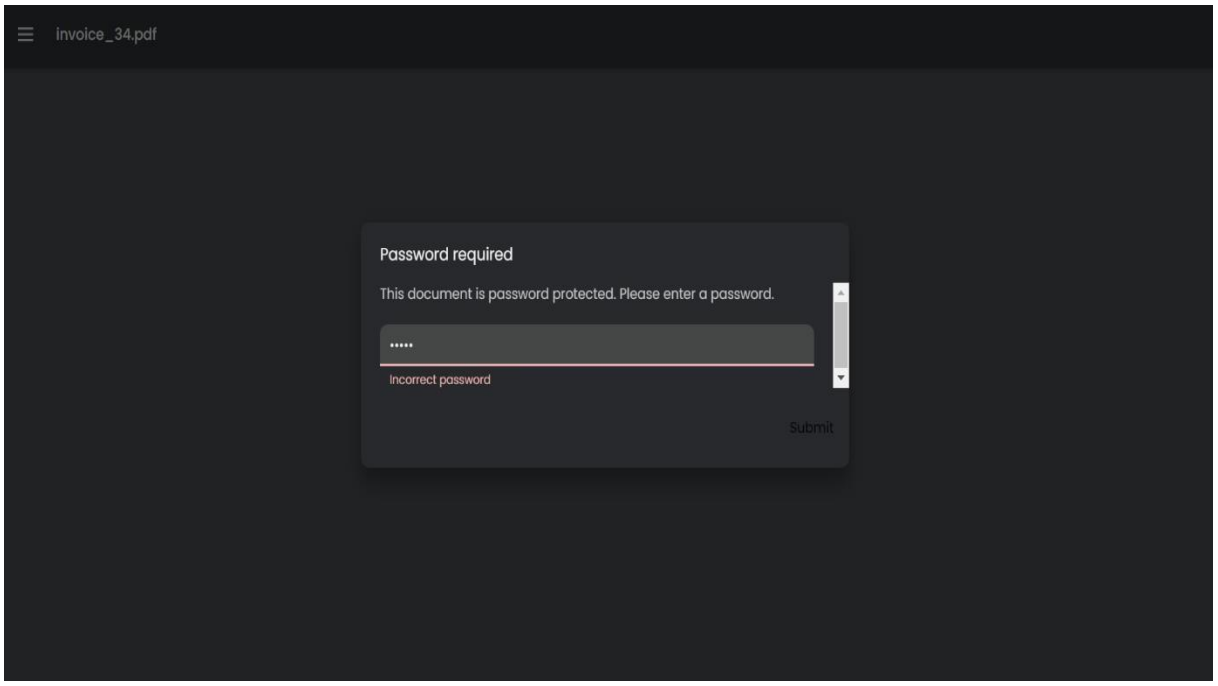

Figure -25- Saisi d'une clé publique valide pour la vérification

Une fois la facture vérifiée électroniquement, elle est prête à être délivrée comme s'affiche dans la figure ci-dessous :

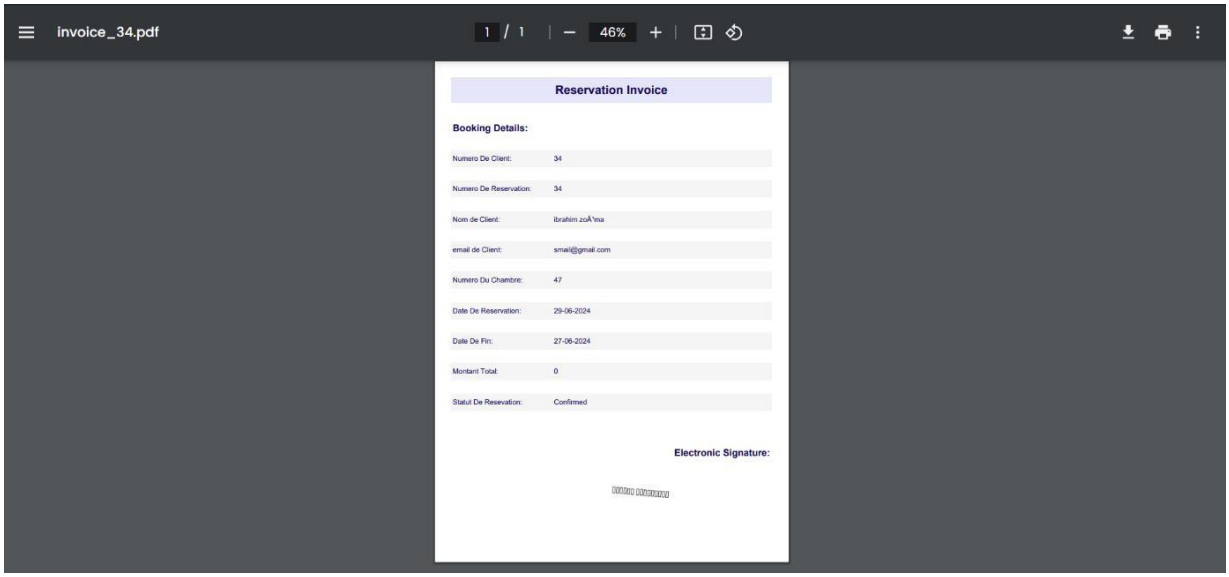

Figure -26- Vérification de la facture signée électroniquement réussi

Conclusion

Dans ce chapitre, après avoir illustré la conception du système, à l'aide de la représentation graphique d'UML dans le chapitre précèdent ; en effet, ces différents diagrammes ont facilité à mieux comprendre le fonctionnement du système et la réalisation finale du module sur l'application gestion des réservations d'hôtels. Par la suite, nous avons présenté l'étape d'implémentation du système E-signature, nous avons expliqué les outils de développement qui doivent être utilisés puis nous avons développé un module d'E-signature sur une applications de gestions des réservations d'hôtels afin de signer électroniquement et vérifier les factures énormes générées.

