République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université SAAD DAHLAB 1

MEMOIRE DE FIN D'ETUDE POUR L'OBTENTION DE MASTER PROFESSIONNEL

Filière : Sécurité de systèmes d'information

CHIFFREMENT DES DOCUMENTS DANS UNE PLATEFORME DE GED : AUTHENTIFICATION ET INTEGRITE

Présenté par

- DAHMANI Douniazed
- MOUZAOUI Nawal

Maitre de stage

- MAREDJ AZZE-Eddine

Membres de jury :

- **Promotrice** : BEY Fella
- **Présidente** : OUKID S
- **Examinateur** : BENAISSI

Année Universitaire : 2021-2022

Remerciements

Avant tout on remercie **ALLAH** le tout puissant de nous avoir guidé, aidé et donné la foi, la force et le courage pour accomplir ce travail.

En préambule à ce mémoire, il nous est agréable de citer et adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leurs aides et qui ont contribué à l'élaboration et au bon déroulement de ce travail :

A notre encadreur **Mr MAREDJ Azze-Eddine**

A notre promotrice **Mme BEY Fella**

« Nos remerciements les plus respectueux de nous avoir aidé dans ce travail, le regard critique, juste et avisé que vous aviez porté sur nos travaux ne peut que nous encourager à être engagées dans nos recherches »

A tout le corps enseignants et le personnel du département informatique qui ont contribué de près ou de loin à notre formation.

Aux membres de jury qui auront à juger ce travail et d'avoir accepté de l'examinateur.

A la fin, il nous est agréable d'adresser nos vifs remerciements à tous ceux qui nous ont aidés de près ou de loin à élaborer ce mémoire.

Dédicaces

Je dédie ce modeste travail en signe de reconnaissance et du respect à :

Mes chandelles de vie, mes parents, qui m'ont donné la vie et qui ont toujours été la pour moi.

« Vous avez tous sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous m'avez donné un magnifique modèle de labeur et de persévérance. Je suis redevable d'une éducation dont je suis fière »

Ma chère petite sœur **Ryma**

« Parfois j'oublie que tu es partie et je me sens un peu plus sereine. Dans ces moments j'ai l'impression que la vie s'est arrêtée, avant ton hospitalisation. J'ai ce sentiment que tu es toujours la et que tu pourras assister à ma soutenance et partager ce bon moment avec toi chère sœur. Paix à ton âme la prunelle de mes yeux »

Mes frères Rachid, Sofiane, et mes quatre perles frangines : Kahina, Hayat, Lynda, Nedjma.
Mes chères belles sœurs Lynda et Hakima.

« Qui m'ont toujours entouré et motivé sans cesse tout le long de ce projet, à qui je souhaite un avenir radieux plein de réussite »

Aux membres de ma famille : Nassim, Nora, Lyza, Yassmin, Cherifa, Lyza, Imane, Sara, Sylia, Nabila, Ikram, Farid, Cherif, Thanina.

« Qui m'ont motivé et soutenu durant la réalisation de ce travail, je vous aime énormément »

A notre cher ami **MOULOUD Ibrahim**

« Qui nous a guidé et orienté tout au long de ce projet, à qui je souhaite que de la réussite et du bonheur dans sa vie inchallah »

A mes chères copines Silia, Yassmine, Hamida, Kamelia, Sara, Amel, Katia, Lydia, Lydia, Sadia, Halima, Asma, Lila, Nadia, Massilia, Samia et Sihem.

Aux personnes qui étaient toujours à mes cotés, mes aimables amies, mes collègues.

A tous ces intervenants, je présente mon respect et ma gratitude. **Nawal**

Je voudrais dédier le présent travail tout spécialement

À mes très chers parents

Ma mère **« qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour tout son assistance et sa présence dans ma vie ».**

Mon père **« qui pourra être fier et trouvera ici le résultat de longues années de sacrifices pour m'avoir aidé à avancer dans la vie. Merci pour les valeurs nobles, l'éducation et le soutien permanent venus de toi ».**

A mon frère Abderrahmane et ma petite sœur FatimaElZohra **« qui ont été toujours à mes côtés tout au long de ce projet, à qui je souhaite un avenir radieux plein de réussite »**

A toute ma famille, mes tantes, mes cousines Hanen, Ilhem, Amira, NourElHouda, Bassema, Samira, Ahlem, Nihad, Amina, Serine, Chahinez et Sihem

« Pour ses soutien moral et leurs conseils précieux tout au long de mes études »

A mon cher grand-père

« A qui je souhaite une bonne santé »

A mon cher binôme Nawal

« Pour son entente et sa sympathie »

A mes amis Walid, Narimene, Hayet, Fedwa, Achoik

« Pour leurs aides et supports dans les moments difficiles »

A tous ceux qui m'aiment.

A tous ceux que j'aime.

Enfin, à toute personne ayant participé de loin ou de près à la réalisation de ce travail **DOUNIAZED**

Résumé

Dans l'entreprise, l'information avec tous ses formats (papier, électronique. etc.) est un capital aussi important que le capital humain, aussi primordial que le capital financier, et qu'il faut gérer convenablement. Maîtriser ce capital est pour l'entreprise d'aujourd'hui le principal enjeu afin de survivre, réagir et relever le défi du progrès. De nos jours, le défi est lancé grâce à la gestion électronique de documents (GED) qui s'avère se trouver au centre des procédures critiques de toute entreprise. Vu la fragilité et la facilité de manipulation de l'information électronique, ce capital, aussi important soit-il, est exposé à de grands risques de perte, si on ne peut satisfaire aux exigences portant sur l'intégrité, l'authenticité, la fiabilité de cette information numérique. Ce problème concerne aussi bien les archivistes, les auteurs de documents, les gestionnaires de documents que les concepteurs de systèmes. C'est dans ce cadre-là que se définit le sujet de notre mémoire dont le principal objectif est d'étudier les différents aspects liés à la cryptographie pour assurer l'intégrité, l'authenticité des documents électroniques dans une plateforme de gestion électronique de documents (GED). Le travail qu'on a fait dans ce mémoire consiste à implémenter la partie accès et diffusion des documents dans un système de GED, et à implémenter un outil de signature numérique, s'appuyant sur une technologie cryptographique. La solution que nous avons développé et que sera exposée le long de ce mémoire de Master consiste à signer numériquement des documents en se basant sur la cryptographie asymétrique et en garantissant l'identité du signataire par l'utilisation des fonctions de hachage et des certificats numériques.

Mots clés : document électronique, cryptographie asymétrique, signature numérique, certificat numérique, fonction de hachage.

Abstract

In the company, information in all its formats (paper, electronic, etc.) is a capital as important as human capital, as essential as financial capital, and must be managed properly. Mastering this capital is for the company of today the main stake in order to survive, react and take up the challenge of progress. Nowadays, the challenge is launched thanks to electronic document management (EDM) which is at the center of the critical procedures of any company. Given the fragility and ease of manipulation of electronic information, this capital, as important as it is, is exposed to great risks of loss, if we cannot meet the requirements concerning the integrity, authenticity and reliability of this digital information. This problem concerns archivists, document authors, document managers as well as system designers. It is within this framework that is defined the subject of our thesis whose main objective is to study the various aspects related to cryptography to ensure the integrity, authenticity of electronic documents in a platform of electronic document management (EDM). The work we have done in this thesis consists in implementing the access and distribution of documents in an EDM system, and in implementing a digital signature tool, based on a cryptographic technology. The solution that we have developed and that will be exposed along this Master thesis consists in digitally signing documents based on asymmetric cryptography and guaranteeing the identity of the signatory by using hash functions and digital certificates.

Keywords: electronic document, asymmetric cryptography, digital signature, digital certificate, hash function.

ملخص

في الشركة ، المعلومات بجميع أشكالها (الورقية ، الإلكترونية ، إلخ) هي رأس مال لا يقل أهمية عن رأس المال البشري ، وضرورية مثل رأس المال المالي ، ويجب إدارتها بشكل صحيح. إن إتقان رأس المال هذا هو بالنسبة للشركة اليوم الحصة الرئيسية من أجل البقاء والتفاعل والاستجابة لتحدي التقدم. في الوقت الحاضر ، يتم إطلاق التحدي بفضل إدارة المستندات التي تقع في قلب الإجراءات الحرجة لأي شركة. نظرًا لهشاشة وسهولة التلاعب بالمعلومات (EDM) الإلكترونية الإلكترونية ، فإن رأس المال هذا ، على الرغم من أهميته ، يتعرض لمخاطر كبيرة تتمثل في الخسارة ، إذا لم نتمكن من تلبية المتطلبات المتعلقة بسلامة هذه المعلومات الرقمية ومصداقيتها وموثوقيتها. تتعلق هذه المشكلة بالمحفظين ومؤلفي المستندات ومديري المستندات وكذلك مصممي النظام. في هذا الإطار ، تم تحديد موضوع أطروحتنا التي يتمثل هدفها الرئيسي في دراسة الجوانب المختلفة المتعلقة بالتشفير لضمان سلامة وصحة المستندات الإلكترونية في منصة إدارة يتمثل العمل الذي قمنا به في هذه الأطروحة في تنفيذ الوصول إلى المستندات وتوزيعها .(EDM) المستندات الإلكترونية ، وتنفيذ أداة التوقيع الرقمي ، بناءً على تقنية التشفير. الحل الذي طورناه والذي سيتم عرضه على طول EDM في نظام أطروحة الماجستير هذه يتمثل في توقيع المستندات رقميًا بناءً على التشفير غير المتماثل وضمان هوية الموقّع باستخدام وظائف التجزئة والشهادات الرقمية.

الكلمات الدالة. وثيقة إلكترونية ، تشفير غير متماثل ، توقيع رقمي ، شهادة رقمية ، وظيفة تجزئة

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Dans notre vie quotidienne, qu'elle soit personnelle ou professionnelle, nous sommes amenés à utiliser plusieurs dizaines de documents, voire des centaines. Ainsi, avec le développement de l'informatique et des technologies associées, nous sommes arrivés à gérer des documents sous forme électronique, aussi bien en ce qui concerne les identifiants que les contenus : c'est la gestion électronique de documents, aussi dite gestion de documents électroniques et pour plus de précision gestion électronique de documents électroniques.

Le principal objectif de notre travail est d'étudier les différents aspects liés à la cryptographie pour assurer l'intégrité, l'authenticité, la confidentialité et le non répudiation des documents électroniques dans une plateforme de gestion électronique de documents (GED).

La cryptographie, ou l'art de crypter, d'encoder des informations, est désormais devenue une science à part entière. Au carrefour des mathématiques, de l'informatique et parfois de la physique, elle réalise ce dont la civilisation a besoin depuis son existence : le secret. Pour éviter la guerre, pour protéger les gens, il faut parfois cacher quelque chose…

Pendant de nombreuses années, la GED a été la mauvaise relation de l'informatique. Seules les entreprises qui doivent traiter beaucoup de documents prendraient le risque. La GED s'impose progressivement dans les systèmes d'information au travers d'applications ciblées et rentables. C'est pour cette raison que l'GED est désormais considérée par de nombreuses organisations comme un facteur important de productivité et d'efficacité, ainsi qu'un moyen de concurrence.

La GED représente « un ensemble d'outils et de techniques qui permettent de dématérialiser, classer, gérer et stocker des documents vivants dans le cadre normal des activités d'entreprise ».

Le travail qu'a été demandé dans ce mémoire consiste à implémenter la partie accès et diffusion des documents dans un système de GED, et à implémenter un outil de signature numérique, s'appuyant sur une technologie cryptographique. La solution que nous avons développé et que sera exposée le long de ce mémoire de Master consiste à signer numériquement des documents en se basant sur la cryptographie asymétrique et en garantissant l'identité du signataire par l'utilisation des certificats numériques.

Le mémoire est organisé en quatre chapitres :

Le premier chapitre est consacré à la définition des concepts de bases et les regards sur la gestion électronique des documents (GED).

Le deuxième chapitre est consacré à la définition des concepts de bases et les principes essentiels dans le domaine de la cryptographie.

Le troisième chapitre traite l'analyse des besoins et la conception de la solution que nous avons proposée.

Le quatrième chapitre regroupe les outils pour la réalisation de la solution proposée et quelques interfaces de notre application.

Nous terminons ce travail par une conclusion générale et quelques perspectives.

Chapitre 1

La gestion électronique des documents

1- Introduction

Une entreprise acquiert et produit tout au long de son activité un grand nombre de documents. Certains sont vitaux, et doivent être conservés pour répondre à l'environnement réglementaire. D'autres encore, les documents dits « de travail » tels que les comptes-rendus, les rapports, les documents bureautiques, peuvent être consultés dans le but de prendre une décision. Par conséquent, la gestion et la conservation des documents au sein de l'entreprise sont des activités essentielles. Elles répondent à des objectifs d'ordre juridique et légal, à des enjeux patrimoniaux en constituant une mémoire d'entreprise et conservant les documents relatifs à l'histoire et à l'activité de l'entreprise et à des enjeux stratégiques.

2- La gestion électronique de document : Concepts et définitions

En 1996, Jacques Chaumier définissait la Gestion Electronique de Documents comme un « ensemble de logiciels concourant à réaliser les diverses étapes de la chaîne de traitement d'un document : acquisition, restitution, diffusion» [19]

La gestion électronique de documents ou GED désigne l'ensemble des techniques utilisant d'une part les ressources de l'ordinateur et ses périphériques d'entrée (numériseur optique), de stockage (disque magnétique, disque optique numérique) et de sortie (imprimante laser) et d'autre part les ressources d'un logiciel documentaire ou d'un système de gestion de bases de données pour saisir, indexer, stocker, rechercher, consulter et transmettre information. [2]

2.1 Les types de la GED

Il existe plusieurs types de GED définis dans les points suivants:

- La GED administrative qui porte sur la gestion de documents électroniques administratifs, comme les factures, les bons de commande, pour accéder rapidement aux images de ces documents.

- La GED bureautique se base sur les plateformes de bureautique permettant de gérer les documents vivants dans leurs formats d'origine (Word, Excel) par exemple des cahiers des charges, des fiches, des comptes rendus.

- La GED documentaire gère les documents de référence de l'entreprise comme les documents normatifs, l'offre de référence.

- La GED technique gère les documents techniques propres à un métier comme les plans.

2.2 Principes généraux du fonctionnement d'un système de gestion électronique des documents

Il existe plusieurs principes du fonctionnement d'un système de gestion électronique de documents :

- Intégration de document :

Lorsqu'on intègre un fichier dans un outil de GED, ce processus d'intégration, peut se faire de plusieurs manières. Elles peuvent elles-mêmes conduire à plusieurs étapes dans le processus. En effet l'intégration dépend de fichier initial (papier, fax, document électronique : mail, PDF, etc. Ces derniers posent moins de problèmes car ils ne nécessitent pas une numérisation de l'information).[3]

- L'indexation des documents :

L'indexation doit être dissociée de la numérisation. Cette dissociation doit permettre par exemple de numériser des documents et de les ranger sans indexation dans des boites à lettres d'images, de créer des indexations sans y associer d'emblée des images, de rattacher un document numérisé à un nombre illimité d'indexations différentes et, à l'inverse, de rattacher à une même indexation un nombre illimité d'images. L'indexation doit pouvoir se faire document par document ou par lots de documents.

L'enregistrement des données doit pouvoir se faire en longueur variable pour économiser de la place mémoire.[2]

- Stockage des documents :

Le stockage des documents est très important et il faut prendre en considération plusieurs facteurs. Les serveurs de stockage doivent répondre à certains besoins comme suit :

- De volumétrie des documents.
- De temps d'accès aux informations.
- De type de documents et de leur impact stratégique, dont il faut comprendre quelles sont les conséquences tant du point de vue légal qu'économique pour l'entreprise si un document n'est pas conservé.
- De respect des contraintes légales des documents[3]

Ces quatre facteurs sont très importants, car ils vont définir :

- L'espace de stockage nécessaire à un temps T ainsi que l'espace prévisionnel.
- Le temps maximum d'attente pour accéder à un document et donc le type de disques qu'il faut prévoir pour répondre aux besoins de l'entreprise.
- Les documents à durée de vie courte qui pourront être supprimés selon l'impact stratégique et légal de ce dernier, afin de libérer de l'espace.
- L'espace de backup pour la GED afin de pouvoir reconstituer « la bibliothèque de l'entreprise »en cas de panne.[3]

- La recherche :

La recherche doit être multicritères et multi champs. Une requête doit pouvoir intégrer:

- ✓ les opérateurs booléens (ET, OU, SAUF),
- ✓ les opérateurs arithmétiques,
- ✓ les troncatures gauche et droite,
- ✓ au moins quatre niveaux de parenthèses

On doit pouvoir combiner une étape de recherche avec un nouveau critère, faire un historique des étapes de recherche et afficher le résultat de la recherche par pertinence décroissante avec indication de la nature et de la provenance du document.[2]

- Restitution des documents :

Les documents stockés au moyen d'un système de GED doivent pouvoir être restitués conformément à l'original afin d'être consultés, imprimés, transmis ou intégrés dans des applicatifs tels que : ERP (Entreprise Resource Planning), tableau de décisions, logiciels comptables, etc.[3]

3- Le document numérique/électronique: définition et contraintes

Ici on va voir la définition d'un document numérique ou électronique, et toutes ses contraintes

3.1 Définition d'un document

Si l'on réfère au plus connu et au plus utilisé des dictionnaires. Le Robert, nous trouvons le mot document la définition suivante : « Tout écrit qui sert de preuve ou de renseignement.» Cette définition est riche d'enseignement quant à la perception de la notion de document. La consultation du vocabulaire de la documentation publié par l'Association française de normalisation (AFNOR) sous ce même mot nous précise qu'il s'agit d'un « Ensemble de supports d'information, des données existantes et leur significations». Cette définition plus technique de la notion de support. Il ne peut y avoir de document sans support de l'information, objet matériel dans ou sur lequel sont représentées les données apportées par le document. Il y a de nombreux exemples de reportages diffusés à la télévision en direct n'ayant donné lieu à aucun enregistrement sur un support matériel et dont l'existence est ainsi disparue. [19]

Les documents sont les porteurs, les produits et la trace des transactions. Les transactions (actions menées à travers un objet) sont des actions communiquées d'une personne à une autre, d'une personne à un dépôt d'informations (exemple: un meuble à dossiers, une base de données sur ordinateur), ou d'un dépôt d'informations à une personne ou à un ordinateur. Un document représente alors un récapitulatif de toutes les communications associées à une transaction d'affaires. Les transactions doivent passer par au moins une couche de logiciels et par plusieurs couches de matériels ou connexions afin d'être communiquées [Bear94a]. Une transaction peut être aussi définie comme étant une action publique impliquant plus d'une personne et pour que cette action soit entamée et complétée, elle doit avoir un point de départ et un point final.[4]

Traditionnellement, les documents ont été définis comme étant des objets physiques (fichiers papier, registres, etc.) contenant des informations. Cependant, cette ancienne conception du document n'est plus valide à l'ère électronique. En effet, avec les technologies électroniques, les documents peuvent être transportés d'un support à un autre, et d'un contexte à un autre (en les copiant, en les digitalisant, etc.) De plus, l'information contenue dans les documents n'est plus désormais lisible et compréhensible par l'homme qu'à travers les logiciels et le matériel utilisés pour créer ces documents. En un mot, l'objet physique n'est pas le document, mais le support du document [5] .