Conclusion générale

Durant la réalisation de ce mémoire, nous avons présenté la thématique et la solution proposée dans le cadre d'un projet de fin d'étude qui consiste à concevoir un système de signature électronique des documents. La transformation numérique est un bouleversement induit par la technologie, c'est un processus qui permet aux organisations et entreprises d'intégré cette dernière au milieu de leurs activités, ce qui est le cas pour les administrations développées, dorénavant, elles optent pour l'administration électronique et la dématérialisation de l'organisation au complet, des concepts adapté à la technologie qui mènent à de nouvelles innovations tel que l'intégration des signatures électronique des documents interne d'une organisation à la place de la signature manuelle afin de diminuer le nombre colossal de papier et ancre consommer quotidiennement, permettre la réduction des coûts et enfin pour améliorer la qualité du travail.

D'après l'étude de l'existant et l'analyse du besoin, le processus signature manuscrite consomme beaucoup de papier et d'encre, prend une grande durée pour être classé et terminé ce qui mène à l'augmentation des coûts de consommation, sans oublier les anomalies techniques qui apparaissent toujours durant le traitement et qui prennent du temps aussi pour être réglé.

C'est pourquoi nous avons proposé de concevoir un système de signature électronique, car principalement, il facilite l'échange des documents dans leur format électronique entre des différentes entités, ainsi qu'avec les usagers et les établissements externe. Avec la disposition d'un système de gestion de document, des dossiers au format électronique seront signés puis vérifiés électroniquement ainsi que l'intégration d'un système d'archivage électronique sera possible.

Ce projet a fait l'objet d'une expérience intéressante, a permis d'acquérir de nouvelles informations et connaissances ainsi d'exploité mes études durant le cursus universitaire.

Les solutions proposées dans ce mémoire ne se prétendent nullement être les meilleurs, car en système d'information, il existe toujours des anomalies et une maintenance est obligatoire pour assurer la robustesse d'une organisation.

D’autres aspects futurs sont envisagés pour élargir et approfondir le sujet du thème du mémoire sont :

- Signer les dossiers électroniquement en ligne sans avoir à se déplacer dans l’organisation ;
- Alignement stratégique d’une dématérialisation national des signatures de documents ;
- Réaliser une intégration du système de signature électronique sur des cartes d’identité électronique ;
- Mettre à disposition un système chargé de la gestion des certificats électronique qualifié par le gouvernement en Algérie.
- Telles sont les perspectives en matière d’étude qu’ouvre thème objet du mémoire.

Bibliographie

Webographie

- La dématérialisation : définition, méthodes et comparatifs, URL : https://www.archimag.com/demat-cloud/2019/11/13/glossaire-dematerialisation-10-mots-cles-definitions#securite
- LUDOVIC DESAUBRY ; sur la dématérialisation des dossiers documentaires : les enjeux technique https://memsic.ccsd.cnrs.fr/mem_00523899/document
- BONITA Soft La dématérialisation, https://fr.bonitasoft.com/bibliotheque/la-dematerialisation
- Bill FASSINOU, URL : https://www.developpez.com/actu/248771/Des-chercheurs-ont-reussi-a-briser-des-signatures-numeriques-de-documents-PDF-de-21-des-visionneuses-PDF-les-plus-connues/
- La signature électronique (2018) CLUSIF, URL : https://clusif.fr
- Fonctionnement de la signature électronique ; URL : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html
- Algorithme de chiffrement ; URL : https://stormimon.developpez.com/dotnet/signature-electronique/
- Constructions et vérification d'une signature électronique, URL : http://igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html
- La différence entre le coffre-fort numérique et E-archivage, URL : https://www.oodrive.fr/blog/securite/difference-entre-coffre-fort-electronique-et-archivage-numerique/
- Le parapheur électronique ; URL : https://www.neoledge.com/fr/parapheur-electronique-rival-parapheur-papier/?fbclid=IwAR1U7uHf1Eez16_BwLmMWhmm20RYtlB_exSKufVcrzyQCyyAzrv1CiBQcy4
- Visual Studio Code définition ; URL : https://bility.fr/definition-visual-studio-code/
- JavaScript définition ; URL : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203585-javascript/

- HTML définition ; URL : https://www.chiny.me/html-c-est-quoi-3-1.php
- CSS définition ; URL : https://www.ionos.fr/digitalguide/sites-internet/web-design/quest-ce-que-le-css/
- Bootstrap définition ; URL : https://www.journaldunet.com/developpeur/1159810-bootstrap-definition-tutoriels-astuces-pratiques/
- StarUML définition ; URL : https://air.imag.fr/index.php/StarUML
- WAMP SERVER définition ; URL : https://blog.lws-hosting.com/divers/quest-ce-que-wamp-guide-convivial-pour-les-debutants/

Ouvrages

- Dimitri Mouton, 1iere édition, Eyrolles le juillet 12, 2012, une préface sur la sécurité de la dématérialisation de la signature électronique au coffre-fort numérique, 310pages.
- Jean-Luc PAROUTY, Roland DIRLEWANGER, Dominique VAUFREYDAZ, la signature électronique, contexte, applications et mise en œuvre.
- L'Association française de normalisation est l'organisation française qui représente la France auprès de l'Organisation internationale de normalisation (ISO).

Annexe

Annexe 01 : la loi n°15-04 du 1er février 2015 fixant les règles générales relatives à la signature et à la certification électronique

Art. 18. — Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 100.000 DA à 500.000 DA, tout titulaire d'un certificat électronique qui continue à l'utiliser tout en sachant que ledit certificat est arrivé à échéance ou révoqué.

Art. 19. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 11 Rabie Ethani 1436 correspondant au 1er février 2015.

Abdelaziz BOUTEFLIKA.

———★———

Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques.

———

Le Président de la République,

Vu la Constitution notamment, ses articles 119, 120, 122, 125 et 126 ;

Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale ;

Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;

Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;

Vu l'ordonnance n° 75-59 du 26 septembre 1975, modifiée et complétée, portant code de commerce ;

Vu la loi n° 84-17 du 7 juillet 1984, modifiée et complétée, relative aux lois de finances ;

Vu la loi n° 88-01 du 12 janvier 1988 portant loi d'orientation sur les entreprises publiques économiques ;

Vu la loi n° 90-21 du 15 août 1990, modifiée et complétée, relative à la comptabilité publique ;

Vu la loi n° 2000-03 du 5 Joumada El Oula 1421 correspondant au 5 août 2000, modifiée, fixant les règles générales relatives à la poste et aux télécommunications ;

Vu l'ordonnance n° 03-03 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003, modifiée et complétée, relative à la concurrence ;

Vu la loi n° 04-02 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004, modifiée et complétée, fixant les règles applicables aux pratiques commerciales ;

Vu la loi n° 04-04 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004 relative à la normalisation ;

Vu la loi n° 04-08 du 27 Joumada Ethania 1425 correspondant au 14 août 2004, modifiée et complétée, relative aux conditions d'exercice des activités commerciales ;

Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008 portant code de procédure civile et administrative ;

Vu la loi n° 09-03 du 29 Safar 1430 correspondant au 25 février 2009 relative à la protection du consommateur et à la répression des fraudes ;

Vu la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication ;

Après avis du Conseil d'Etat ;

Après adoption par le Parlement ;

Promulgue la loi dont la teneur suit :

TITRE I

DISPOSITIONS GENERALES

Chapitre 1er

Objet

Article 1er. — La présente loi a pour objet de fixer les règles générales relatives à la signature et à la certification électroniques.

Chapitre 2

Définitions

Art. 2. — Il est entendu par :

1- Signature électronique : données sous forme électronique, jointes ou liées logiquement à d'autres données électroniques, servant de méthode d'authentification.

2- Signataire : personne physique qui détient des données de création de signature électronique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente.

3- Données de création de signature électronique : données uniques, telles que des codes ou des clés cryptographiques privés, que le signataire utilise pour créer une signature électronique.

4- Dispositif de création de signature électronique : matériel ou logiciel destiné à mettre en application les données de création de signature électronique.

5- Données de vérification de signature électronique : des codes, des clés cryptographiques publiques ou d'autres types de données, qui sont utilisées pour vérifier une signature électronique.

6- Dispositif de vérification de signature électronique : matériel ou logiciel destiné à mettre en application les données de vérification de signature électronique.

7- Certificat électronique : document sous forme électronique attestant du lien entre les données de vérification de signature électronique et le signataire.

8- Clé cryptographique privée : chaîne de chiffres détenue exclusivement par le signataire et utilisée pour créer une signature électronique, cette clé est liée à une clé cryptographique publique.

9- Clé cryptographique publique : chaîne de chiffres mise à la disposition du public afin de lui permettre de vérifier la signature électronique, elle est insérée dans le certificat électronique.

10- Autorisation : désigne le régime d'exploitation de services de certification électronique et se matérialise par le document officiel délivré au prestataire de manière personnelle lui permettant de commencer la fourniture effective de ses services.

11- Tiers de confiance : personne morale qui délivre des certificats électroniques qualifiés ou éventuellement fournit d'autres services en matière de certification électronique au profit des intervenants dans la branche gouvernementale.

12- Prestataire de services de certification électronique : personne physique ou morale qui délivre des certificats électroniques qualifiés et fournissant éventuellement d'autres services en matière de certification électronique.

13- Intervenants dans la branche gouvernementale : institutions et administrations publiques, établissements publics tels que définis par la législation en vigueur, institutions nationales autonomes, autorités de régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale.

14- Titulaire de certificat électronique : personne physique ou morale à laquelle un prestataire de services de certification ou un tiers de confiance a délivré un certificat électronique.

15- Politique de certification électronique : ensemble des règles et procédures organisationnelles et techniques liées à la signature et à la certification électroniques.

16- Audit : vérification de la conformité par rapport à un référentiel.

Chapitre 3

Principes généraux

Art. 3. — Sans préjudice de la législation en vigueur, nul ne peut être contraint d'accomplir un acte juridique signé électroniquement.