Pour résoudre ce problème, il faut mettre à jour la définition du terme 'document' indépendamment de son format et de son support, comme c'est le cas des archives australiennes qui définissent le document comme suit :

Contenu : c'est I ‘information, par exemple : texte, données, symboles, images, sons. etc.

Structure : c'est l'apparence et l‘arrangement du contenu, par exemple : les liens entre les champs, le langage, le style, etc.

Contexte : c'est l'information de base qui permet de comprendre les environnements techniques et commerciaux entourant le document, par exemple : métadonnées, applications logistiques, provenance, etc [6].

3.2 Définition d'un document électronique

Un document électronique est un document qui peut être manipulé, transmis ou traité par un ordinateur numérique [5].

Ainsi, le qualificatif «électronique» fait référence au mode de représentation des informations, c'est le mode numérique par opposition au mode analogique. Les origines des documents électroniques sont diverses :

- Documents non numériques (papier, vidéo, son, etc) qui sont numérisés par captage de l’image;
- Documents numériques issus des traitements de texte, tableur, etc ;
- Documents créés à partir de différents supports numériques et non numériques (palette graphique permettant en même temps le dessin électronique et la numérisation des dessins, etc).

Les données dans les environnements électroniques sont très transformatives, participant ainsi à une surabondance d'activités transactionnelles. Les systèmes automatiques ont la capacité de saisir et d'enregistrer beaucoup plus d'informations descriptives qu'il l'était techniquement et économiquement possible avec les systèmes manuels. De plus, les documents électroniques sont extrêmement faciles à traiter; ils sont :

-**reproductibles :** un même document peut être reproduit sur plusieurs écrans ou imprimantes simultanément, dupliqué sur support magnétique, transféré sur une autre machine, etc;

- **modifiables :** on peut faire du couper-coller, des remises en page, etc;

- **transmissibles** : par les réseaux informatiques locaux ou à grande distance. [3]

3.3 Les caractéristiques d'un document électronique

Consignation de l'information : tandis que le contenu d'un document traditionnel est consigné sur un support papier ou autre, à l'aide de caractères alphabétiques ou illustrations, compréhensibles par l'homme, le contenu d'un document électronique est consigné sur un support [5] ou même plusieurs (comme c'est le cas du multimédia : texte+son+vision)[6] , et est représenté par un code binaire qui doit être transformé afin que le document puisse être lisible par les humains;

Support : contrairement au document traditionnel dont le contenu est consigné sur un support (papier, etc.) et ne peut en être séparé, le contenu d'un document électronique peut être transféré d'un support à un autre souvent d'un type différent (s'il est récupéré par un autre système, ou si la technologie d'enregistrement devient archaïque); [4]

Structure : la structure d'un document traditionnel fait partie intégrante du document sur papier et elle est évidente à l'utilisateur, la structure matérielle d'un document électronique ne l'est pas et elle dépend du choix de l'auteur du document du système informatique et de l'espace utilisable sur le dispositif de stockage. C'est pourquoi il faudrait construire une structure logique du document permettant l'identification du document et la représentation de chacun de ses éléments constitutifs; [4]

Métadonnées : ce sont des données sur les données, c'est un concept essentiel pour les documents électroniques puisque leur compréhension et leur évidence en tant que preuves

dépendent entre autres de ces métadonnées sur le contexte (opérationnel et administratif) et la structure des documents;

Identification : contrairement aux documents traditionnels, un document électronique n'est pas une entité matérielle, il est plutôt une entité logique qui est le résultat d'une activité ou d'une opération et qui en prouve l'existence. Ces documents électroniques peuvent avoir des contreparties sur papier (lettres, contrats, etc). Comme ils peuvent ne pas en avoir du tout (documents en protocole HyperText, systèmes multimédias, etc) [4].

Conservation : contrairement à la conservation des documents traditionnels qui ne nécessite que l'établissement des bonnes conditions pour éviter les dommages. La conservation des documents électroniques nécessite un entretien régulier qui consiste à transférer les documents sur d'autres supports pour assurer la pérennité de lecture avec les équipements en usage, vu l'évolution rapide des technologies et des systèmes informatiques [5].

3.4 Gérer un document en dix étapes

Pour la plupart des collaborateurs, gérer un document numérique c'est simplement:

- Ouvrir un outil de traitement de texte,
- Saisir et une fois le travail terminé,
- Enregistrer le fichier quelque part,
- Puis éventuellement le diffuser par messagerie ou via papier. [1]

C'est une vision restrictive lorsqu'il s'agit de valoriser et de pérenniser les informations pour l'entreprise. Loin de se limiter à ces quelques actions, gérer un document implique dix fonctions tout au long du cycle de vie d'un document:

- Rédiger, valider, formater et publier, stocker, classer, diffuser, rechercher, restituer/imprimer, réviser, archiver.[1]

Le document passe aussi par divers états qu'il faut pouvoir gérer:

- Brouillon ou Draft lorsque le document est en cours d'élaboration par l'auteur.
- Terminé lorsque le document satisfait l'auteur et est prêt à être diffusé.
- Vérifié lorsque le document est vérifié quant à sa qualité, sa conformité aux règles de présentation et sa cohérence.

- Validé lorsque le document est approuvé par une fonction ou un service autorisé à diffuser le document.[1]
- Diffusé lorsque le document est mis à la disposition des utilisateurs pour application et/ou information.
- Périmé lorsque le document n'est plus adapté et est retiré à ses détenteurs.
- Archivé lorsque le document n'est plus consulté régulièrement mais qu'une trace de son existence demeure pour une durée définie.
- Détruit lorsque le document n'est pas archivé ou que le délai d'archivage est écoulé la maîtrise du document passe ainsi par plusieurs étapes.

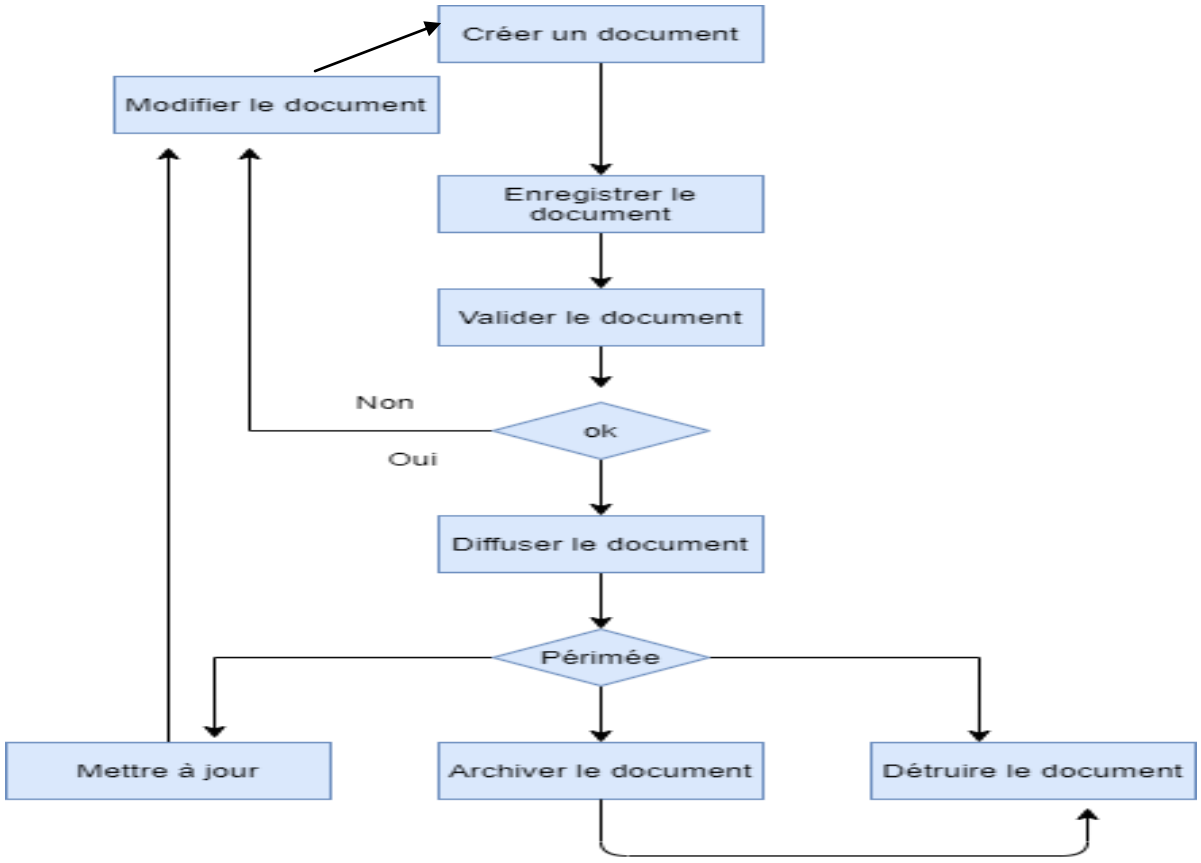


Figure 1 : Modélisation de la maitrise des documents

Ce schéma représente une modélisation de la maitrise des documents, tout d'abord on crée le document, on l'enregistre et puis on le valide. Si la validation est effectuée on diffuse le document, sinon il passe à la modification. Le document diffusé, s'il est périmé, soit on le détruit directement ou bien l'archiver et le détruire, sinon le mettre à jour et il va passer à la modification (Voir la figure 1).

3.5 Le cycle de vie du document numérique

L'Aproged dans son référentiel La maîtrise du cycle de vie du document numérique, définit quatre grandes étapes présentées ci-dessous.[7]

La création

La création du document numérique peut être le résultat d'un traitement automatisé (création directement sous forme numérique), ou le résultat d'une numérisation de documents papiers. Dans ce cas, il est nécessaire d'avoir des consignes pour la création et la mise en forme du document pour pouvoir en garantir l'exploitation ultérieure. [20]

- L'enregistrement. On parle également de copie numérique. Cette phase correspond à la « mémorisation du document pour des utilisations ultérieures (conservation, diffusion, archivage) » ; on peut également inclure un système de workflow lors de l'enregistrement.

– Le classement .Il est nécessaire de ranger le document dans un espace informatique (serveur, …) accessible aux utilisateurs. L'organisation du classement doit être compatible avec le plan de classement. [20]

- L'indexation. On détermine alors les termes et les expressions clés pour pouvoir retrouver le document dans le système de classement par la suite. [20]

La gestion

Concerne les opérations qui interviennent sur le document après sa création. On parle souvent de sécurité et de droits d'accès (cela peut passer par des opérations de cryptage, de restriction d'actions sur le contenu ou d'occultation de champs). Il s'agit de rendre le document accessible aux personnes autorisées. Le document numérique étant facilement

reproductible et modifiable, il est également nécessaire de pouvoir gérer les différentes versions de ce document.[7]

La diffusion

On distingue deux techniques de restitution du document :

- le mode push : c'est la mise à disposition des documents que l'utilisateur va chercher dans la base. Il doit alors se connecter au système de GED. Il lui est possible de visualiser les documents après une recherche et une sélection (si celui-ci est autorisé à accéder au document).[20]
- le mode pull : c'est la distribution du document. Le système transfère automatiquement les documents (souvent par la messagerie électronique) à des destinataires qui sont désignés préalablement. Il faut alors bien gérer les listes de diffusion (changement d'adresses électroniques, départ de l'entreprise, …) pour que les bonnes personnes puissent avoir les bons documents. [20]

La conservation

L'objectif de la conservation des documents est de prouver, de mémoriser, de comprendre et de communiquer. Il faut donc conserver dans le temps la lisibilité des documents numériques et de ses composants. Cela implique un choix de formats judicieux. [7]

3.6 L'acquisition des documents numériques

L'acquisition numérique

L'acquisition numérique pour que l'information puisse être gérée par un ordinateur, elle doit être disponible sous forme numérique. Il existe trois modes d'acquisition :

- **l'acquisition directe sous forme numérique,** que ce soit un texte saisi sur un logiciel de traitement de texte ou une photo créée avec un appareil numérique.
- **La collecte et l'assemblage de documents déjà numériques**, Dans ce cas, les documents sont situés sur différents postes ou serveurs. Il suffit alors de les rassembler, les indexer et les convertir en un format unique.

- **La conservation numérique de documents analogiques**, Il existe plusieurs technologies pour numériser les documents (les scanners, les cartes de numérisation, …) [7]

La numérisation des documents

« La numérisation permet de passer d'une représentation analogique de la réalité à une représentation numérique par échantillonnage. » La numérisation (ou digitalisation en anglais) est la conversion d'un objet réel (image, texte, …) en une suite de nombres permettant de représenter cet objet en informatique ou en électronique numérique.

Le poids du fichier va dépendre de la fréquence d'échantillonnage et de l'amplitude de la quantification. C'est pourquoi il est important de bien connaître ses besoins et de choisir la technologie adaptée aux types de documents (différents selon qu'on ait des documents textes, images ou vidéos, etc.). [7]

Bien choisir son format lors de la mise en place d'une solution de GED, le choix du format d'enregistrement des fichiers doit se faire en fonction des besoins et des usages répertoriés au sein de l'entreprise :

- modification/réutilisation des documents
- nécessité d'une gestion des versions de documents
- modalités de création ou d'acquisition
- pérennité dans l'accès aux documents
- interopérabilité entre les plates-formes
- assemblage de fragments divers au sein d'un même document
- intégration de documents multimédia : comprennent des textes, des images fixes ou animées

On remarque une coexistence de nombreux formats incompatibles. On peut distinguer des formats propriétaires, des normes et des standards.

4- Conclusion

La GED permet de localiser rapidement l'information, en quelques clics. Le document est facilement accessible. Il peut être partagé par plusieurs personnes au même moment. La GED garantit également la sécurité des données et crée une dynamique de travail collaboratif.

Chapitre 2 :

La cryptographie des documents

1- Introduction

La cryptographie est par définition l'art de cacher l'information. Elle désigne l'ensemble des techniques qui permettent de chiffrer les messages. Son objectif principal est de permettre à deux personnes de communiquer à travers un canal peu sûr de telle sorte qu'un opposant ne puisse pas comprendre ce qui est échangé. La cryptographie a toujours eu une grande importance dans l'histoire. Actuellement les réseaux informatiques exigent son utilisation pour assurer la confidentialité des données transmises notamment dans la téléphonie mobile, le paiement bancaire, les pièces d'identité, la télésanté, etc.

2- Histoire de la cryptologie

Les origines de la cryptographie remontent à plus de 4000 ans, avec la découverte d'une tombe égyptienne à Saqqarah où reposait un haut responsable de la Ve dynastie des pharaons. Les écrits retrouvés sur les parois du sarcophage contenaient des hiéroglyphes modifiés. Ces nouveaux symboles représentent le premier élément essentiel de la cryptographie : une modification volontaire de l'écriture. Les découvertes archéologiques égyptiennes montrent ainsi que la cryptographie, et plus précisément la transmission sûre d'informations, sont aussi anciennes que l'invention de l'écriture elle-même.[8]

Figure 2 : Exemple d'un Scytale[i]

Le premier exemple de cryptographie a été conçu durant l'Antiquité, entre le Xe et le VIIe siècle av. J.-C., avec une technique de chiffrement par transposition utilisée par les Spartiates et les Athéniens pendant la guerre du Péloponnèse. Ce chiffrement consiste à réorganiser les caractères d'un message. Au moyen de deux bâtons identiques (appelés Scytales, voir Figure 2) partagés par l'expéditeur et le destinataire, un message écrit sur une bandelette enroulée sur ces bâtons n'aurait plus aucune signification une fois la bandelette déroulée. Par la suite les

systèmes de chiffrements deviennent de plus en plus compliqués jusqu'à l'invention des machines qui encodent. Ces dernières sont destinées à transmettre des messages d'un point à un autre sur de grandes distances, à l'aide de codes secrets pour une transmission rapide et fiable. On peut par exemple citer la création par Edison du télégraphe utilisant le code Morse au XIXe siècle ou encore les machines Enigma (voir Figure 3) de Sherbius dont les nazis se servaient pendant la Seconde Guerre mondiale.[8]

Figure3 : Machine Enigma[ii]

Figure4 : Pierre de Rosette[iii]

3- Définition de la cryptographie

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.[9]

La cryptologie est essentiellement basée sur l'arithmétique. Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis de faire des calculs sur ces chiffres pour :

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (ciphertext) par opposition au message initial, appelé message en clair (plaintext) ; [9]
- faire en sorte que le destinataire saura les déchiffrer. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement.[9]

La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement. Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, le déchiffrement nécessite quant à lui une clé de déchiffrement. On distingue généralement deux types de clés:

- **Les clés symétriques :** il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète. [9]
- **Les clés asymétriques** : il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement. [9]

On appelle décryptement (le terme de décryptage peut être utilisé également) le fait d'essayer de déchiffrer illégitimement le message (que la clé de déchiffrement soit connue ou non de l'attaquant).[9]

Lorsque la clé de déchiffrement n'est pas connue de l'attaquant on parle alors de cryptanalyse ou crypto analyse (on entend souvent aussi le terme plus familier de cassage)[9]

Cryptanalyse : On appelle cryptanalyse la reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques. Ainsi, tout cryptosystème doit nécessairement être résistant aux méthodes de cryptanalyse.

La cryptologie : est la science qui étudie les aspects scientifiques de ces techniques, c'est-à-dire qu'elle englobe la cryptographie et la cryptanalyse

3.1 Les buts de la sécurité

La cryptographie correspond à l'art du secret, aujourd'hui elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numérique et aux fonctions de hachage. Voici les buts de la cryptographie :

Confidentialité : La notion de confidentialité se définit par le fait qu'une information donnée n'est lisible que par les personnes concernées. Les données confidentielles sont ainsi protégées contre les interceptions sur le médium de communication ou contre la lecture par des personnes non-autorisées.[10]

Intégrité : Outre la confidentialité, un autre aspect très important de la sécurité informatique consiste à assurer l'intégrité des données échangées par les usagers. La notion d'intégrité fait référence à ce que les données d'un échange n'aient pas pu être altérées durant le transfert, soit pour des raisons de qualité de transmission (dans le cas d'une connexion sans-fil distante, par exemple) ou encore par un adversaire dans le cadre d'une attaque de type man-in-the-middle.[10]

Authentification : Le principe de l'authentification est d'assurer que notre interlocuteur (humain ou machine) est bel et bien celui qu'il prétend être. Dans le monde numérique, il s'agit habituellement de s'assurer que celui qui interagit avec le système le fait conformément à la politique de sécurité en vigueur pour un système donné. [10]

Non-répudiation : Le concept de non-répudiation fait référence au fait qu'une personne ne peut nier la modification d'un donnée. [10]

3.2 Les classements de la cryptographie

Pour présenter la cryptographie et ses enjeux actuels, il est souvent bon de rappeler comment tout a commencé afin d'amener petit à petit certains de ces grands principes .

3.2.1 Le chiffrement à clé privée

C'est avec le chiffrement que tout commence : l'idée est de pouvoir rendre inintelligible de l'information (un message, un document, etc.) à une tierce personne indiscrète. Ainsi, un schéma de chiffrement comporte trois éléments :

- **La génération de clés Gen :** elle permet de créer une clé k tirée aléatoirement à partir d'un ensemble donné,[11]
- **Le chiffrement Enc :** chiffre un message m avec une clé k pour produire un chiffré c que l'on note c = Enck(m),[11]
- **Le déchiffrement Dec :** à partir d'un chiffré c et d'une clé k, il permet de récupérer m. Nous avons la relation Deck(Enck(m)) = m.[11]

Ainsi pour communiquer secrètement, deux personnes doivent préalablement avoir généré puis partagé une même clé privée k. Alors, l'utilisation des algorithmes de chiffrement et de déchiffrement leur assurera une correspondance confidentielle du moment que personne

n’entre en possession de la clé k. En possession de k, Dounia peut utiliser Enck(m) pour produire un chiffré c qu’elle communiquera à Nawal. À son tour, il utilisera cette même clé k avec Deck(c) afin de récupérer le message initial m. Cela introduit la première application toute naturelle du chiffrement, illustrée dans la figure5.[11]

Une deuxième utilisation évidente du chiffrement consiste à garder pour soi la clé k et consigner des documents secrets (un journal intime, le plan d’une carte au trésor, d’une invention, etc.) si l’on n’a pas la garantie que le support de l’information ne tombe pas en de mauvaises mains.[11]

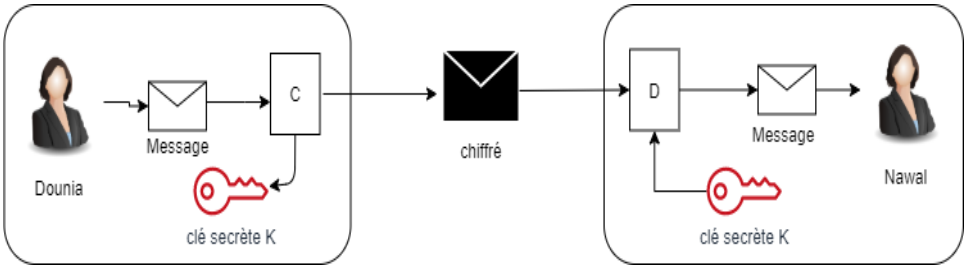


Figure 5 **:** Le chiffrement symétrique.

3.2.2 Cryptographie classique

La cryptographie classique décrit une période antérieure aux ordinateurs, où les principaux outils utilisés consistaient à remplacer des caractères par d'autres et à les transposer dans des séquences différentes tout en gardant secrètes les procédures de cryptage ou de décryptage. Sans cela, le système est complètement inefficace car n'importe qui peut déchiffrer le message chiffré[12]. Cette classe de méthodes regroupe deux types de cryptographie :

3.2.2.1 Cryptographie par transposition : On distingue la transposition simple par colonne et la transposition complexe par colonne.

3.2.2.2 Cryptographie par substitution : Ce mode de cryptage remplace les lettres d'un message texte par d'autres lettres, chiffres ou autres symboles. En raison de la méthode de substitution, les substitutions mono-alphabétiques et poly-alphabétiques sont distinguées.

- **Le chiffrement de César**

Pendant la guerre des Gaules, Jules César envoyait des messages chiffrés à Cicéron qui était resté en poste au Sénat à Rome. L'historien Suétone, archiviste de l'Empereur Hadrien au I-II ème siècle, rapporte dans les «Vies des douzes Césars» que le célèbre Jules avait l'habitude de remplacer chaque lettre par celle située trois places plus loin dans l'alphabet. [13]

Écrivons le message M = lumière, en utilisant l'alphabet occidental contemporain :

A= {a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} On aura :

Message clair : **l u m i e r e**

Message crypté : **O X P L H U H** et l'on dit que ce chiffrement est une substitution mono alphabétique.

Le code de César fut très solide jusque dans les années 800, date où l'islam vivait son âge d'or. De façon étonnante, c'est l'étude des textes du Coran qui développa beaucoup de recherches sur les lettres, le but étant de déterminer si un texte donné avait bien été écrit par la main du prophète. [13]

On découvrit alors l'importance de l'étude des fréquences d'apparition des lettres dans un message, et c'est le «Philosophe des Arabes», Al-Kindi, auteur de 290 livres, qui expliqua la méthode pour décrypter un message obtenu avec un alphabet de substitution. Son «Manuscrit sur le déchiffrement des messages cryptographiques» a été retrouvé en 1987 dans les archives d'Istanbul.[13]

Si l'on sait maintenant que l'étude des fréquences d'apparition des lettres (ou des couples de lettres) dans les messages permet d'initier la cryptanalyse de César, on peut signaler que la découverte d'Al Kindi mit énormément de temps avant d'être connue en Occident. Le livre de Singh explique en détail comment la cryptanalyse des messages entre Marie Stuart et ses partisans a permis l'inculpation puis l'exécution de la reine pour tentative de régicide.[13]

➢ Le chiffrement de Vigénère

Un chiffrement historique un peu plus avancé a été décrit par Blaise de Vigénère, un diplomate, dans son traité des chiffres en 1586. Désormais, la clé n'est plus un seul nombre compris entre 0 et 25 mais un mot de taille arbitraire t où chaque lettre correspond à un décalage. Ainsi, la première lettre de la clé donne le décalage de la première lettre du message, la deuxième lettre donne le décalage de la deuxième lettre et ainsi de suite.[11]

Pour mieux comprendre le fonctionnement du Carré de Vigénère nous vous proposons cet exemple :

Supposons que nous voulons coder le texte « CARRE DE VIGENERE » avec la clé « MALICE ». On commence par écrire la clef sous le texte à coder :

C	A	R	R	E	D	E	V	I	G	E	N	E	R	E
M	A	L	I	C	E	M	A	L	I	C	E	M	A	L

Pour coder la lettre C, la clef est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M. On trouve O. Puis on continue, jusqu'à ce qu'on ait fini de chiffrer notre texte. En chiffrant le texte « Carré de Vigénère », on obtient donc le texte « OAUZG HG VTOGRQRP ». Cet algorithme de cryptographie ainsi que celui de César sont les premiers des algorithmes à clef privée.

3.2.3 Cryptographie moderne

À partir des années 70, on voit apparaître énormément de nouveaux concepts cryptographiques, sans que l'on ait forcément de solution efficace, tels que le chiffrement basé sur l'identité, les calculs multiutilisateurs, les signatures aveugles, les preuves à divulgation nulle de connaissance, les fonctions de hachage et la liste peut être très longue. Pour beaucoup, nous retrouvons ces outils encore maintenant dans des versions actualisées, plus sécurisées, plus efficaces, dont la sécurité est également plus assurée. D'ailleurs, la sécurité d'un schéma cryptographique, son évaluation ainsi que sa compréhension, devient des sous-domaines à part de la discipline. Désormais, la cryptographie est vouée à être utilisée au travers de l'informatique et la sécurité s'exprime en fonction des capacités des ordinateurs contemporains.[11]

La cryptographie moderne est divisée en deux parties distinctes :

- La cryptographie à clé secrète, ou encore appelée symétrique.
- La cryptographie à clé publique, dite également asymétrique.
- Les fonctions de hachage.

3.2.3.1 Chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement.[9]

Le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles. Ainsi, le moindre algorithme (tel qu'un OU exclusif) peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas).[9]

Toutefois, dans les années 1940, Claude Shannon démontra que pour être totalement sûr, les systèmes à clés privées doivent utiliser des clés d'une longueur au moins égale à celle du message à chiffrer. [9]

De plus, le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.[9]

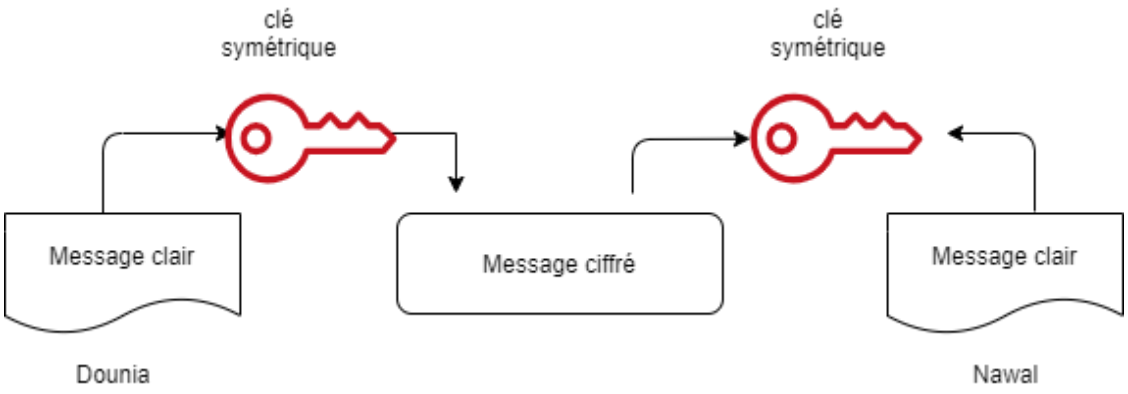


Figure 6 **:** chiffrement symétrique.

Le principal inconvénient d'un cryptosystème à clé secrète (appelé aussi cryptosystème symétrique) provient de l'échange des clés. En effet, le chiffrement symétrique repose sur l'échange d'un secret (les clés) et pose le problème de la distribution des clés. [9]

D'autre part, un utilisateur souhaitant communiquer avec plusieurs personnes en assurant de niveaux de confidentialité distincts doit utiliser autant de clés privées qu'il a d'interlocuteurs. Pour un groupe de N personnes utilisant un cryptosystème à clés secrètes, il est nécessaire de distribuer un nombre de clés égal à N * (N-1) / 2.[9]

Ainsi, dans les années 1920, Gilbert Vernam et Joseph Mauborgne mirent au point la méthode du One Time Pad (méthode du masque jetable, parfois appelée One Time Password, OTP), basée sur une clé privée, générée aléatoirement, utilisée une et une seule fois, puis

détruite. À cette même époque par exemple, le Kremlin et la Maison Blanche étaient reliés par le fameux téléphone rouge, c'est-à-dire un téléphone dont les communications étaient cryptées grâce à une clé privée selon la méthode du masque jetable. La clé privée était alors échangée grâce à la valise diplomatique (jouant le rôle de canal sécurisé). [9]

Nous pouvons citer l'algorithme DES comme un exemple de chiffrement symétrique moderne,

- **Algorithme Data Encryption Standard (DES)**

Principe du DES

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de « 1 » dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme. [9]

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit. La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16. Étant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7,2 × 1016) clés différentes ! [9]

Algorithme du DES

Les grandes lignes de l'algorithme sont les suivantes[9] :

➤ Fractionnement du texte en blocs de 64 bits (8 octets).

➤ Permutation initiale des blocs.

➤ Découpage des blocs en deux parties : gauche et droite, nommées G et D.

➤ Étapes de permutation et de substitution répétées 16 fois (appelées rondes).

➤ Recollement des parties gauche et droite puis permutation initiale inverse.

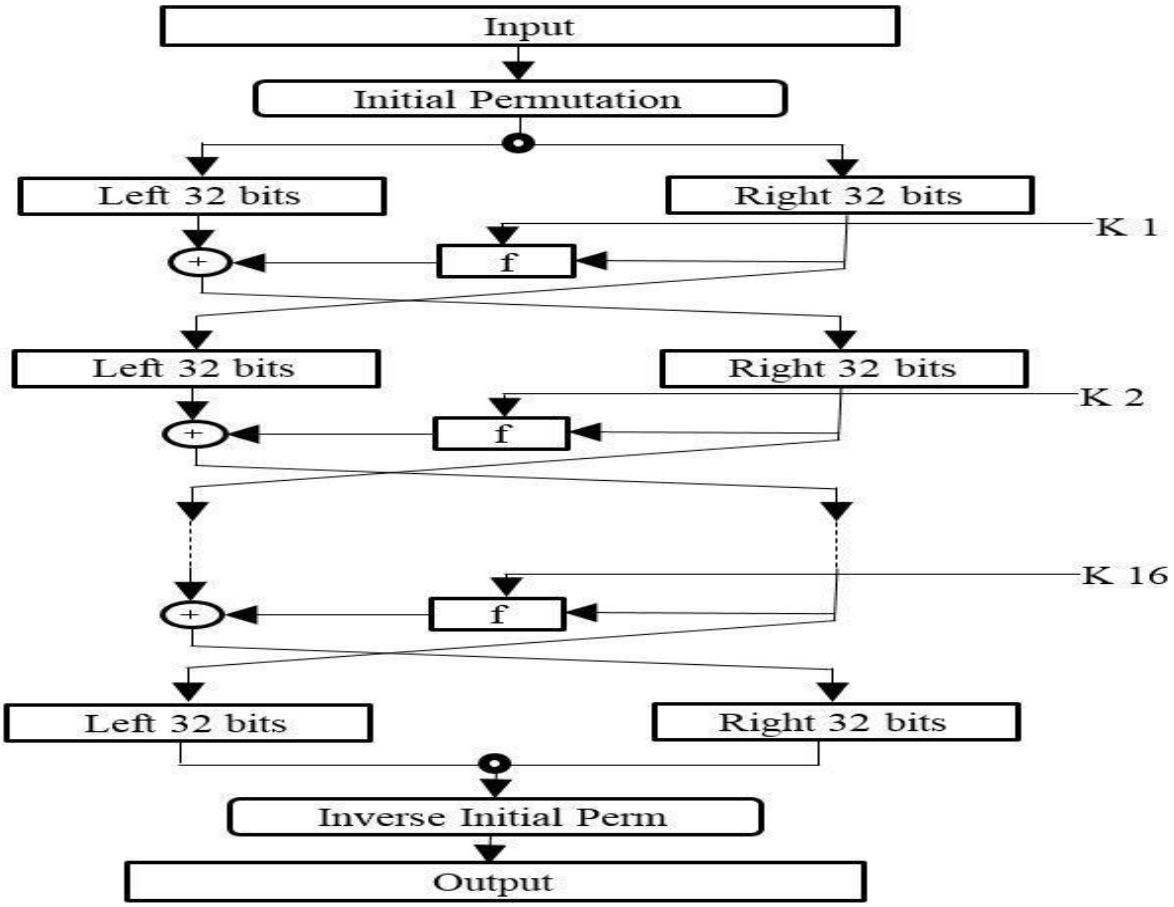


Figure 7 : Algorithme DES[iv].

Génération de clés

Étant donné que l'algorithme du DES présenté ci-dessus est public, toute la sécurité repose sur la complexité des clés de chiffrement. L'algorithme ci-dessous montre comment obtenir à partir d'une clé de 64 bits (composé de 64 caractères alphanumériques quelconques) 8 clés diversifiées de 48 bits chacune servant dans l'algorithme du DES[9]

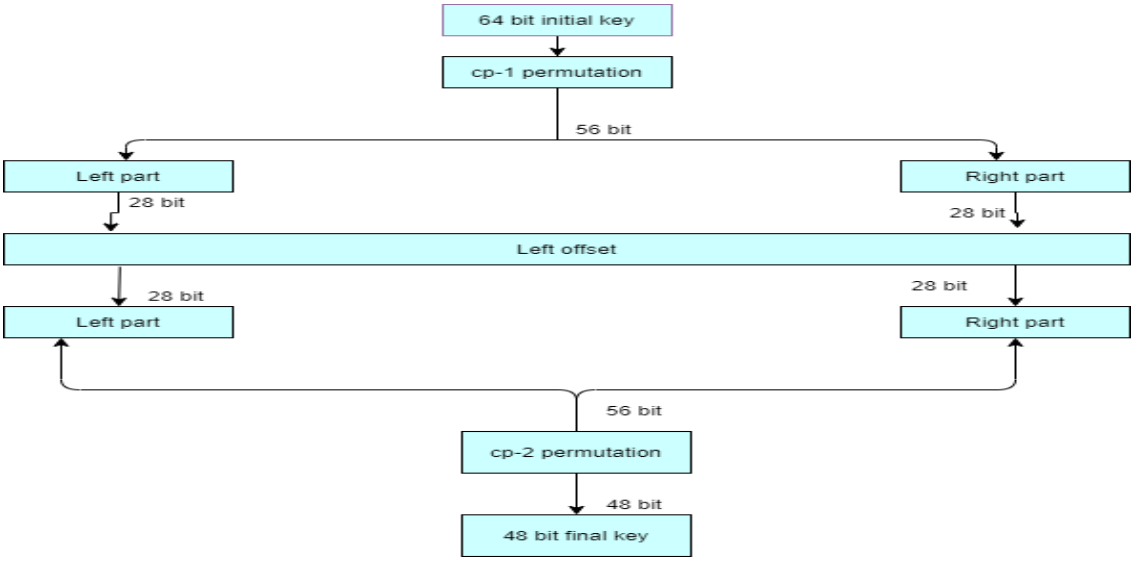


Figure 8 : Génération de clé.

➢ Advanced Encryption Standard (AES)

Le chiffrement AES est le standard actuel en termes de cryptographie. Il est pour le moment indéchiffrable à moins d'utiliser une méthode de force brute. Une clé de 128 bits est utilisée pour la version standard d'AES. Initialement, le chiffrement de Rijndael (gagnant du concours AES) prévoyait en plus des chiffrements par clés de 192 et 256 bits. Les tailles de clés différentes ne changent pas le fonctionnement de l'algorithme. La seule différence se trouve dans le nombre de fois que les quatre opérations de la deuxième phase sont réalisées. Le Tableau 10 indique le nombre d'itérations (Nr) effectuées. Ce nombre dépend du nombre de colonnes que contient la matrice contenant la clé (Nk) ainsi que de son nombre de lignes (Nb). Ainsi, dans AES 128 bits, le nombre de tours de boucle sera égal à Nr - 1. Son fonctionnement se déroule en plusieurs étapes (généralement appelés « rounds »).[14]

	NK	Nb	Nr
128	4	4	10
192	6	4	12
256	8	4	14

Tableau1 : Tableau du nombre d'itérations par rapport à la clé.

3.2.3.2 Chiffrement asymétrique

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman. Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :

➤ Une clé publique pour le chiffrement ;

➤ Une clé secrète pour le déchiffrement.

Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). À partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé. Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire LDAP). Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).[9]

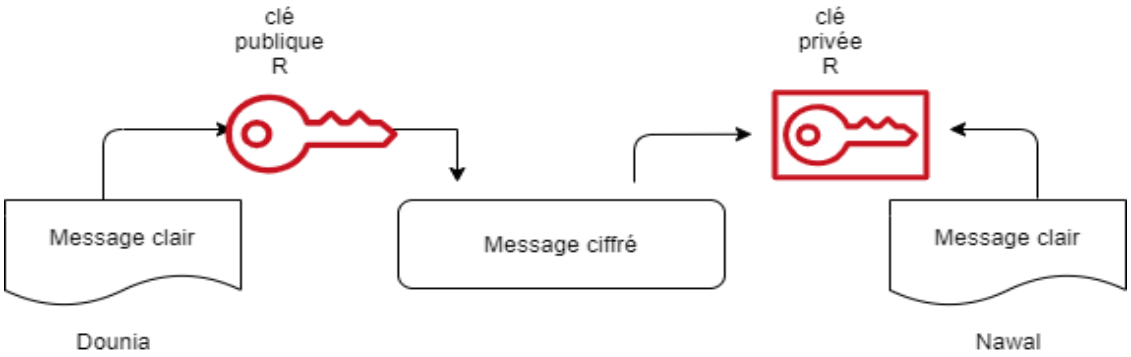


Figure10 : chiffrement Asymétrique.