Art. 4. — Le document signé électroniquement est conservé dans sa forme d'origine. Les modalités de conservation du document signé électroniquement sont définies par voie réglementaire.

Art. 5. — Toutes les données et informations à caractère personnel recueillies par les prestataires de service de certification électronique, les tiers de confiance et les autorités de certification électronique ainsi que les bases de données qui les contiennent doivent être hébergées sur le territoire national et ne peuvent être transférées en dehors de celui–ci que dans les cas prévus par la législation en vigueur.

TITRE II

DE LA SIGNATURE ELECTRONIQUE

Chapitre 1er

Principes d'assimilation et de non-discrimination de la signature électronique

Art. 6. — Une signature électronique a pour fonction d'authentifier l'identité du signataire et de manifester l'adhésion de ce dernier au contenu de l'écrit sous forme électronique.

Art. 7. — La signature électronique qualifiée est une signature électronique qui satisfait aux exigences suivantes :

1- être réalisée sur la base d'un certificat électronique qualifiée,

2- être liée uniquement au signataire,

3- permettre l'identification du signataire,

4- être conçue au moyen d'un dispositif sécurisé de création de signature électronique,

5- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif,

6- être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

Art. 8. — Seule la signature électronique qualifiée est assimilée à une signature manuscrite, qu'elle soit le fait d'une personne physique ou morale.

Art. 9. — Nonobstant les dispositions de l'article 8 suscité, une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif qu'elle :

1. se présente sous forme électronique, ou

2. ne repose pas sur un certificat électronique qualifié, ou

3. n'est pas créée par un dispositif sécurisé de création de signature électronique.

Chapitre 2

Des dispositifs de création et de vérification de la signature électronique qualifiée

Art. 10. — Le dispositif de création de la signature électronique qualifiée doit être sécurisé.

Art. 11. — Le dispositif sécurisé de création de signature électronique est un dispositif de création de signature électronique qui satisfait aux exigences suivantes :

1- il doit, au moins, garantir, par les moyens techniques et les procédures appropriées, que :

a. les données utilisées pour la création de la signature électronique ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit assurée par tous les moyens techniques disponibles au moment de l'homologation ;

b. les données utilisées pour la création de la signature électronique ne puissent être trouvées par déduction et que la signature électronique soit protégée contre toute falsification par les moyens techniques disponibles au moment de l'homologation ;

c. les données utilisées pour la création de la signature électronique puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2- il ne doit pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Art. 12. — Le dispositif de vérification de la signature électronique qualifiée doit être fiable.

Art. 13. — Le dispositif fiable de vérification de la signature électronique est un dispositif de vérification de la signature électronique qui satisfait aux exigences suivantes :

1. les données utilisées pour vérifier la signature électronique correspondent aux données affichées lors de la vérification de la signature électronique ;

2. la signature électronique soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché ;

3. le contenu des données signées puisse être, si nécessaire, déterminé de manière sûre lors de la vérification de la signature électronique ;

4. l'authenticité et la validité du certificat électronique requis lors de la vérification de la signature électronique soient vérifiées de manière sûre ;

5. le résultat de la vérification ainsi que l'identité du signataire soient clairement et correctement affichés.

Art. 14. — La conformité du dispositif sécurisé de création de signature électronique qualifiée et du dispositif fiable de vérification de signature électronique qualifiée aux exigences édictées aux articles 11 et 13 ci-dessus est attestée par l'entité nationale en charge de l'homologation des dispositifs de création et de vérification de la signature électronique.

TITRE III

DE LA CERTIFICATION ELECTRONIQUE

Chapitre 1er

Du certificat électronique qualifié

Art. 15. — Le certificat électronique qualifié est un certificat électronique qui satisfait aux exigences suivantes :

1. être délivré par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée ;

2. ne peut être délivré qu'au signataire ;

3. doit comporter notamment :

a. une mention indiquant que le certificat électronique est délivré à titre de certificat électronique qualifié,

b. l'identification du tiers de confiance ou du prestataire de services de certification électronique autorisé émetteur du certificat électronique ainsi que le pays dans lequel il est établi,

c. le nom du signataire ou un pseudonyme permettant d'identifier ledit signataire,

d. la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat électronique est destiné,

e. des données de vérification de signature qui correspondent aux données de création de signature électronique,

f. l'indication du début et de la fin de la période de validité du certificat électronique,

g. le code d'identité du certificat électronique,

h. la signature électronique qualifiée du prestataire de services de certification électronique ou du tiers de confiance, qui délivre le certificat électronique,

i. les limites à l'utilisation du certificat électronique, le cas échéant,

j. les limites à la valeur des transactions pour lesquelles le certificat électronique peut être utilisé, le cas échéant et,

k. une référence au document certifiant la représentation d'une autre personne physique ou morale, le cas échéant.

Chapitre 2

Des autorités de certification électronique

Section 1

De l'autorité nationale de certification électronique

Art. 16. — Il est créé, auprès du Premier ministre, une autorité administrative indépendante jouissant de la personnalité morale et de l'autonomie financière, dénommée autorité nationale de certification électronique ci-après désignée « autorité ».

Les crédits nécessaires au fonctionnement de l'autorité sont inscrits au budget de l'Etat.

Art. 17. — Le siège de l'autorité est fixé par voie réglementaire.

Art. 18. — L'autorité est chargée de promouvoir l'utilisation et le développement de la signature et la certification électroniques et de garantir la fiabilité de leurs usages.

Dans ce cadre, elle a pour missions :

1. d'élaborer sa politique de certification électronique et veiller à son application, après avis favorable de l'entité en charge de l'approbation ;

2. d'approuver les politiques de certification électronique émises par les Autorités gouvernementale et économique de certification électronique ;

3. de conclure les conventions de reconnaissance mutuelle à l'international ;

4. de proposer au Premier ministre des avant-projets de textes législatifs ou réglementaires portant sur la signature électronique ou la certification électronique ;

5. d'auditer les Autorités gouvernementale et économique de certification électronique à travers l'entité gouvernementale en charge de l'audit.

L'Autorité est consultée pour la préparation de tout projet de texte législatif ou réglementaire en relation avec la signature ou la certification électroniques.

Art. 19. — L'Autorité est composée d'un conseil et de services techniques et administratifs.

Le conseil de l'Autorité se compose de cinq (5) membres, dont le président, nommés par le Président de la République en raison de leurs compétences, notamment, en matière des sciences techniques relatives aux technologies de l'information et de la communication (TIC), du droit des (TIC) et de l'économie des (TIC).

Le conseil dispose de toutes les prérogatives pour l'accomplissement des missions de l'Autorité, à ce titre il peut faire appel à toute compétence susceptible de l'aider dans ses travaux.

Le mandat des membres du conseil de l'Autorité est fixé à quatre (4) ans renouvelable une seule fois.

Art. 20. — Les services techniques et administratifs de l'Autorité sont gérés par un directeur général nommé par le Président de la République, sur proposition du Premier ministre.

L'organisation, le fonctionnement et les missions de ces services sont précisés par voie réglementaire.

Art. 21. — La fonction de membre du conseil de l'Autorité et du directeur général est incompatible avec tout autre emploi public, emploi dans le secteur privé, profession libérale, tout mandat électif, toute publicité ou subvention ainsi que la détention directe ou indirecte de tout intérêt dans les sociétés intervenant dans le secteur des technologies de l'information et de la communication (TIC).

Art. 22. — Le président du conseil de l'Autorité est ordonnateur de paiement, il peut déléguer cette prérogative au directeur général.

Art. 23. — Les décisions du conseil de l'Autorité sont prises à la majorité, en cas d'égalité des voix, celle du président est prépondérante.

Art. 24. — Le système de rémunération du président et des membres du conseil de l'Autorité et du directeur général est fixé par voie réglementaire.

Art. 25. — Le conseil de l'Autorité adopte son règlement intérieur qui sera publié au *Journal officiel*.

Section 2

De l'Autorité gouvernementale de certification électronique

Art. 26. — Il est créé auprès du ministre chargé de la poste et des technologies de l'information et de la communication, une autorité gouvernementale de certification électronique jouissant de l'autonomie financière et de la personnalité morale.

Art. 27. — La nature, la composition, l'organisation et le fonctionnement de cette Autorité gouvernementale de certification électronique sont fixés par voie réglementaire.

Art. 28. — L'Autorité gouvernementale de certification électronique est chargée du suivi et du contrôle de l'activité de certification électronique des tiers de confiance ainsi que la fourniture de services de certification électronique au profit des intervenants dans la branche gouvernementale.

Dans ce cadre, elle a pour missions :

1. d'élaborer et soumettre pour approbation, à l'Autorité, sa politique de certification électronique et veiller à son application ;

2. d'approuver les politiques de certification émises par les tiers de confiance et veiller à leurs applications ;

3. de conserver les certificats électroniques expirés et les données liées à leurs délivrances par les tiers de confiance afin de les remettre aux Autorités judiciaires compétentes, le cas échéant, conformément aux dispositions législatives et réglementaires en vigueur ;

4. de publier le certificat électronique de clé publique de l'Autorité ;

5. de transmettre à l'Autorité, périodiquement ou sur sa demande, l'ensemble des informations relatives à l'activité de certification électronique ;

6. de procéder à l'audit des tiers de confiance à travers l'entité gouvernementale chargée de l'audit, conformément à la politique de certification.

Section 3

De l'Autorité économique de certification électronique

Art. 29. — L'Autorité en charge de la régulation de la poste et des télécommunications est désignée, au sens de la présente loi, autorité économique de certification électronique.

Art. 30. — L'Autorité économique de certification électronique est chargée du suivi et du contrôle des prestataires de services de certification électronique qui fournissent les services de signature et de certification électroniques au profit du public.

Dans ce cadre, elle a pour missions :

1. d'élaborer et soumettre pour approbation, à l'Autorité, sa politique de certification électronique et veiller à son application ;

2. de délivrer des autorisations aux prestataires de service de certification électronique, après avis favorable de l'Autorité ;

3. d'approuver les politiques de certification émises par les prestataires de services de certification électronique et veiller à leurs applications ;

4. de conserver les certificats électroniques expirés et les données liées à leurs délivrances par les prestataires de services de certification électronique afin de les remettre aux autorités judiciaires compétentes, le cas échéant, conformément aux dispositions législatives et réglementaires en vigueur ;

5. de publier le certificat électronique de clé publique de l'Autorité ;

6. de prendre les mesures nécessaires pour assurer la continuité de services en cas d'incapacité du préstataire de services de certification électronique de fournir ses services ;

7. de transmettre à l'Autorité, périodiquement ou sur sa demande, l'ensemble des informations relatives à l'activité de certification électronique ;