Ce système est basé sur une fonction facile à calculer dans un sens (appelée fonction à trappe à sens unique ou one-way trapdoor function) et mathématiquement très difficile à inverser sans la clé privée (appelée trappe). [9]

À titre d'image, il s'agit pour un utilisateur de créer aléatoirement une petite clé en métal (la clé privée), puis de fabriquer un grand nombre de cadenas (clé publique) qu'il dispose

dans un casier accessible à tous (le casier joue le rôle de canal non sécurisé). Pour lui faire parvenir un document, chaque utilisateur peut prendre un cadenas (ouvert), fermer une valisette contenant le document grâce à ce cadenas, puis envoyer la valisette au propriétaire de la clé publique (le propriétaire du cadenas). Seul le propriétaire sera alors en mesure d'ouvrir la valisette avec sa clé privée. [9]

➢ Le chiffrement RSA

Le chiffrement RSA a été inventé en 1977 par les mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman. Les initiales de leur nom ont donné RSA. Même si l'idée de base est la même que celle de Diffie-Hellman, (échanger une clé avec un grand nombre de personnes), son fonctionnement est différent bien qu'il soit basé sur la difficulté à factoriser de très grands nombres premiers. Il est massivement utilisé à travers le monde. Avec tous les utilisateurs du réseau Internet, il serait inimaginable d'utiliser un chiffrement symétrique. C'est pour cette raison que la clé privée est calculée avec RSA. Comme les algorithmes asymétriques sont plus lents que les symétriques, RSA ne calcule que la clé qui servira à chiffrer les données avec un chiffrement symétrique tel qu'AES. [14]

Pour générer la clé publique qui se compose des nombres n et e, on doit choisir deux très grands nombres premiers distincts p et q d'une taille d'au moins 2512 bits chacun dans le but de former une clé de 1024 bits afin d'être suffisamment sûre. Ensuite, on devra calculer **n** qui est égal à **p * q**. Elle doit, après cela, calculer **φ(n) = (p-1) * (q-1),** qui va permettre de calculer la clé de décryptage d. Ensuite, elle doit choisir un exposant **e** qui est premier avec **φ(n).**[14]

La clé publique va être constituée de **e** et **n**. Ainsi grâce à **e** et **n** on pourra chiffrer un message **m** avec le calcul suivant : **m*e mod n**. Ensuite, pour calculer la clé de décryptage, il faut que **e * d mod φ(n) ≡ 1**. En résumé, pour trouver **d**, il faut faire le calcul suivant : **e -1 mod φ(n).**[14]

➢ Le cryptosystème d'El Gamal

La sécurité d'El Gamal est basée sur la difficulté de problème du logarithme discret et le problème de Diffie-Hellman. Ce système est décrit dans cette section. [15]

1. (pk, sk) ← G (1^{λ}): Générer un grand nombre premier aléatoire p et un générateur α du groupe multiplicatif $(Z)^*_p$ Sélectionner un entier aléatoire a, 1 ≤ a ≤ p − 2, et calculer $(\alpha)^a$mod p. La clé publique est (p, α, α^a) ; et la clé privée est a.

2. c ← Epk (m) : Représenter le message comme un entier m dans l'intervalle [0, p − 1]. Sélectionner un entier aléatoire k où 1 ≤ k ≤ p − 2. Calculer $\gamma = \alpha^k$ mod p et $\delta = m \cdot (\alpha^a)^k$ mod p. Le ciphertext est c = (γ, δ).

3. m ← Dsk(c) : Pour récupérer m en clair à partir de c, calculer le plaintext $m = (\gamma)^{-a} \cdot \delta$ mod p.

4- La signature numérique à paires de clés publique/privée

L'objectif d'une signature numérique est de permettre à un destinataire d'un message de vérifier l'intégrité des données et de contrôler l'identité de leur expéditeur. Cette vérification s'appuie sur la clé publique de l'émetteur du message. [16]

Le tableau recense les principaux algorithmes dédiés à la signature numérique à clé publique.

Algorithme	Description
RSA (Rivest Shamir Adleman), 1978	Conçu par R. Rivest, A. Shamir et L. Adleman, ce système de chiffrement asymétrique par blocs s'appuie sur des clés de longueur variable. La sécurité du schéma repose sur la difficulté de la factorisation en nombres premiers. L'algorithme a été rendu public.
DSA (Digital Signature Algorithm), 1991	Conçu par D. W. Kravitz (NSA), cet algorithme est le standard des applications de signature numérique fédérales. L'algorithme a été rendu public.
GOST (Gosudarstvennyi Standard of Russia Federation), 1994	Conçu par le service de cryptographie russe, cet algorithme est le standard des applications de signature numérique russes. L'algorithme a été rendu public.
ESIGN, 1990	Conçu par A. Fujiaski et T. Okamoto, cet algorithme est le standard des applications de l'opérateur de télécommunications japonais NTT. L'algorithme a été rendu public.

Tableau 2 : Principaux algorithmes de signature numérique à clé publique.

Avant de détailler comment réaliser une signature numérique, rappelons brièvement le fonctionnement des algorithmes de chiffrement à clé publique. Les algorithmes cryptographiques à clés publiques, ou asymétriques, sont les algorithmes les plus utilisés de nos jours pour échanger des clés de chiffrement de session et pour la signature électronique. À l'inverse des algorithmes cryptographiques à clé secrète, ou symétrique, deux clés sont générées pour chaque utilisateur (privée, publique). Ces clés sont calculées à partir de règles précises, fondées sur la théorie des nombres. Nous verrons par la suite un exemple de calcul de bi clé.[16]

La figure 12 illustre la paire de clés publique/privée que possède John.

Figure 12 : Paire de clés publique/privée (bi clé)

La clé publique peut être diffusée alors que la clé privée doit être soigneusement protégée. Si John souhaite envoyer un message à Joe, il chiffre le message avec la clé publique de Joe. De la sorte, seul Joe peut déchiffrer le message qui lui est destiné à l'aide de sa clé privée (voir la figure 13) .[16]

Figure 13 : John envoie un message à Joe.

Si Joe décide d'envoyer un message à John, il chiffre le message avec la clé publique de John, de sorte que seul John puisse le déchiffrer à l'aide de sa clé privée (voir figure 14).

Figure 14 : Joe envoie un message à John.

4.1 Signature numérique

La séquence d'échanges qui suit permet de signer un message à l'aide de l'algorithme RSA :

1. Avec la paire de clés générée (privée/publique), John peut créer une signature électronique de son message certifiant que c'est bien lui qui a créé le message. Pour ce faire, John passe le message à transmettre dans une fonction de hachage afin de créer une empreinte unique du message. [16]

2. John chiffre cette empreinte avec sa clé privée afin d'obtenir la signature électronique de John pour le message à transmettre. La clé privée de John étant unique et non diffusée, il est le seul à pouvoir obtenir cette signature (voir figure 15).

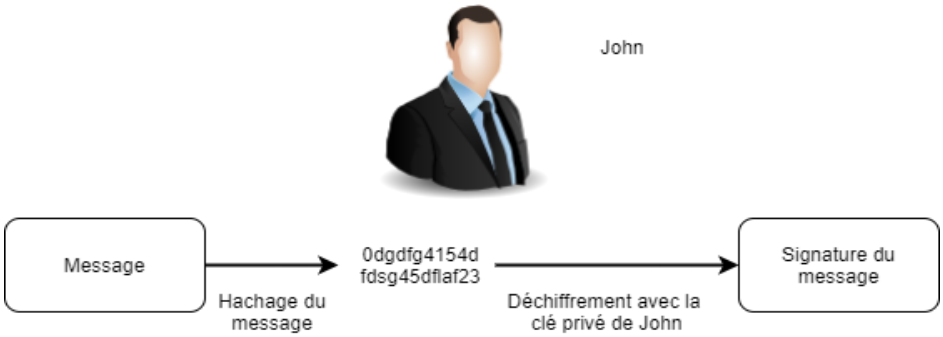


Figure 15 : Signature d'un message par John.

3. Une fois le message signé, John envoie le message et la signature à Joe. John peut aussi chiffrer le message avec la clé publique de Joe afin d'assurer la confidentialité du message (voir figure 16)

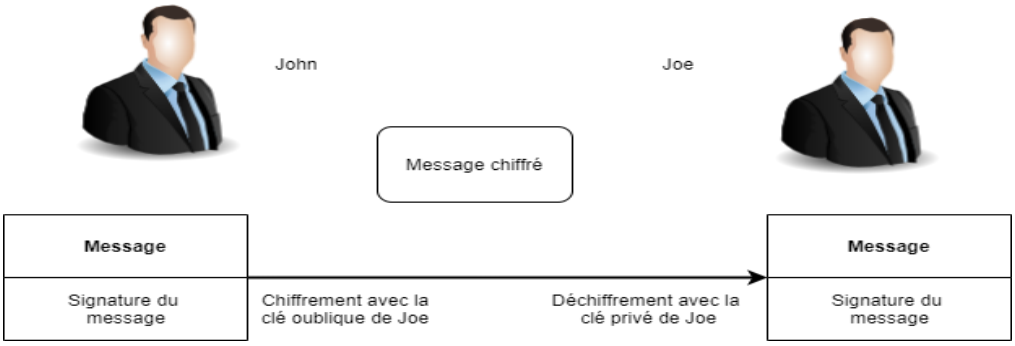


Figure 16 : John envoie un message chiffré et signé à Joe.

4. Pour vérifier la signature électronique de John, Joe fait passer le message reçu dans la même fonction de hachage que John.

5. En parallèle, il déchiffre la signature de John avec la clé publique de John.

6. Les deux actions précédentes lui permettent d'obtenir deux empreintes, celle du message reçu et celle du message envoyé par John. Si les deux empreintes sont égales, c'est le message original écrit par John. Sinon, il y a problème (voir figure 17). La vérification d'une signature peut être réalisée à l'aide d'un programme informatique intégré, par exemple, à un logiciel de messagerie.

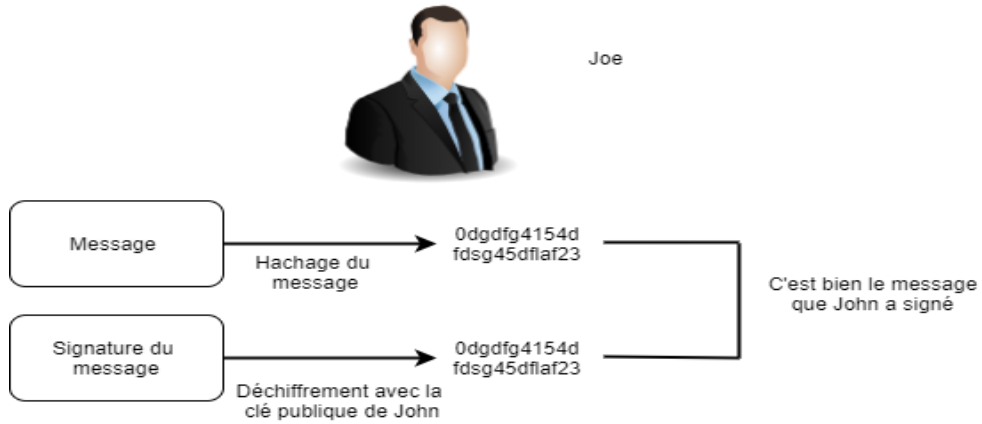
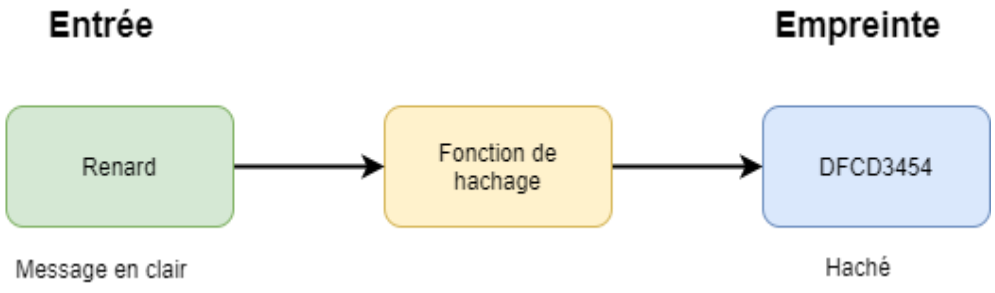


Figure 17 : Joe vérifie le message envoyé par John.

5- Fonction de hachage

Une fonction de hachage (parfois appelée fonction de condensation) est une fonction permettant d'obtenir un condensé (appelé aussi condensat ou haché, message digest) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense.[9]

La fonction de hachage doit être telle qu'elle associe un et un seul hachée à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (one-way function) afin qu'il soit impossible de retrouver le message original à partir du condensé. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dit « à brèche secrète ».[9]



Message en clair Haché

Figure 18 : fonction de hachage.

Ainsi, le haché représente en quelque sorte l'empreinte digitale (finger print) du document.[9]

Les algorithmes de hachage les plus utilisés actuellement sont:

- **MD5 (MD signifiant Message Digest)**

Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier) ;

- **SHA (Secure Hash Algorithm, pouvant être traduit par algorithme de hachage sécurisé)**

Crée des empreintes d'une longueur de 160 bits. SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 264 bits en le traitant par blocs de 512 bits.

Le SHA-1 est dit sûr parce qu'il est infaisable, d'un point de vue informatique, de trouver un message qui correspond à un condensé de message donné, ou de trouver deux messages différents qui produisent le même condensé de message. Toute modification apportée à un message en transit entraînera, avec une très forte probabilité, un condensé de message différent et la vérification de la signature échouera.[17]

SHA-1 est utilisé pour calculer un résumé de message pour un message ou un fichier de données fourni en entrée. Le message ou le fichier de données doit être considéré comme une chaîne de bits. La longueur du message est le nombre de bits du message (le message vide a une longueur de 0). Si le nombre de bits dans un message est un multiple de 8, pour des raisons de compacité, nous pouvons représenter le message en hexadécimal. Le but du remplissage du message est de faire en sorte que la longueur totale d'un message rempli soit un multiple de 512. SHA-1 traite séquentiellement des blocs de 512 bits lors du calcul du résumé du message. Le texte suivant spécifie la manière dont le remplissage doit être effectué. En résumé, un "1" suivi de un "0" suivis d'un nombre entier de 64 bits est ajouté à la fin du message afin de produire un message de longueur 512 * n. Le nombre entier de 64 bits est la longueur du message original. Le message rembourré est ensuite traité par le SHA-1 sous forme de n blocs de 512 bits.[17]

6- Les certificats

Les algorithmes du chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique. Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP) ou bien d'un site web.[18]

Toutefois ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée. En effet un pirate peut corrompre la clé publique présente dans l'annuaire en le remplaçant par sa clé publique.[18]

Ainsi, le pirate sera en mesure de déchiffrer tous les messages qui auront été chiffrés avec la clé présente dans l'annuaire.[18]

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA, Certification Authority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).[18]

6.1 La structure d'un certificat

Les certificats sont des petits fichiers divisés en deux parties :

➢ La partie contenant les informations.

➢ La partie contenant la signature de l'autorité de certification.

La structure des certificats est normalisée[18] par le standard X.509 de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

➢ La version de X.509 à laquelle le certificat correspond.

➢ Le numéro de série du certificat.

➢ L'algorithme de chiffrement utilisé pour signer le certificat.

➢ Le nom (DN, Distinguished Name) de l'autorité de certification émettrice.

➢ La date de début de validité du certificat.

➢ La date de fin de validité du certificat.

➢ L'objet de l'utilisation de la clé publique.

➢ La clé publique du propriétaire du certificat.

➢ La signature de l'émetteur du certificat (thumbprint).

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification ; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de **l'autorité de certification**.[18]

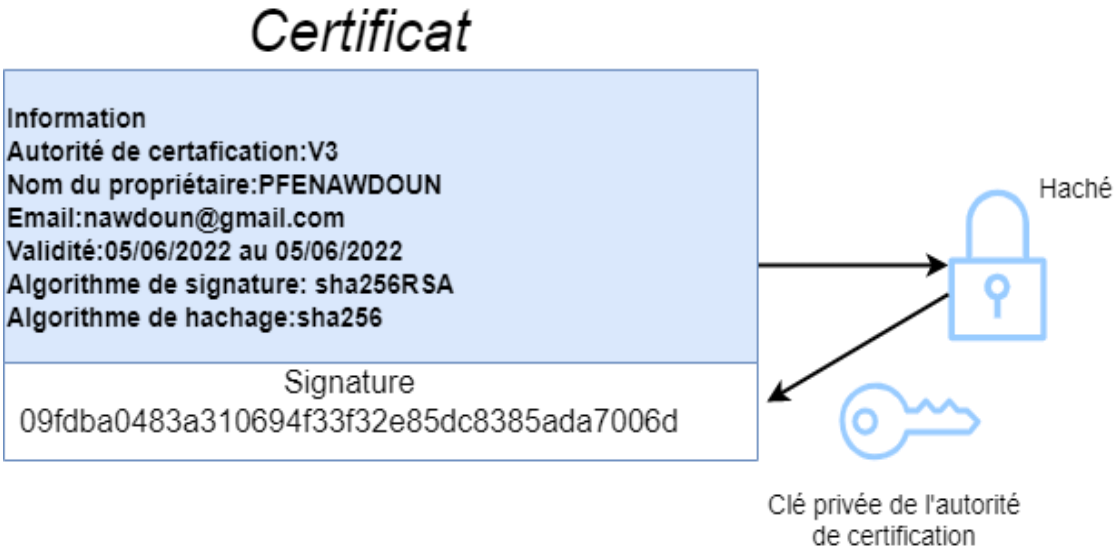


Figure 19 : Le certificat du destinataire.

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.

Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification.

Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.[18]

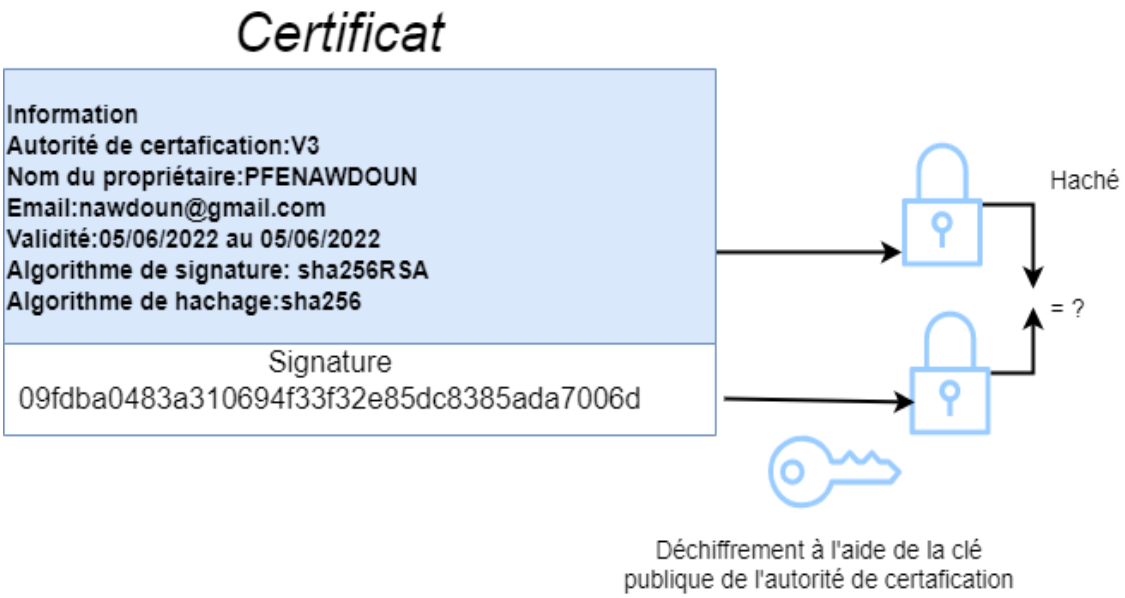


Figure 20 : Déchiffrement à l'aide de la clé publique de l'autorité de certification.