8. d'auditer les demandeurs d'autorisation elle-même ou à travers les cabinets d'audit accrédités, conformément à la politique de certification ;

9. de veiller à l'existence d'une concurrence effective et loyale en prenant toutes les mesures nécessaires afin de promouvoir ou de rétablir la concurrence entre les prestataires de services de certification électronique ;

10. d'arbitrer les litiges qui opposent les prestataires de services de certification électronique entre eux ou avec les utilisateurs conformément à la législation en vigueur ;

11. de requérir des prestataires de services de certification électronique et de toute personne concernée, tout document ou information utile pour l'accomplissement des missions qui lui sont dévolues par la présente loi ;

12. d'élaborer le cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique et le soumettre à l'Autorité pour approbation ;

13. d'éffectuer tout contrôle conformément à la politique de certification électronique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique ;

14. de produire les rapports et statistiques publiques ainsi qu'un rapport annuel comportant la description de ses activités, sous réserve de la protection de la confidentialité.

L'autorité économique de certification électronique signale tout fait à caractère pénal au ministère public relevé à l'occasion de l'exercice de ses missions.

Section 4

Des voies de recours

Art. 31. — Les décisions prises par l'Autorité économique de certification électronique peuvent faire l'objet de recours auprès de l'Autorité dans un délai d'un (1) mois à compter de leur notification. Ce recours n'est pas suspensif.

Art. 32. — Les décisions prises par l'Autorité peuvent faire l'objet de recours auprès du Conseil d'Etat dans un délai d'un (1) mois à compter de leur notification. Ce recours n'est pas suspensif.

Chapitre 3

Du régime juridique de la prestation de service de certification électronique

Section 1

Du prestataire de services de certification électronique

Sous-section 1

De l'attestation d'éligibilité et de l'autorisation

Art. 33. — La prestation de service de certification électronique est soumise à une autorisation délivrée par l'autorité économique de certification électronique.

Art. 34. — Tout demandeur d'une autorisation pour la prestation de service de certification électronique doit réunir les conditions suivantes :

— être de droit algérien pour la personne morale ou de nationalité algérienne pour la personne physique ;

— disposer de capacités financières suffisantes ;

— avoir des qualifications et une expérience avérée dans le domaine des technologies de l'information et de la communication pour la personne physique ou le gérant de la personne morale ;

— ne pas avoir fait l'objet de condamnation pour crime ou délit incompatible avec l'activité de prestation de services de certification électronique.

Art. 35. — Préalablement à l'octroi de l'autorisation, une attestation d'éligibilité est délivrée pour une durée d'une (1) année, renouvelable une seule fois, elle est délivrée à toute personne physique ou morale pour la mise en place de tous les moyens nécessaires à l'activité de certification électronique.

Dans ce cas, l'attestation est notifiée dans un délai maximum de soixante (60) jours à compter de la date de réception de la demande attestée par un accusé de réception.

Le détenteur de cette attestation ne peut fournir les services de certification électronique qu'après l'obtention de l'autorisation.

Art. 36. — L'autorisation est délivrée au détenteur de l'attestation d'éligibilité et notifiée dans un délai maximum de soixante (60) jours à compter de la date de réception de la demande de l'autorisation attestée par un accusé de réception.

Art. 37. — Le refus de délivrance de l'attestation d'éligibilité et de l'autorisation doit être motivé, il est notifié contre un accusé de réception.

Art. 38. — L'autorisation est assortie d'un cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique ainsi que la signature du certificat électronique du prestataire par l'autorité économique de certification électronique.

Art. 39. — L'attestation d'éligibilité et l'autorisation sont personnelles et ne peuvent être cédées à des tiers.

Art. 40. — L'autorisation est délivrée pour une durée de cinq (5) ans. Arrivée à terme, elle est renouvelée conformément aux conditions définies dans le cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

L'autorisation est soumise au paiement d'une contrepartie financière dont le montant est fixé par voie réglementaire.

Sous-section 2

De la prestation de service de certification électronique

Art. 41. — Le prestataire de services de certification électronique est chargé de l'enregistrement, de l'émission, de la délivrance, de la révocation, de la publication et de la conservation des certificats électroniques, conformément à sa politique de certification approuvée par l'autorité économique de certification électronique.

Art. 42. — Le prestataire de services de certification électronique doit préserver la confidentialité des données et des informations liées aux certificats électroniques délivrés.

Art. 43. — Le prestataire de services de certification électronique ne peut recueillir des données personnelles qu'après consentement explicite de l'intéressé.

Le prestataire ne doit recueillir que les données personnelles nécessaires à la délivrance et à la conservation du certificat électronique. Ces données ne peuvent être traitées à d'autres fins.

Art. 44. — Préalablement à la délivrance du certificat électronique, le prestataire de services de certification électronique doit vérifier la complémentarité des données de création et vérification de signature.

Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de services de certification électronique délivre un ou plusieurs certificats électroniques à toute personne qui en fait la demande.

En ce qui concerne les personnes morales, le prestataire de services de certification électronique tient un registre contenant l'identité et la qualité du représentant légal de la personne morale qui fait usage de la signature liée au certificat électronique qualifié, de manière à pouvoir établir l'identité de la personne physique à chaque utilisation de cette signature électronique.

Art. 45. — A la demande du titulaire du certificat électronique qualifié, préalablement identifié, le prestataire de services de certification électronique révoque le certificat électronique dans les délais fixés dans la politique de certification.

Le prestataire de services de certification électronique révoque également un certificat électronique qualifié lorsque :

1. il a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat électronique ne sont plus conformes à la réalité ou que la confidentialité des données de création de signature a été violée ;

2. il n'est plus conforme à la politique de certification ;

3. le prestataire de services de certification est informé du décès de la personne physique ou de la dissolution de la personne morale titulaire du certificat électronique.

Le prestataire de services de certification électronique est tenu d'informer le titulaire du certificat électronique qualifié de la révocation et sa motivation.

Le prestataire de services de certification électronique est tenu de notifier au titulaire, dans les délais prescrits dans la politique de certification, l'expiration de son certificat électronique qualifié.

La révocation d'un certificat électronique qualifié est définitive.

Art. 46. — Conformément à sa politique de certification approuvée par l'autorité économique de certification électronique, le prestataire de services de certification électronique, prend les mesures nécessaires afin de répondre à une demande de révocation.

La révocation est opposable aux tiers à partir de sa publication, conformément à la politique de certification électronique du prestataire de services de certification électronique.

Art. 47. — Le prestataire de services de certification électronique est tenu de transférer à l'autorité économique de certification électronique les informations concernant les certificats électroniques qualifiés après leur expiration en vue de leur conservation.

Art. 48. — Le prestataire de services de certification électronique ne peut ni conserver, ni copier les données de création de signature de la personne à laquelle il a fourni un certificat électronique qualifié.

Art. 49. — Les prestataires de services de certification électronique ont l'obligation d'appliquer des tarifs pour les services fournis en adéquation avec les principes de tarification définis par l'autorité économique de certification électronique et fixés par voie réglementaire.

Art. 50. — Le prestataire de services de certification électronique fournit ses services dans le cadre des principes de transparence et de non-discrimination.

Le prestataire de services de certification électronique ne peut refuser de fournir ses services sans motif valable.

Sous-section 3

Du contrôle et de l'audit

Art. 51. — Un audit d'évaluation est réalisé, sur requête du détenteur de l'attestation d'éligibilité, préalablement à l'octroi de l'autorisation de prestation de services de certification électronique, par l'autorité économique de certification électronique ou par un cabinet d'audit accrédité, conformément à la politique de certification électronique de l'autorité économique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

Art. 52. — Le contrôle des prestataires de services de certification électronique par l'autorité économique s'effectue, notamment, à travers des audits périodiques et des contrôles inopinés, conformément à la politique de certification de l'autorité économique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

Section 2

De la responsabilité du prestataire de services de certification et du titulaire de certificat électronique

Sous-section 1

Des obligations et de la responsabilité du prestataire de services de certification électronique

Art. 53. — Un prestataire de services de certification électronique qui délivre un certificat électronique qualifié est responsable du préjudice causé à tout organisme ou personne physique ou morale qui se fie à ce certificat électronique, pour ce qui est de :

1. l'exactitude de toutes les informations contenues dans le certificat électronique qualifié à la date où il a été délivré et la présence, dans ce certificat électronique, de toutes les données prescrites pour un certificat électronique qualifié ;

2. l'assurance que, au moment de la délivrance du certificat électronique, le signataire identifié dans le certificat électronique qualifié détenait les données de création de signature correspondant aux données de vérification de signature fournies ou identifiées dans le certificat électronique ;

3. l'assurance que les données de création et de vérification de signature puissent être utilisées de façon complémentaire ;

Sauf si le prestataire de services de certification électronique apporte la preuve qu'il n'a commis aucune négligence.

Art. 54. — Le prestataire de services de certification électronique qui a délivré un certificat électronique qualifié est responsable du préjudice résultant de la non révocation de ce certificat, causé à un organisme ou à une personne physique ou morale qui se prévaut du certificat électronique, sauf si le prestataire de services de certification électronique apporte la preuve qu'il n'a commis aucune négligence.

Art. 55. — Le prestataire de services de certification électronique peut indiquer, dans un certificat électronique qualifié, les limites fixées à son utilisation, à condition que cette indication soit visible et compréhensible par des tiers. Dans ce cas, le prestataire de services de certification électronique ne peut être tenu responsable du préjudice résultant de l'usage d'un certificat électronique qualifié qui dépasse les limites fixées à son utilisation.

Art. 56. — Le prestataire de services de certification électronique peut indiquer, dans un certificat électronique qualifié, la valeur maximale des transactions pour lesquelles le certificat électronique peut être utilisé, à condition que cette indication soit visible et compréhensible par des tiers. Dans ce cas, le prestataire de services de certification électronique n'est pas responsable des dommages qui résultent du dépassement de cette valeur maximale.

Art. 57. — Le prestataire de services de certification électronique n'est pas responsable du préjudice résultant du non-respect des conditions d'utilisation des données de création de la signature électronique par le titulaire du certificat électronique qualifié.

Art. 58. — Le prestataire de services de certification électronique informe l'autorité économique de certification électronique dans un délai défini dans la politique de certification de cette autorité, de son intention de cesser ses activités de prestataire de services de certification électronique ainsi que de toute action qui pourrait conduire à la cessation de ses activités.

Dans ce cas, le prestataire de services de certification électronique se conforme aux dispositions de la politique de certification de l'autorité économique de certification électronique relatives à la continuité de service.