6.2 Niveau de signature

On distingue différents types de certificats selon le niveau de signature :

➢**Les certificats auto signés** sont des certificats à usage interne, signé par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto signés.[18]

➢**Les certificats signés par un organisme de certification** sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.[18]

6.3 Types d'usages

Les certificats servent principalement dans trois types de contextes :

➢**Le certificat client**, stocké sur le poste de travail de l'utilisateur ou embarqué dans un conteneur tel qu'une carte à puce, permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte

d’identité numérique utilisant une paire de clés asymétriques d’une longueur de 512 à 1 024 bits.[18]

➢**Le certificat serveur** installé sur un serveur web permet d’assurer le lien entre le service et le propriétaire du service. Dans le cas d’un site web, il permet de garantir que l’adresse (URL) et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL.[18]

➢**Le certificat VPN** est un type de certificat installé dans les équipements réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d’une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IPSec). [18]

7- Conclusion

La cryptographie a défini les notions de sécurité et prouvé la sécurité de cryptosystèmes de chiffrement, de codes d’authentification de message et de signature numériques. De plus, des protocoles de plus haut niveau, comme des systèmes de communications sécurisées ou de votes électroniques, ont été conçus.

Chapitre 3 :

Analyse et Conception du Système.

1- Introduction

Un projet, au sens commun du terme, est un ensemble d'activités et d'actions coordonnées, qui mobilisent des ressources dans un intervalle de temps précis, avec un début et une fin, afin de répondre à un besoin clairement identifié. L'analyse et la conception sont des parties primordiales dans le cycle de vie d'un projet. Le langage de modélisation UML est celui qui a été choisi en raison de la place prépondérante qu'elle occupe dans le génie logiciel. En effet, UML est le langage consensuel qui est adopté dans la plupart des projets de construction de système logiciel. C'est une notation graphique destinée à la création de modèles orientés objet en vue de conception et de l'analyse des systèmes.

2- L'étude préliminaire

2.1 Identification des besoins

Dans une plateforme de gestion électronique de documents (GED), des documents sont échangés entre les divers acteurs du système. Une des préoccupations majeures de ces acteurs la « confiance ». Le document a-t-il bien envoyé par la personne mentionnée ? Le document reçu n'a-t-il pas subi des modifications lors sa transmission ? N'a-t-il pas été carrément changé ?

Afin de rassurer les utilisateurs de tels systèmes, des algorithmes de protection et de sécurisation des comptes utilisateurs et des documents échangés sont donc nécessaires. C'est dans cette perspective que s'inscrit le présent sujet.

2.2 Description du travail à réaliser

Le présent projet de Master vise à proposer des algorithmes pour garantir les accès ainsi que l'authentification et l'intégrité des documents dématérialisés échangés entre les différents acteurs de tels systèmes. Le travail consistera en une implémentation de la partie accès et diffusion de documents dans un système de GED, et en implémentation d'algorithmes de signature numérique, s'appuyant sur une technologie cryptographique, qui garantit l'authenticité et l'intégrité des documents dématérialisés, autrement dit des documents numériques.

L'intégrité d'un document numérique permet de garantir que ce fichier n'a pas été falsifié. Pour assurer l'intégrité d'un document électronique il faut prendre en compte la lisibilité de ce dernier, la stabilité informationnelle du contenu et la traçabilité des opérations sur ce document. L'authenticité sera assurée par un cachet numérique qui verrouille et crypte le document et garantit, de fait, son authenticité.

2.3 Recueil des besoins fonctionnels

La capture des besoins fonctionnels est focalisée sur le métier des utilisateurs. Elle qualifie plutôt le risque d'un système inadapté aux utilisateurs. Notre analyse consiste à étudier précisément la spécification fonctionnelle de manière à obtenir une idée de ce que va réaliser notre système en terme de métier. **Modifier la figure carrément**

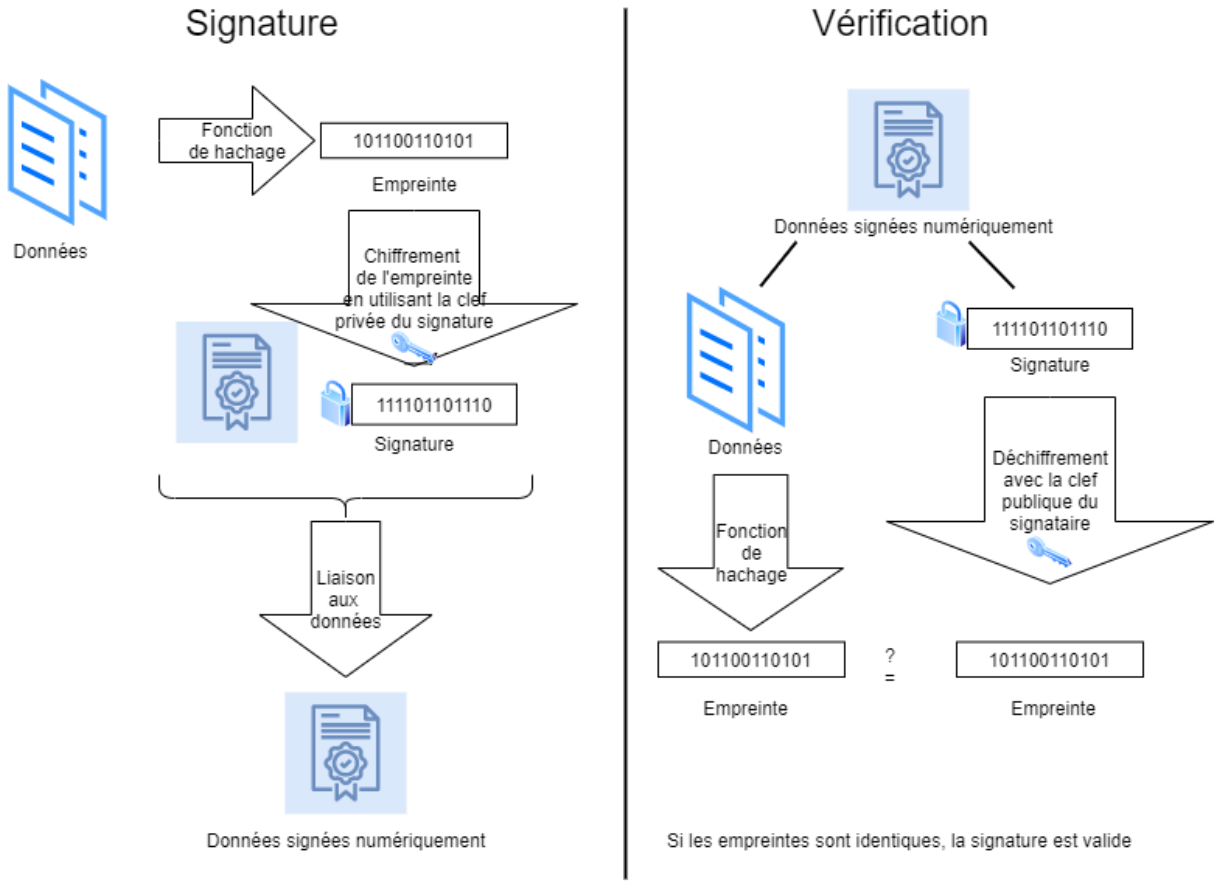


Figure 21 : Mécanisme de la signature à réaliser.

Le processus métier de la signature numérique des documents se résume en deux parties essentielles :

a- Le signataire :

A partir des informations à signer :

- On calcule la valeur du hachage cryptographique des données D ;
- On chiffre cette valeur avec sa propre clé privée, ce qu'implique la signature ;
- On transmet les données, la signature, l'identité du signataire et les deux algorithmes utilisés ;

b- Le récepteur :

- Reçoit les données D et la signature chiffrée SC ;
- Applique le hachage cryptographique à D et trouve le H1 ;
- Récupère la clé publique du signataire à partir de son identité ;
- L'utilise pour déchiffrer la signature reçue SC et trouve H2 ;
- Compare H1 et H2 ;
- La signature valide s'ils sont identiques ;

2.4 Recueil des besoins techniques

La capture des besoins techniques, qui recense toutes les contraintes et les choix dimensionnant la conception du système, les outils et le matériel sélectionné ainsi que la prise en compte des contraintes d'intégration avec l'existant.

Les choix techniques adoptés pour le projet sont comme suit :

- ✓ La modélisation du système avec UML et l'outil StarUML.
- ✓ L'algorithme sha1 pour le hachage.
- ✓ L'algorithme RSA pour le cryptage asymétrique.

2.5 Analyse fonctionnelle et définition des objectifs

La capture des besoins fonctionnels, produit un modèle de besoins focalisé sur le métier des utilisateurs. Cette étape élimine le risque d'avoir un système inadapté aux besoins des utilisateurs.

2.5.1 Identification des cas d'utilisation

2.5.1.1 L'outil StarUML

Pour une présentation des diagrammes UML on a choisi StarUML V3 qui est un logiciel de modélisation UML, qui a été « cédé comme open source » par son éditeur, conçu pour les

développeurs logiciels afin de modéliser des systèmes et de gérer les processus de développement.

2.5.1.2 Diagramme de cas d'utilisation

Le développement d'un nouveau système ou l'amélioration d'un système existant doit répondre à un ou plusieurs besoins. Le maitre d'ouvrage, c'est-à-dire celui qui demande la création du logiciel, n'est généralement pas un informaticien. Il lui faut donc un moyen simple d'exprimer ses besoins. C'est le rôle des diagrammes de cas d'utilisation que de permettre l'expression des besoins de l'utilisateur de façon beaucoup plus facile. Ils permettent de recenser les principales fonctionnalités du système.

Les diagrammes de cas d'utilisation sont composés d'acteurs et de cas d'utilisation. Un acteur est un utilisateur, humain ou non, du système qui est doté d'un nom qui correspond à son rôle. Un cas d'utilisation est une manière spécifique d'utiliser le système. Il permet de décrire ce que le futur système devra faire, sans spécifier comment il le fera.

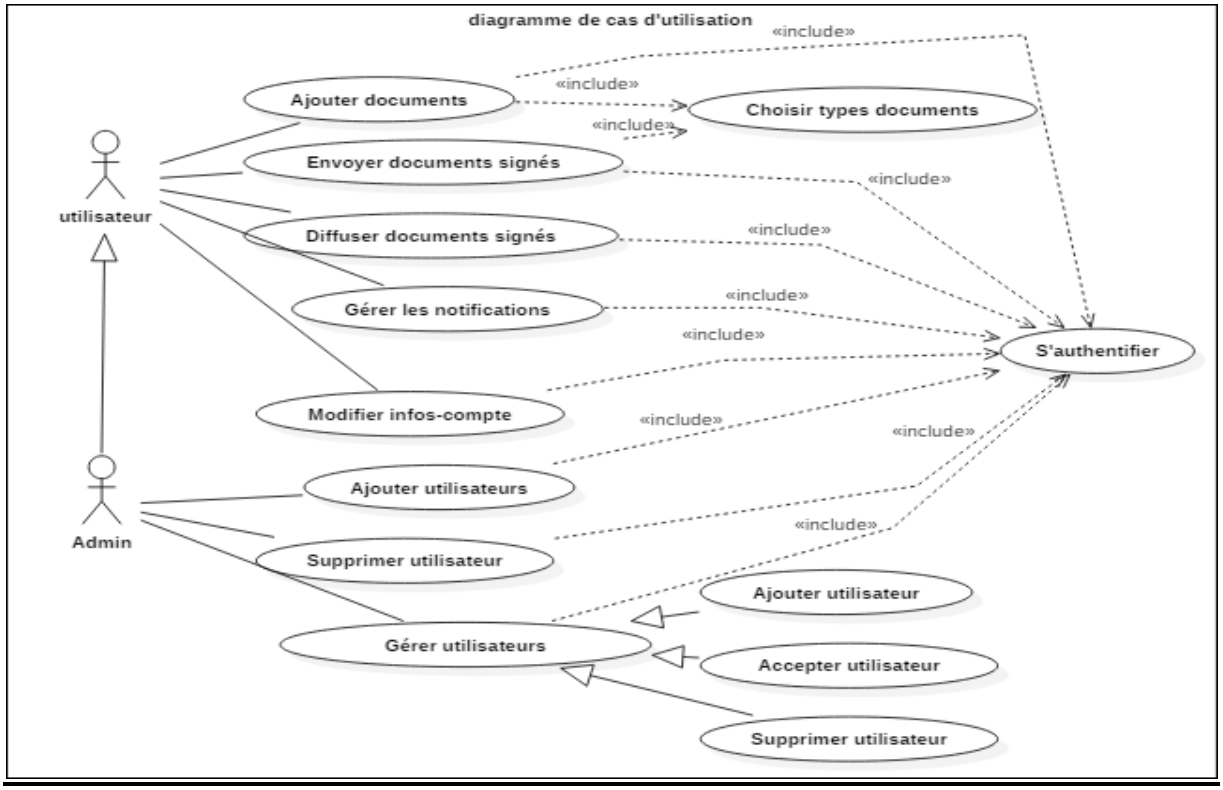


Figure 22 : diagramme de cas d'utilisation.

a) <u>Scénario de cas d'utilisation « Authentification » :</u>

1. L'utilisateur renseigne le login et le mot de passe,
2. Le système vérifie l'identité de l'utilisateur,
3. Le système affiche la page d'accueil.

b) Scénario de cas d'utilisation « Envoyer document signé» :

1. L'utilisateur1 renseigne le login et le mot de passe,
2. Le système vérifie l'identité de l'utilisateur,
3. Le système choisit le document,
4. L'utilisateur1 télécharge un fichier et sa clé privée dans le serveur,
5. Le serveur lit les données, il signe le document,
6. L'utilisateur2 reçoit le document envoyé par l'utilisateur1,
7. Le serveur vérifie la signature, l'utilisateur2 télécharge ou visualise le document reçu.

c) Scénario de cas d'utilisation « Recevoir document signé» :

1. Si, le document envoyé n'a pas subi de modifications lors de l'envoie, l'utilisateur2 le télécharge ou bien le visualise (document sécurisé),
2. Sinon, le document n'est pas sécurisé.

2.6 La conception

2.6.1 Diagramme de classe

Il s'agit d'une vue statique du système, autrement dit, les concepts du domaine qui seront manipulés à l'intérieur du système et leur relations les uns aux autres. Le diagramme de classes est le diagramme le plus important dans une conception orientée objet. Alors que le diagramme de cas d'utilisation montre le système du point de vue des acteurs, le diagramme de classes montre la structure interne.

La figure du diagramme 2 représente le diagramme de classes de l'application, il a été illustré avec StarUML.

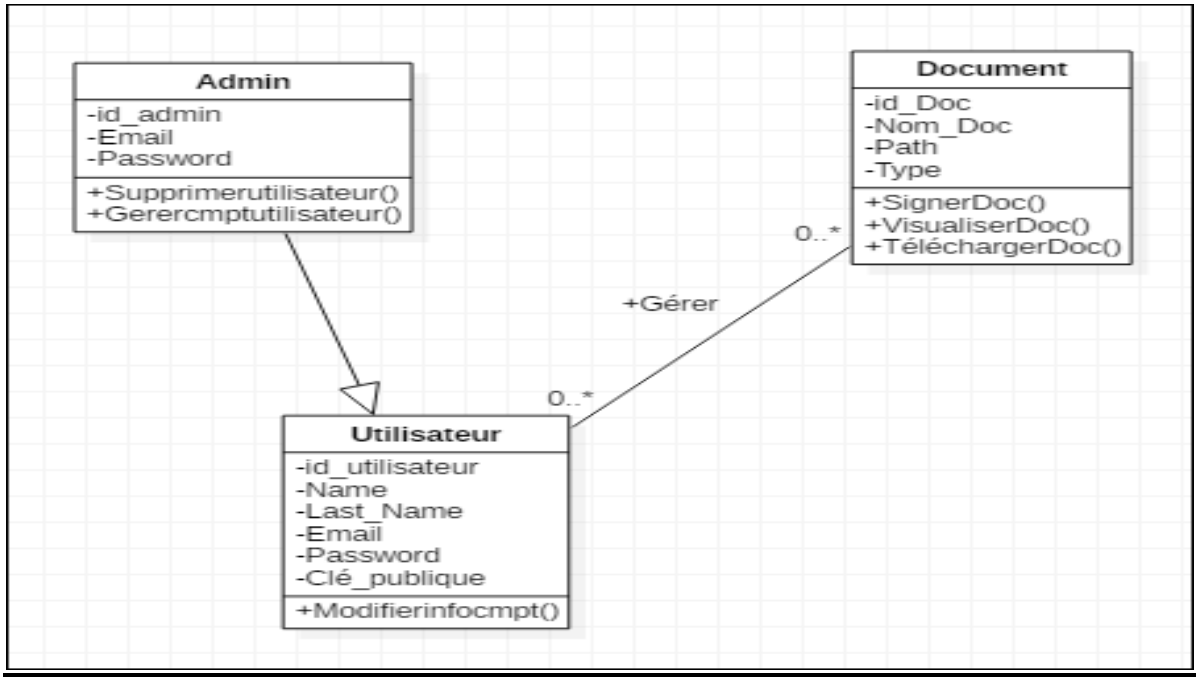


Figure 23 : Diagramme de classe.

2.6.2 Diagramme de séquences

Un diagramme de séquence indique l'interaction entre plusieurs acteurs. Les schémas suivants représentent dans chaque cas les diagrammes de séquences. Ils ont été réalisés par l'outil StarUML.