La cessation d'activité engendre le retrait de l'autorisation.

Art. 59. — Le prestataire de services de certification électronique qui cesse ses activités pour des raisons indépendantes de sa volonté, doit informer immédiatement l'autorité économique de certification électronique qui procède à la révocation de son certificat électronique qualifié après appréciation des raisons évoquées.

Dans ce cas, le prestataire prend les mesures nécessaires, prévues dans la politique de certification électronique de l'autorité économique, pour la conservation des informations liées aux certificats électroniques qualifiés délivrés.

Art. 60. — Le prestataire de services de certification électronique est tenu de souscrire aux assurances prévues dans la politique de certification électronique de l'autorité économique.

Sous-section 2

De la responsabilité du titulaire de certificat électronique

Art. 61. — Dès la signature de son certificat électronique, le titulaire est seul responsable de la confidentialité des données de création de sa signature.

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

Lorsqu'un certificat électronique est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut utiliser les données de création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de services de certification électronique.

Art. 62. — Le titulaire ne peut utiliser son certificat électronique qualifié à des fins autres que celles pour lesquelles il a été délivré.

Chapitre 4

De la reconnaissance mutuelle

Art. 63. — Les certificats électroniques délivrés par un prestataire de services de certification électronique établi dans un pays étranger ont la même valeur que ceux délivrés par un prestataire de services de certification électronique établi en Algérie, à condition que ce prestataire étranger agisse dans le cadre d'une convention de reconnaissance mutuelle conclue par l'autorité.

TITRE IV

DES SANCTIONS

Chapitre 1er

Des sanctions pécuniaires et administratives

Art. 64. — Lorsque le prestataire de services de certification électronique ne respecte pas les dispositions de son cahier des charges ou de sa politique de certification électronique approuvée par l'Autorité économique de certification électronique, cette dernière prononce a son encontre une sanction pécuniaire dont le montant varie de deux cent mille dinars (200.000 DA) à cinq millions de dinars (5.000.000 DA), selon la classification des manquements, prévue dans le cahier des charges du prestataire et le met en demeure de se conformer auxdites dispositions dans un délai allant de huit (8) jours à trente (30) jours, selon le cas. Les griefs retenus contre le prestataire lui sont notifiés afin de lui permettre de présenter, dans les délais précités, ses justifications écrites.

Si le prestataire de services ne se conforme pas à la mise en demeure, l'autorité économique prononce à son encontre le retrait de son autorisation et la révocation de son certificat, selon le cas, après avis favorable de l'autorité.

Les modalités de recouvrement des sommes correspondantes à la sanction pécuniaire mentionnée au premier paragraphe du présent article sont fixées par voie réglementaire.

Art. 65. — Dans le cas d'une atteinte à des impératifs exigés par la défense nationale et la sécurité publique par un prestataire de services de certification électronique, l'autorité économique de certification électronique procède, après avis favorable de l'Autorité, au retrait, sans délais, de l'autorisation.

Ses équipements font l'objet de mesures conservatoires conformément à la législation en vigueur et ce, sans préjudice des poursuites pénales.

Chapitre 2

Des dispositions pénales

Art. 66. — Est punie d'une peine d'emprisonnement de trois (3) mois à trois (3) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement, toute personne qui use de fausses déclarations pour l'obtention d'un certificat électronique qualifié.

Art. 67. — Est puni d'une peine d'emprisonnement de deux (2) mois à une (1) année et d'une amende de 200.000 DA à 1.000.000 DA ou de l'une de ces deux peines seulement, tout prestataire de services de certification électronique ayant failli à l'obligation d'informer l'autorité économique de certification électronique de sa cessation d'activité, dans les délais prévus aux article 58 et 59 de la présente loi.

Annexe 02 : Les autorités algériennes de certification électronique

L'autorité nationale de certification électronique

- Art. 16. Il est créé, auprès du Premier ministre, une autorité administrative indépendante jouissant de la personnalité morale et de l'autonomie financière, dénommée autorité nationale de certification électronique ci-après désignée « autorité ». Les crédits nécessaires au fonctionnement de l'autorité sont inscrits au budget de l'état ;
- Art. 17. Le siège de l'autorité est fixé par voie réglementaire ;
- Art. 18. L'autorité est chargée de promouvoir l'utilisation et le développement de la signature et la certification électroniques et de garantir la fiabilité de leurs usages.

L'autorité gouvernementale de certification électronique

- Art. 26. Il est créé auprès du ministre chargé de la poste et des technologies de l'information ; et de la communication, une autorité gouvernementale de certification électronique jouissant de l'autonomie financière et de la personnalité morale ;
- Art. 27. La nature, la composition, l'organisation et le fonctionnement de cette Autorité gouvernementale de certification électronique sont fixés par voie réglementaire ;
- Art. 28. L'Autorité gouvernementale de certification électronique est chargée du suivi et du contrôle de l'activité de certification électronique des tiers de confiance ainsi que la fourniture de services de certification électronique au profit des intervenants dans la branche gouvernementale.

L'autorité économique de certification électronique

- Art. 29. L'Autorité en charge de la régulation de la poste et des télécommunications est désignée, au sens de la présente loi, autorité économique de certification électronique.
- Art. 30. L'Autorité économique de certification électronique est chargée du suivi et du contrôle des prestataires de services de certification électronique qui fournissent les services de signature et de certification électroniques au profit du publique.