2.6.2. a Diagramme de séquence du scénario « demande de création du compte utilisateur »

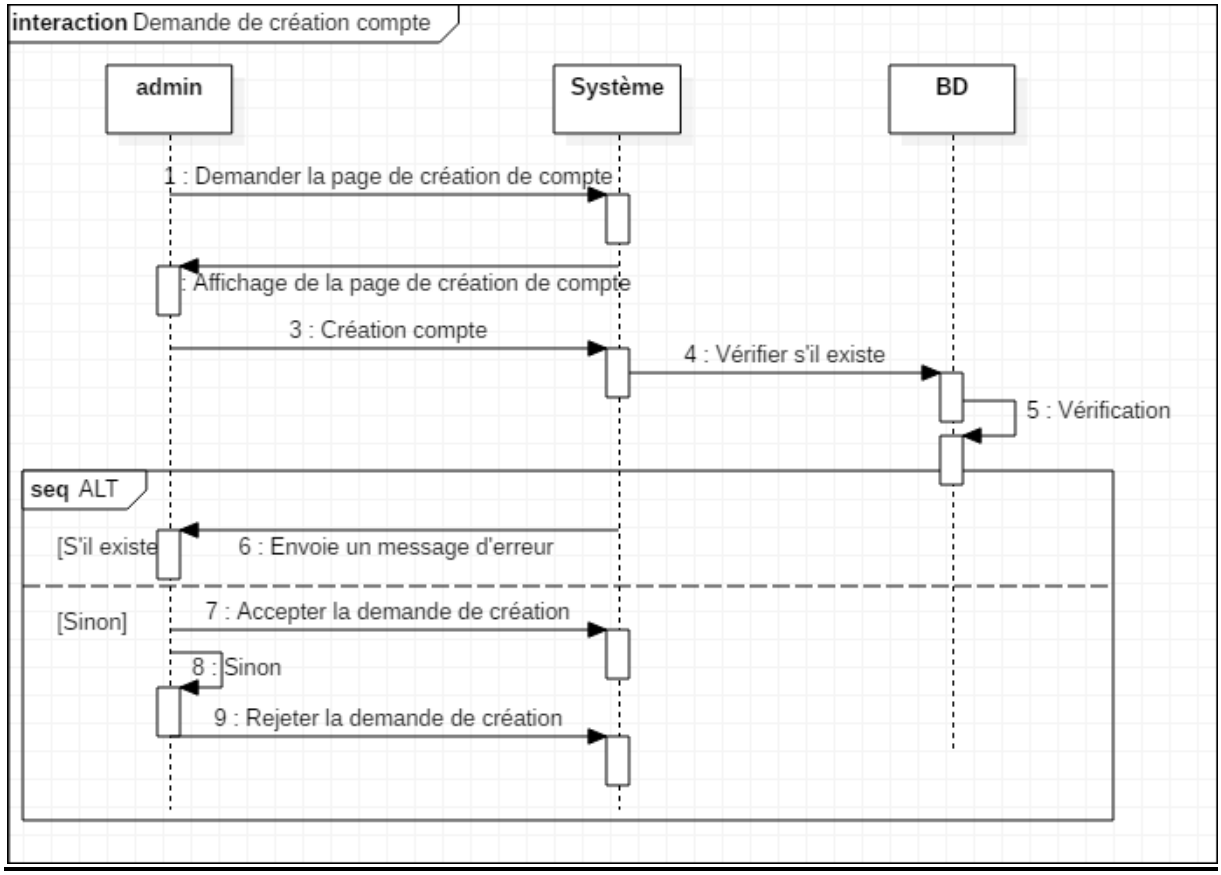


Figure 24 : Diagramme de séquences « Demande de création compte »

2.6.2. b Diagramme de séquence du scénario « Envoyer un document »

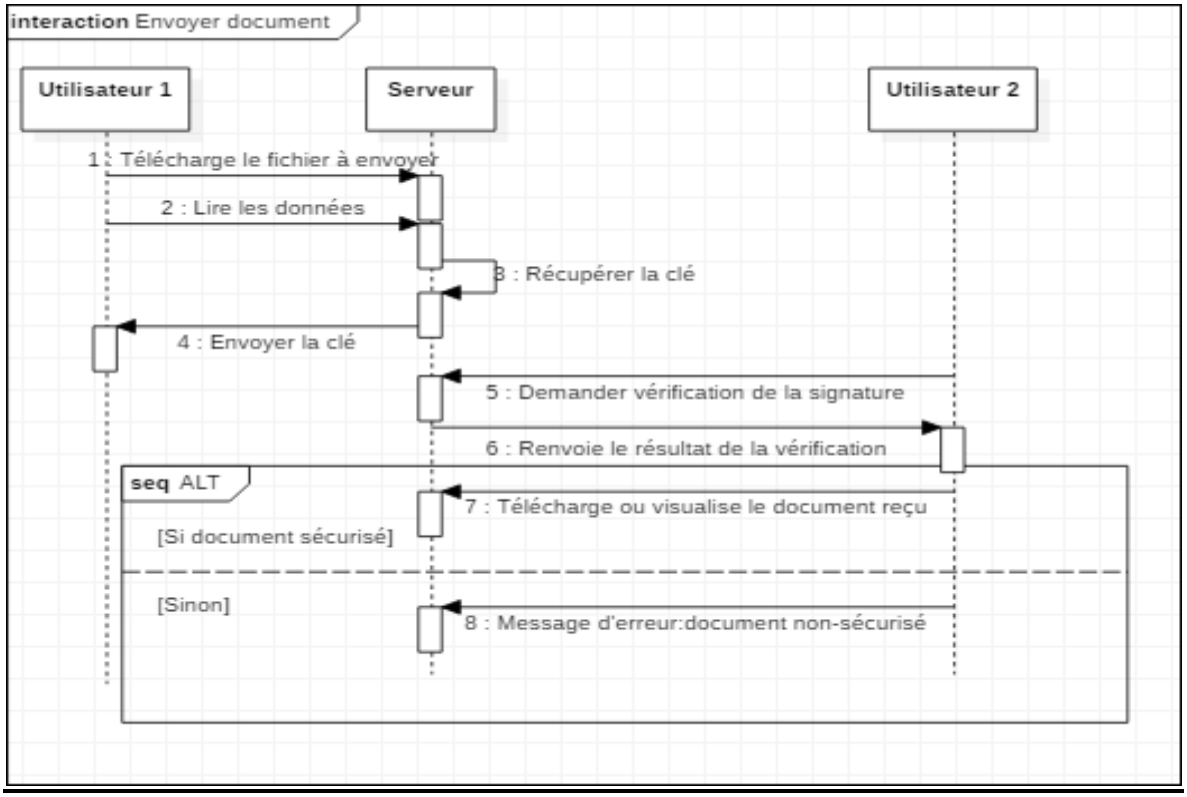


Figure 25 : Diagramme de séquences « Envoyer document »

2.7 Les codes utilisés dans le travail

On a utilisé deux codes dans notre travail, le premier c'est pour crypter et décrypter les informations qui passent entres les pages, et le deuxième c'est pour la signature numérique et sa vérification.

2.7.1 Le code de cryptage/décryptage des informations

Voici le pseudo-code de cryptage des informations :

```
================== Pseudo algorithme encription
================== Input information_pour_cripter Output
informations_cripté Variable Ciphering -> "A....." Option -> 0 Encription_iv -> "13....."
Encription_key -> "nawdo....." Iv_length -> openssl_cipher_iv_length(ciphering) Begin
Encryption -> openssl_encrypt(information.....) Return encryption End
```

Et le pseudo-code de décryptage est :

```
================== Pseudo algorithme encription
================== Input information_pour_cripter Output
informations_cripté Const Ciphering -> "A....." Option -> 0 Encription_iv -> "13....."
Encription_key -> "nawdo....." Begin Iv_length -> openssl_cipher_iv_length(ciphering)
Encryption -> openssl_encrypt(information.....) Return encryption End
```

Ici on a utilisé deux fonctions, fonction de cryptage et de décryptage du passage ou bien l'échange de toutes les informations entre les pages.

2.7.2 Le code de la signature numérique des documents

Le pseudo-code de la signature numérique

```
================== Pseudo algorithme signature ==================
Input data_pour_signer , clé_privée Output signature_detaché Variable Binary_signature
Begin Binary_signature -> openssl_sign(data_pour_signer,binary_signature,clé_privée)
Return binary_signature End
```

Le pseudo-code de la vérification de la signature numérique

```
================== Pseudo algorithme vérification
==================== Input data_pour_verifier, signature_detaché, clé_public
Output Boolean Variable ok Begin Ok-> openssl_verify(data_pour_verifier,
signature_detaché, clé_public) If ok == 1: Return true Else: Return false End
```

Pour créer cette signature numérique, on a d'abord obtenu un certificat de signature qui prouve l'identité de chaque utilisateur. Lorsqu'un utilisateur envoie un document signé numériquement à un autre utilisateur, il faut qu'il envoie également son certificat et sa clé publique. Ces certificats sont émis par une autorité de certification, ils sont généralement valide pendant un an, après quoi le signataire doit renouveler ou obtenir un nouveau certificat de signature afin d'établir son identité.

Voila le certificat qu'on a obtenu :

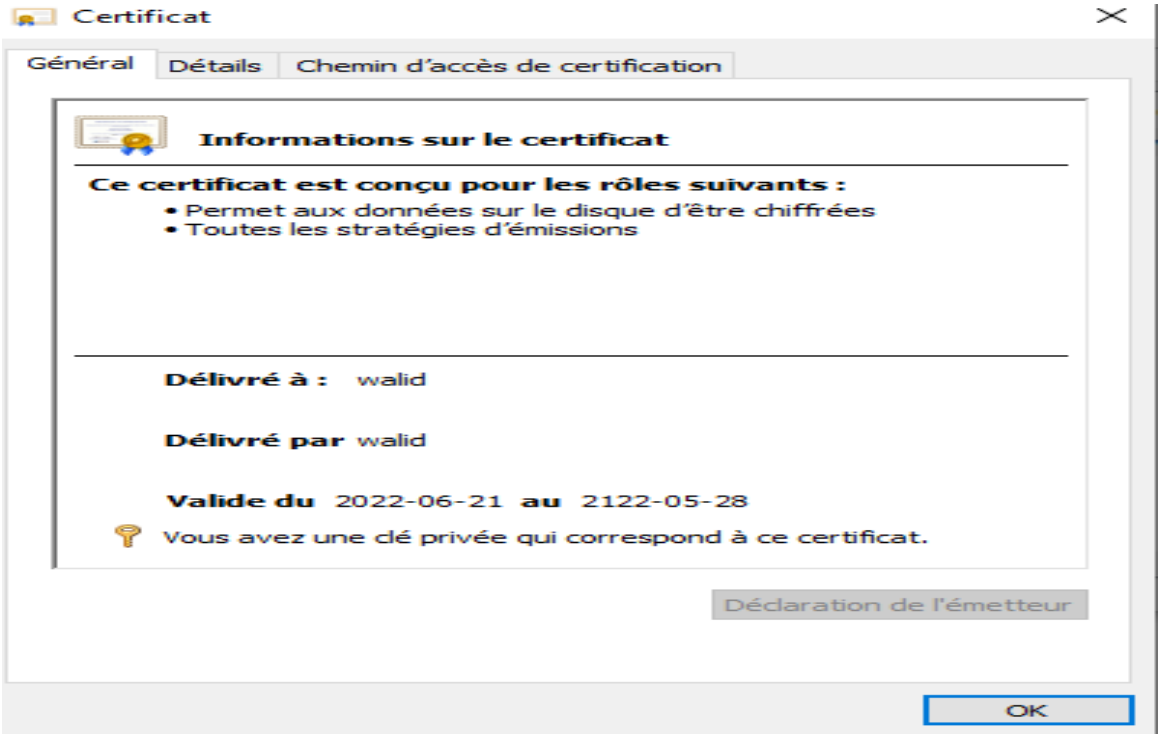


Figure 27 : Les informations sur le certificat obtenu.

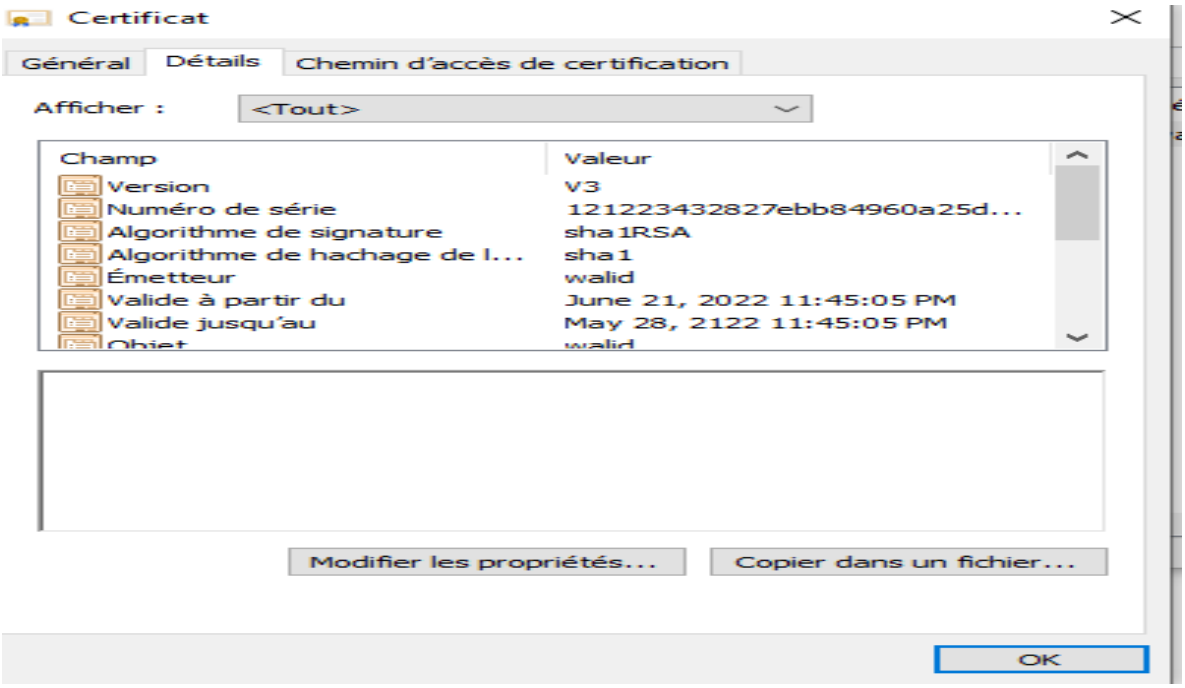


Figure 28 : Les détails sur le certificat obtenu.

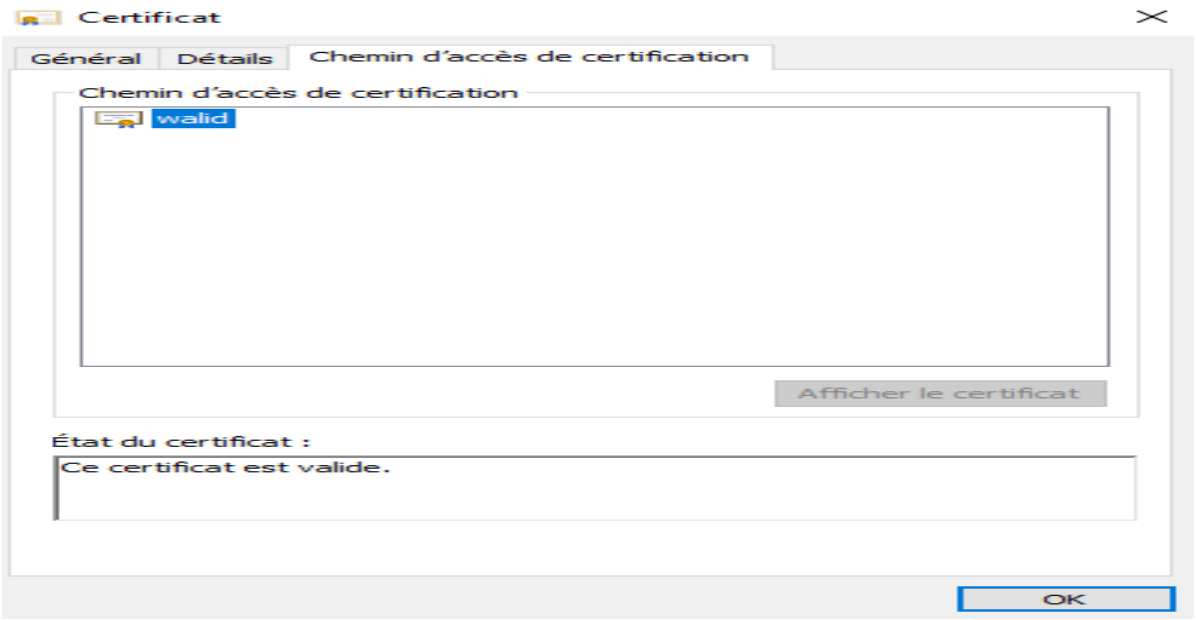


Figure 30 : Le chemin d'accès de certification.

3- Conclusion

Dans ce chapitre, nous avons modélisé un système de cryptographie des documents dans une plateforme de GED, on a appliqué la signature numérique sur les différents formats des documents, pour se faire nous avons utilisé le langage UML pour la conception de la solution proposée. Dans le chapitre qui suit nous allons aborder la partie Réalisation où on a réalisé un système de signature numérique des documents en utilisant des certificats numériques.

Chapitre 4 :

Réalisation

1- Introduction

Le choix du langage s'est porté sur le PHP, qui est un langage de scripts généraliste et Open Source, spécialement conçu pour le développement d'applications Web. Il peut être intégré facilement au HTML. Notre choix s'est porté sur Sublime-text et Bootstrap Studio, qui nous fournissent le confort et la simplicité nécessaires à un développement propre et rapide. Dans le présent chapitre nous allons présenter le système que nous avons conçu. Les principales interfaces du système sont montrées par des captures d'écran.

2- Les outils utilisés pour le codage

2-1 Bootstrap Studio

Bootstrap est un framework développé par l'équipe du réseau social Twitter. Proposé en open source (sous licence MIT), ce framework utilisant le langage 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 ».

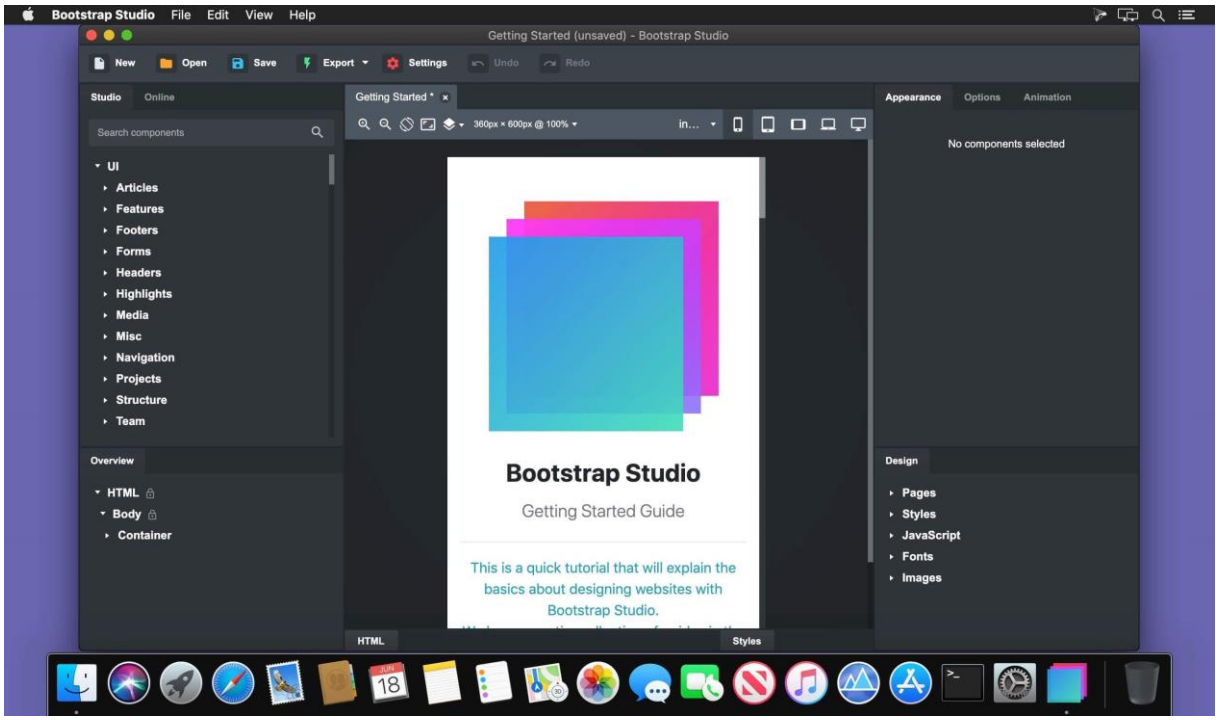


Figure 26: Bootstrap Studio

2- Un essai sur le fonctionnement de l'application

Commençant par la création d'un nouveau compte, l'administrateur ajoute un nouveau utilisateur.

Figure 31 : Demande d'inscription d'un nouvel utilisateur

Une fois l'inscription est effectuée, l'administrateur s'authentifie pour qu'il accepte la demande de création du compte.

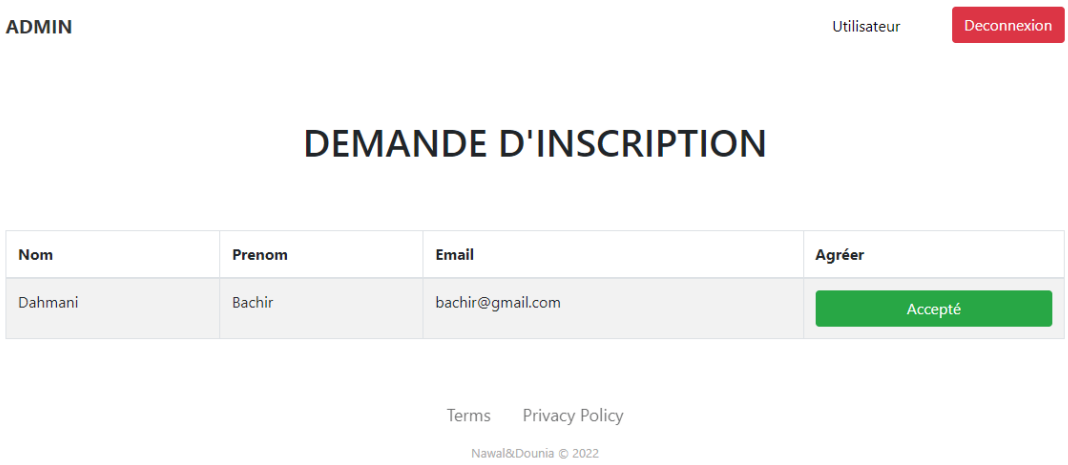


Figure 32 : Accepter la demande de création

Après l'acceptation par l'administrateur, l'utilisateur renseigne son login.

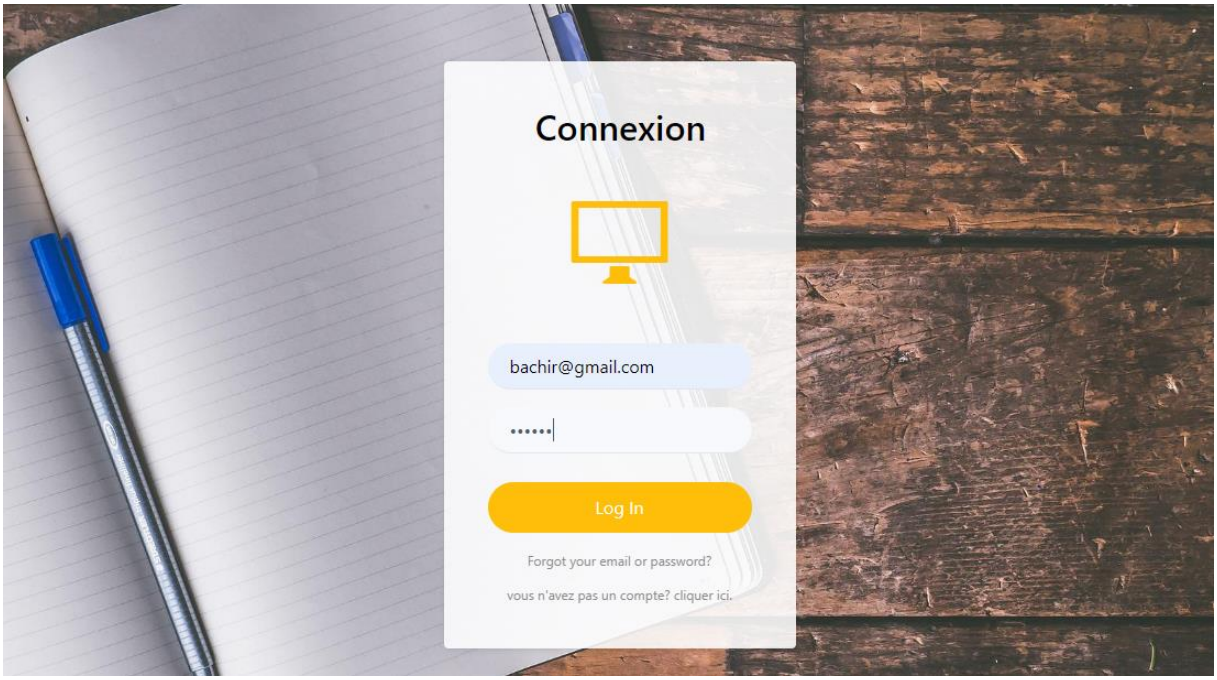


Figure 33 : le login de l'utilisateur

Après la connexion de l'utilisateur, il télécharge sa clé privée.

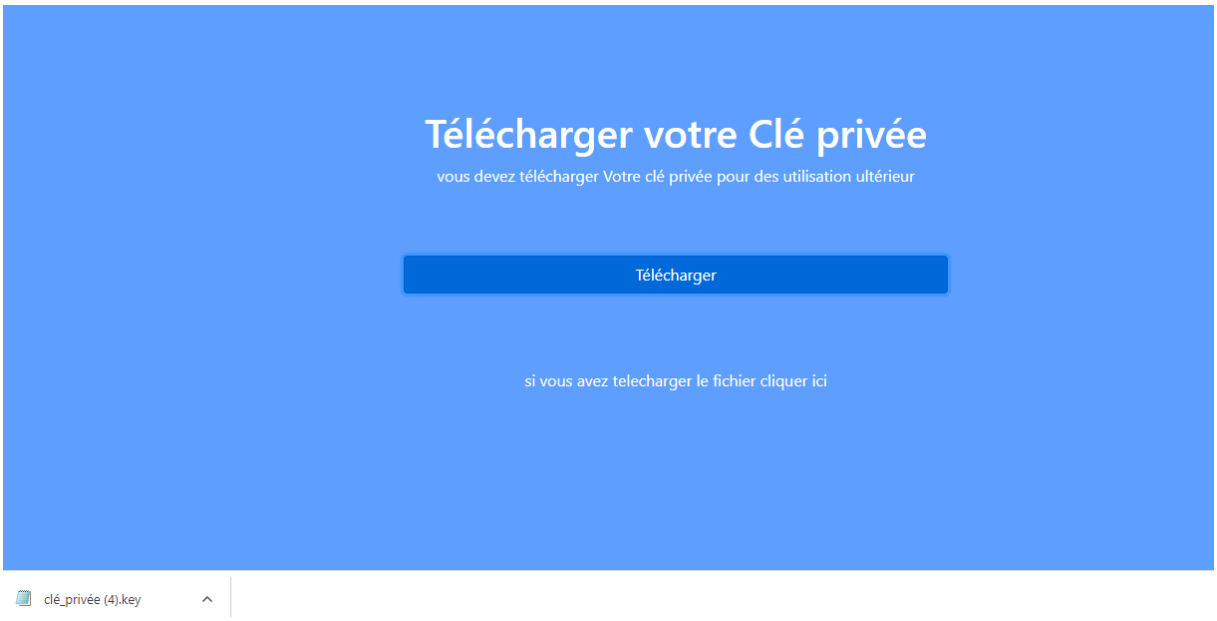


Figure 34 : La clé privée de l'utilisateur

Après le téléchargement de la clé privée, l'utilisateur pourra envoyer des documents à d'autres utilisateurs, il suffit juste de télécharger le fichier à envoyer et sa clé privée.

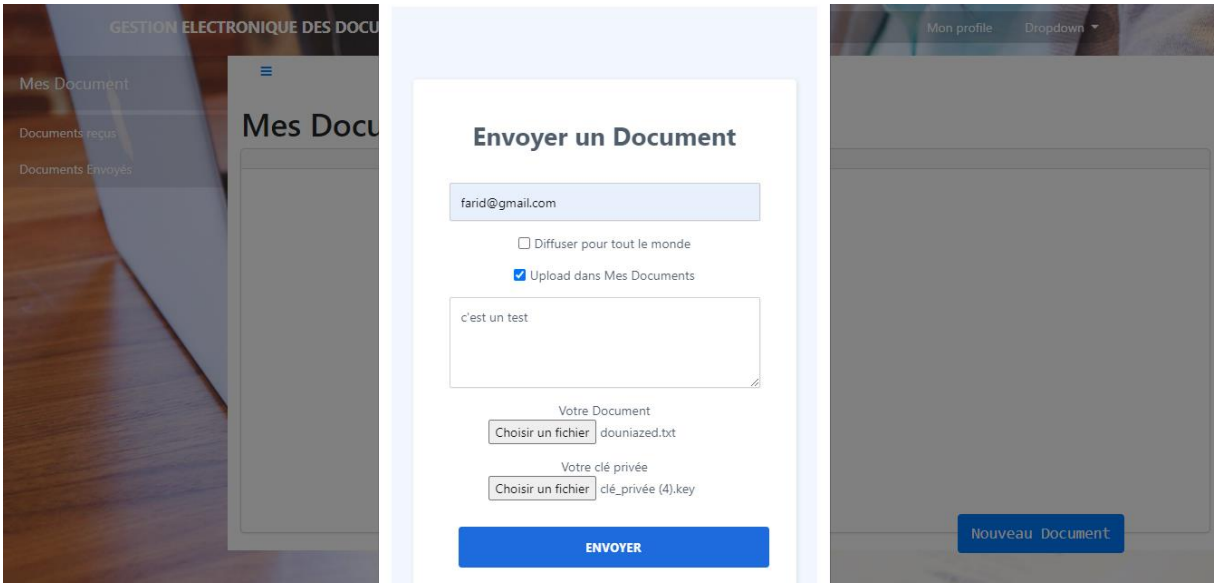


Figure 35 : Envoyer un document

Le récepteur renseigne son login pour la vérification de sa liste des documents reçus.

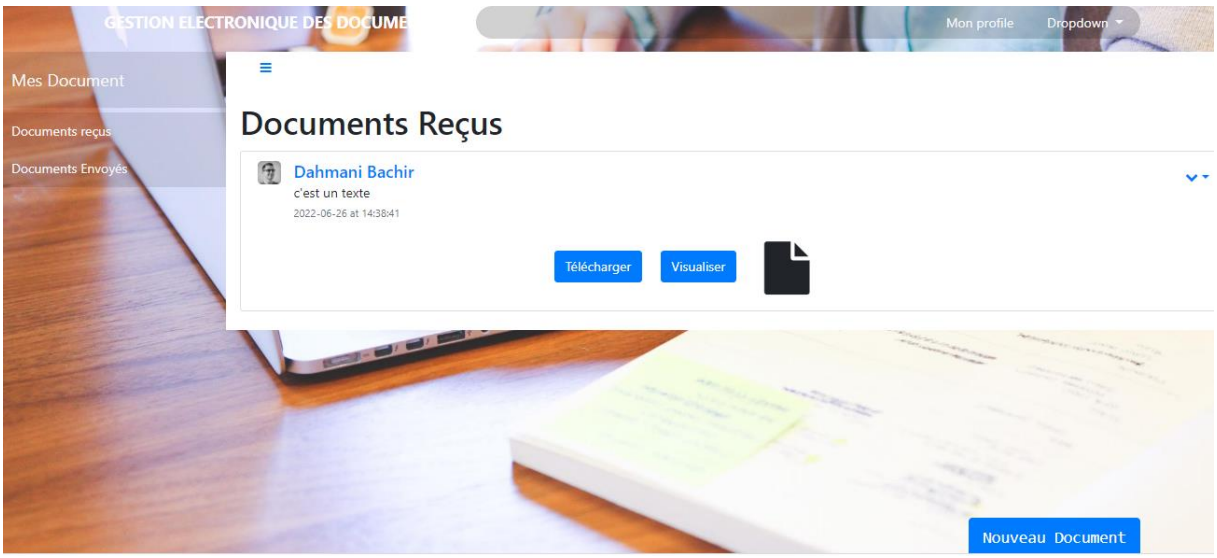


Figure 36 : Les documents reçus

Le récepteur peut télécharger ou bien visualiser le document reçu, si le document reçu n'a pas subi de modifications il le télécharge ou bien le visualise, sinon elle affichera une page d'erreur : le document n'est pas sécurisé.

Figure 37 : Page d'erreur de sécurité « le document n'est pas sécurisé »

3- Les interfaces essentielles de l'application développée

5-1 L'interface de l'authentification

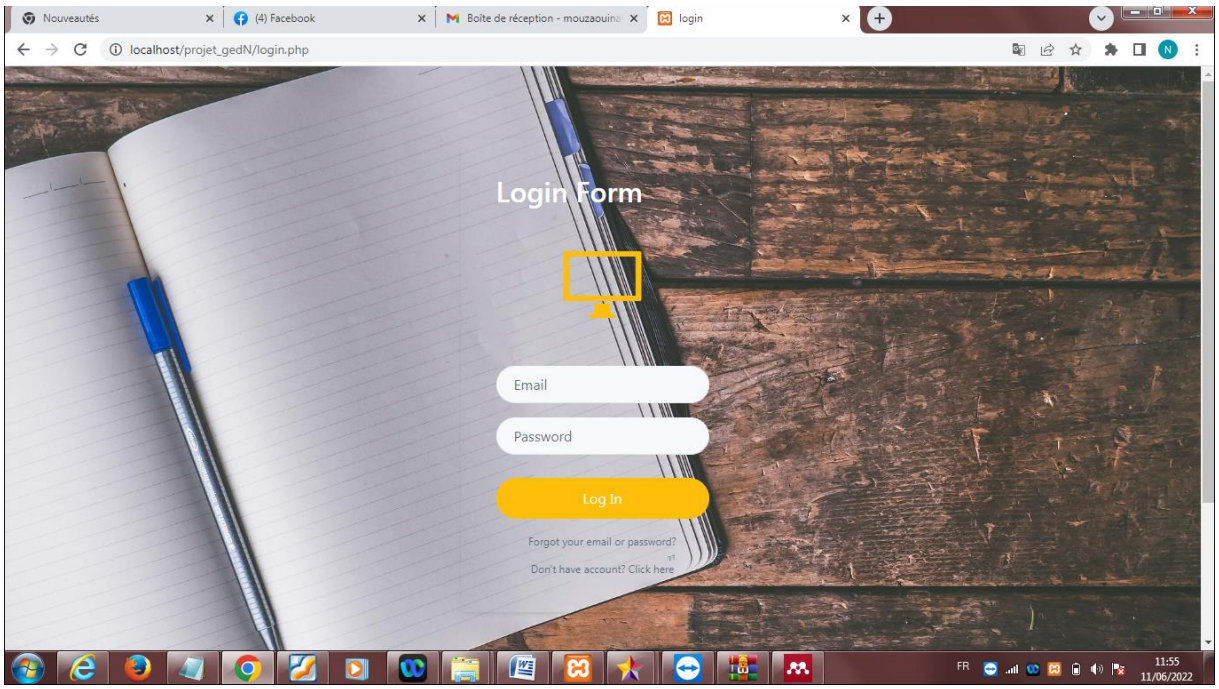


Figure 30 : L'interface de l'authentification

Ce premier lancement nous redirige vers une page d'authentification, un formulaire qui permet de renseigner l'email de l'utilisateur et son mot de passe pour accéder à l'application.

5-2 L'interface de demande de création d'un nouveau compte

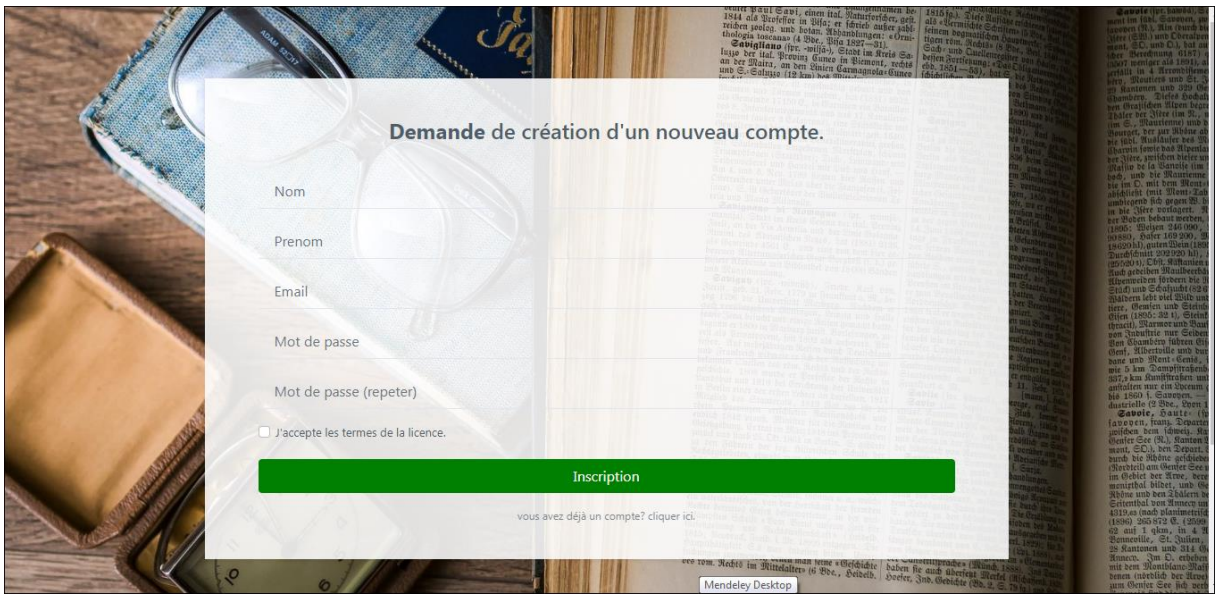


Figure 31 : L'interface de demande de création d'un nouveau compte

Ici l'utilisateur qui ne possède pas un compte déjà, l'administrateur lui donne l'accès à la création d'un nouveau compte. L'administrateur approuve la demande de création du compte, et une clé privée se génère pour l'utilisateur. L'utilisateur doit cacher sa clé privée.

Figure 32 : Téléchargement de la clé privée.

Après que la demande de création du compte est acceptée par l'administrateur, cette page va s'afficher, ou l'utilisateur peut télécharger sa propre clé privée. Une fois la clé privée est téléchargée, il doit cacher le fichier qui contient cette clé.

5-3 L'interface de l'utilisateur

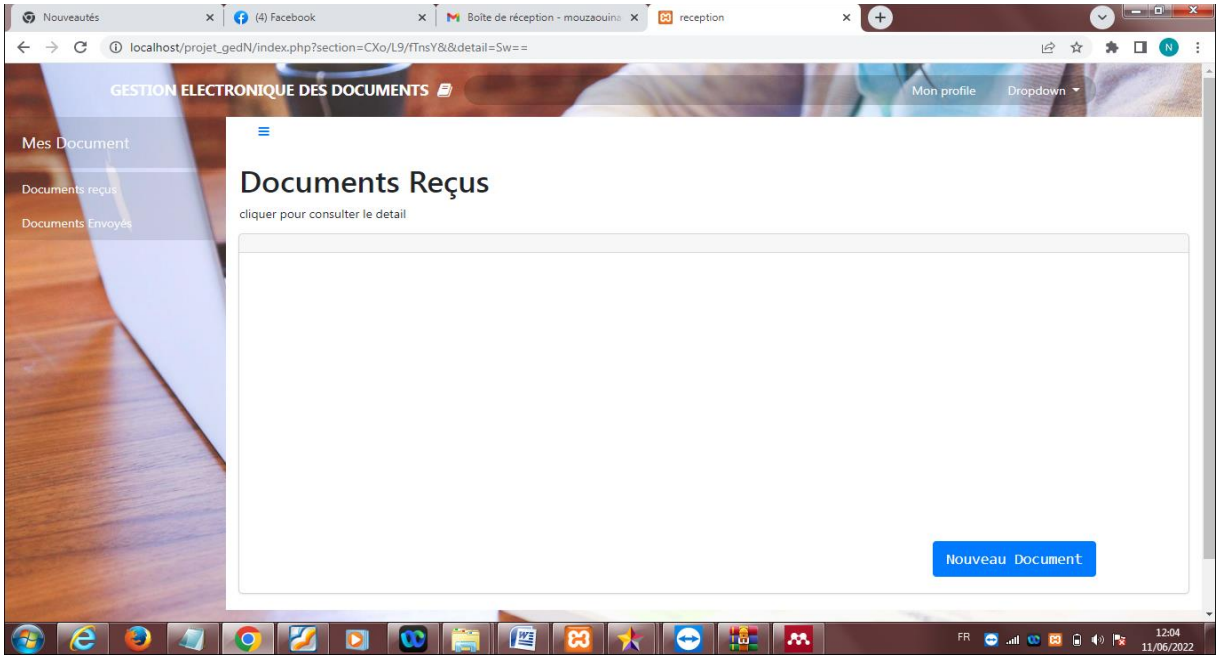


Figure 33 : L'interface de l'utilisateur

L'utilisateur peut envoyer, diffuser et recevoir des documents, les documents doivent être signés numériquement avant l'envoie et aussi vérifiés après la réception (vérifier la signature s'elle est valide sinon le document n'est pas sécurisé).

5-4 L'interface de l'administrateur

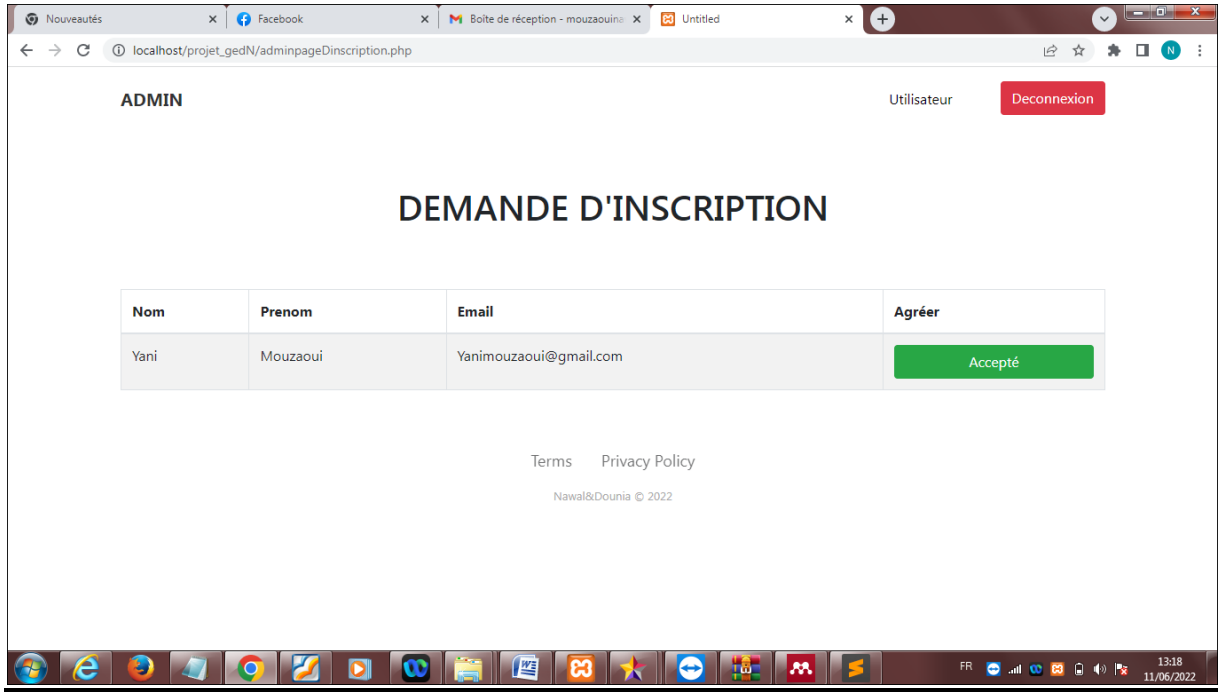


Figure 34 : l'interface 1 de l'administrateur

L'administrateur gère la liste des demandes d'inscription, lorsqu'il accepte la demande d'inscription d'un nouvel utilisateur, une clé privée se génère pour l'utilisateur.

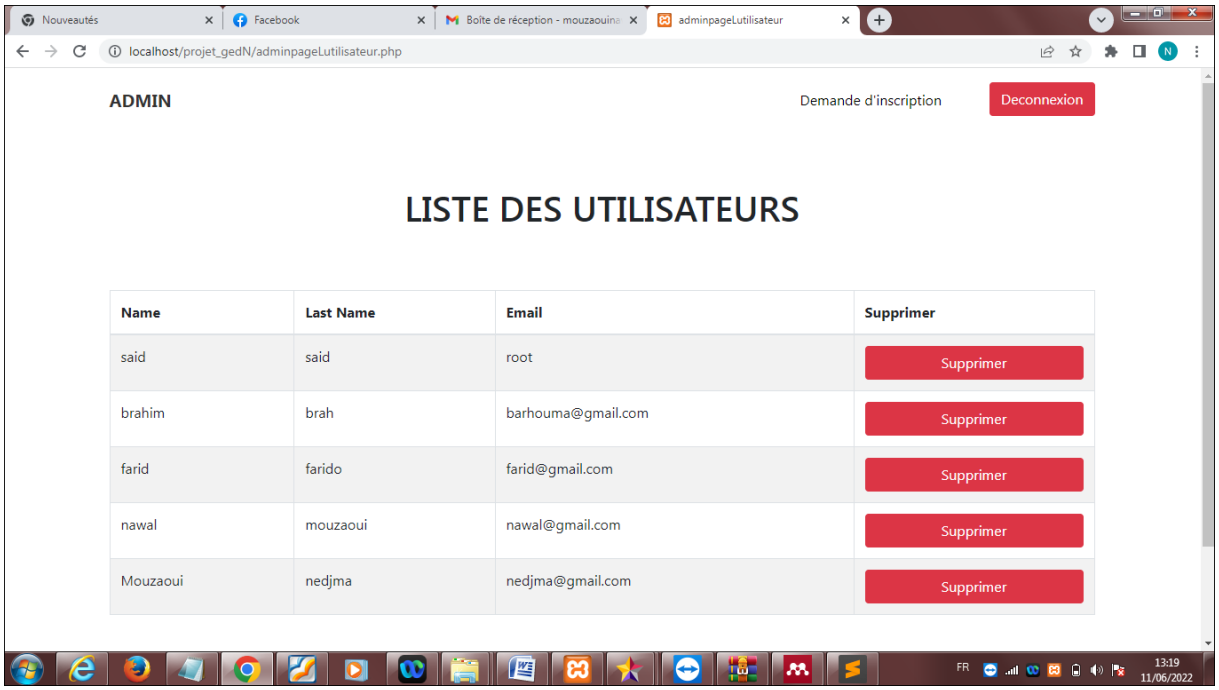


Figure 35 : L'interface 2 de l'administrateur

Un administrateur étant celui qui est chargé de gérer les utilisateurs et leurs comptes ainsi que le système, il doit accéder à toutes les parties de l'application.

5-5 L'interface de l'envoie d'un document

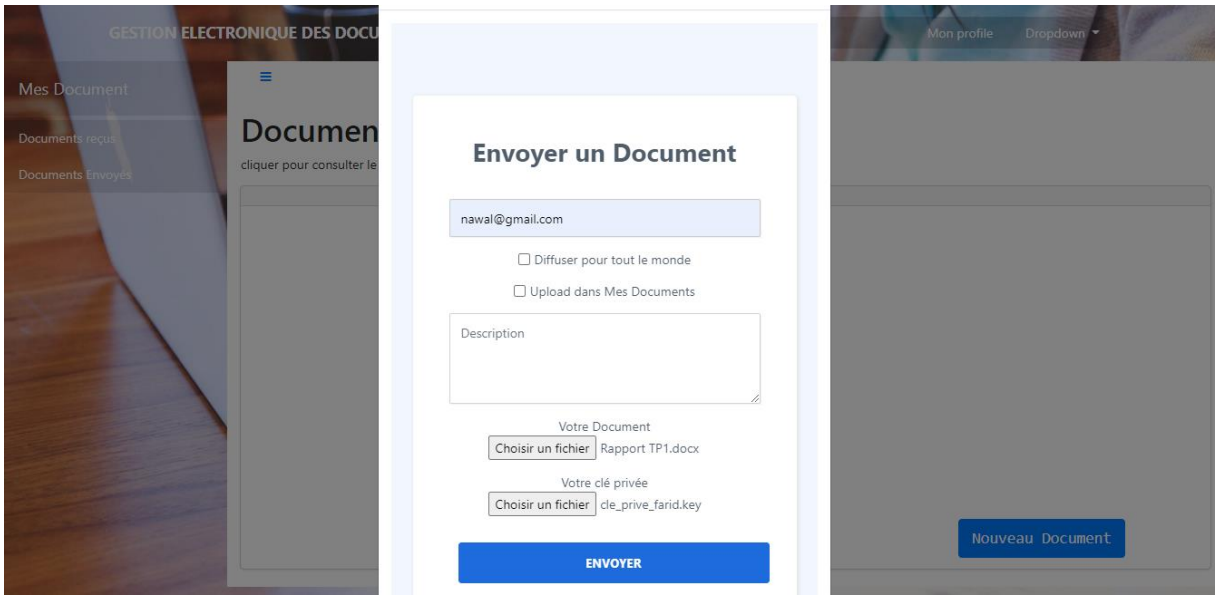


Figure 36 : l'interface de l'envoie du document

Ici l'utilisateur envoie un document, il choisie d'abord le fichier qu'il voudrait envoyer et puis il choisie le fichier ou il a stocké sa clé privée. C'est la qu'on crée la signature numérique du document qui sera envoyé par l'utilisateur, et ça à l'aide du certificat qu'on a obtenu. Lorsque l'utilisateur envoie un document signé numériquement, et envoie également son certificat et sa clé publique, ce certificat est généralement valide pendant un an, après quoi l'utilisateur (signataire) doit renouveler ou obtenir un nouveau certificat de signature afin d'établir son identité.

5-6 visualiser un document non sécurisé

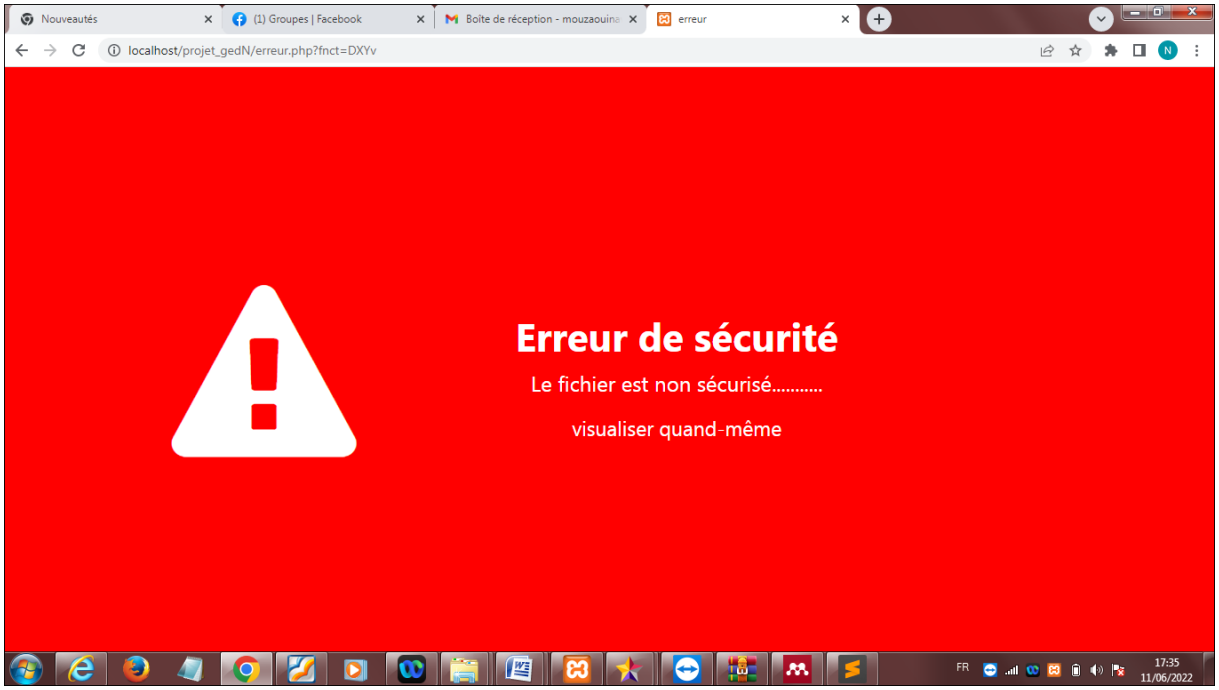


Figure 37 : Visualiser un document non sécurisé

Ici le document s'il a déjà subi des modifications ou bien il est changé carrément par un autre document qui contient juste le même nom, ce message d'erreur de sécurité s'affichera.

4- Conclusion :

Dans ce chapitre, nous avons présenté les différents outils et technologies qui on été utilisés pour réaliser cette solution, nous avons achevé les parties essentielles de la solution en respectant la conception de l'application. Quelques interfaces ont été présentées pour bien clarifier les étapes d'utilisation de la solution proposée dans ce projet de fin d'étude.

Conclusion générale

La cryptographie des documents ou bien plus précisément la signature numérique, est un mécanisme permettant de garantir l'intégrité d'un document électronique d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. La signature numérique va permettre aux établissements qu'ont l'adopté de réduire les dépenses et de gagner du temps et de la flexibilité.

Afin de fixer les idées sur le domaine de la cryptographie, une étude théorique approfondie a été donnée tout au début de ce mémoire. L'analyse et la conception de système réalisé ont été détaillées dans un chapitre séparé, ces détails nous ont permis de réaliser d'une façon solide la cryptographie des documents dans une plateforme de GED. Le travail réalisé a été exposé dans la dernière partie de ce mémoire.

Dans ce projet nous avons réalisé un système de cryptographie des documents de différents formats, ou on a réalisé ce travail avec le langage php. Ce travail est générique car il est utilisable pour et par toute entreprise qui le souhaite et qui dispose des moyens pour l'adopter.

Ce travail constituant un grand chantier, des améliorations ultérieures sont à venir. Ainsi, en guise de perspectives, nous prévoyons l'amélioration vers la signature multiple est une étape très importante pour la mise en valeur de la signature numérique.

Bibliographie

[1] S. Gavillet, “Bien formaliser son projet de GED : préconisations selon le triptyque organisation , technique , humain . Illustration avec le cas du Département Monétique de la To cite this version : Bien formaliser son projet de GED : préconisations selon le triptyque ,” 2012.

[2] H. Sciences, “ETUDE SUR LA GESTION ELECTRONIQUE DE DOCUMENTS,” vol. 4, no. 1, pp. 1–23, 2016.

[3] M. Goncalves and T. Ceillier, “Stratégie , Choix et Mise en œuvre d ’ un système de gestion électronique de documents (GED) Déclaration,” 2010.

[4] S. Kallel, “Mémoire,” 1998.

[5] A. Cunningham, “The archival management of personal records in electronic form: some suggestions,” *Arch. Manuscripts*, vol. 22, no. 1, p. 94, 1994.

[6] International Countil for Archives, *Guide for Managing Electronic Records From an Archival Perspective Committee on Electronic Records February 1997*, no. February. 1997.

[7] A. Liebert, “Master 2 GIDE La Gestion Electronique des documents,” pp. 1–40, 2008.

[8] S. Landry and S. Landry, “Étude de la résistance des algorithmes cryptographiques symétriques face à la cryptanalyse moderne To cite this version : HAL Id : tel-03549775,” 2022.

[9] jean francois PILLOU, “Tout_sur_la_securite_informatique.pdf.” 2013.

[10] M. Leblanc, “Projet Crypto-Share Projet Crypto-Share Assurer la confidentialité des documents de travail,” 2016.

[11] Q. Alamelou, “Protocoles cryptographiques pour l’authentification numérique et le respect de la vie privée,” 2017.

[12] R. Algerienne and D. Et, “Remerciements,” pp. 2020–2021, 2021.

[13] D. Mercier and I. Antilles-guyane, “A LA MATHEMATIQUE,” pp. 59–90, 2002.

[14] B. Hes, D. L. Conseiller, P. Daehne, and P. H. E. S. Gen, “La cryptographie Déclaration,” 2015.

[15] U. De Batna, “Thèse,” 2017.

[16] B. Morin, C. Llorens, and L. Levier, *Tableaux de bord sécurité réseau Offre exceptionnelle sur le site Web du livre ! Élaborer une politique de sécurité réseau et*

mettre en place. 2010.

[17] O. A. M. A. H Kara, "**済無**No Title No Title No Title," *Pap. Knowl. . Towar. a Media Hist. Doc.*, vol. 7, no. 2, pp. 107–15, 2014.

[18] **宗成庆**, *No Title**统计自然语言处理（第二版）*. .

[19] Chaumier, 1996.

[20] Liebert, 2008.

[i] https://s3.amazonaws.com/s3.timetoast.com/public/uploads/photos/12530574/scytale.jpg

[ii] https://th.bing.com/th/id/OIP._hB-Cp87M-ixWJAH3dWjhgHaJI?w=151&h=196&c=7&r=0&o=5&pid=1.7

[iii]https://th.bing.com/th/id/OIP.6OaCHAVOG00zpN3_so8o7wHaJe?w=138&h=180&c=7&r=0&o=5&pid=1.7

[iv]https://www.researchgate.net/profile/Muhammad_Mushtaq31/publication/321587376/figure/download/fig4/AS:568581112987648@1512571709096/Data-Encryption-Standard-DES-Algorithm.png?_sg=LY9QFfSd2CM4zn9ARogTbsX1AyigJLIdiKN2ZtbHiZkJBx7gnP4Sk_EqGHFFKsRME7Czw69ViO8